
Article:
Tzanou, M. and Karyda, S. (2022) Privacy International and Quadrature du Net: One step forward two steps back in the data retention saga? European Public Law, 28 (1). pp. 123-154. ISSN: 1354-3725

https://doi.org/10.54648/euro2022007

Privacy International and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?

Maria TZANOU* & Spyridoula KARYDA**

The present contribution aims to critically reflect on the future direction of data retention at the EU and the national levels by discussing the lessons arising from two seminal Court of Justice of the EU (CJEU) decisions: Privacy International and Quadrature du Net. The article addresses four main themes: (1) the broad reach of EU data privacy law, (2) the detailed typology of permissible data retention models and the conditions applicable to these, (3) the evolving interaction between the CJEU and the European Court of Human Rights (ECtHR) in cases of bulk surveillance, and (4) the relevant legislative developments regarding data retention enshrined in the proposed ePrivacy Regulation. It advances four main lines of criticism. The first concerns the Court's reasoning regarding the expansive scope of application of EU data protection law that – while anticipated – appears unconvincing. The second regards the shortcomings and weaknesses in the CJEU's analysis laying down a taxonomy of permissible data retention systems. The third line of criticism is broader and concerns the progressive re-legitimisation of bulk as well as other surveillance models that seems to be the path undertaken by both the CJEU and ECtHR. Finally, we criticize the ways the EU legislature is trying to 'circumvent' the CJEU's data retention rulings.

Keywords: data retention, EU fundamental rights, Privacy International, Quadrature du Net, bulk data retention, EU data protection law, European Court of Human Rights Big Brother Watch, GDPR, ePrivacy, UK adequacy decisions after Brexit

1 INTRODUCTION

On 6 October 2020, the Grand Chamber of the Court of Justice of the European Union (EU) ('CJEU' or 'the Court') delivered its seminal decisions in two cases

* Senior Lecturer, School of Law, Keele University. Her research focuses on European constitutional and human rights law, privacy, data protection, AI, big data, surveillance and transatlantic data privacy cooperation. She is the author of *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance* (Hart, 2017) and the editor of *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020) and *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Responses* (Routledge, 2021). Email: m.tzanou@keele.ac.uk.

** Associate Councilor (Judge) at the Hellenic Council of State, LL.M. in Space, SatCom and Media Law, University of Luxembourg, Vice-President of the Committee on the implementation of the GDPR and the LED to Greece, EJTN expert on Data Protection and Privacy Rights. Email: rkar64@gmail.com.

Tzanou, Maria & Karyda, Spyridoula. '*Privacy International* and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?'. *European Public Law* 28, no. 1 (2022): 123–154.

that concerned data retention for national security purposes: *Privacy International*[1] and *La Quadrature du Net*.[2] In these, the Court confirmed that bulk metadata retention laws for national security purposes fall within the scope of EU data protection law, it clarified the rules regarding prohibited and permissible surveillance and set out the limits and conditions under which permissible surveillance can be carried out.

The two judgments, along with *HK v. Prokuratuur*[3] rendered on 2 March 2021, are the latest additions to the Court's long and ongoing data retention 'saga',[4] which commenced in 2014 with *Digital Rights Ireland*,[5] where the CJEU invalidated the Data Retention Directive[6] ruling that indiscriminate bulk metadata retention is incompatible with EU law; culminated in 2017 with *Tele2 and Watson*,[7] where the Court held that the *Digital Rights Ireland* principles applied to national laws implementing the invalidated Data Retention Directive; and, continued in 2018 with *Ministerio Fiscal*,[8] in which the CJEU clarified that different types of data retention measures entail different levels of interference to fundamental rights.

Privacy International and *Quadrature du Net* should be read against the background of this line of case-law. However, while *Privacy International* continues along the same lines of this expansive data protection jurisprudence and can be seen as 'another victory for fundamental rights'[9] this time in the context of national security; *Quadrature du Net* marks an important departure from the CJEU's prohibitive approach to bulk data retention to a more nuanced one that cracks the door open for a variety of different permissible surveillance measures if these are carried out under certain criteria and applicable safeguards.

---

1 Case C-623/17 *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790.

2 Joined Cases C 511/18, C 512/18 and C 520/18 *La Quadrature du Net and Others v. Premier Ministre and Others* ECLI:EU:C:2020:791 (hereinafter *Quadrature du Net)*.

3 Case C-746/18 *HK v. Prokuratuur* ECLI:EU:C:2021:152.

4 *See* Mark Cole & Franziska Boehm, *EU Data Retention – Finally Abolished?, Eight Years in Light of Article 8*, 97 Critical Q. Legis. & L. 58, 78 (2014); Edoardo Celeste, *The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios*, 15 Eur. Const. L. Rev. 134, 135 (2019).

5 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12) ECLI:EU:C:2014:238.

6 Directive 2006/24/EC of 15 Mar. 2006 on the retention of data generated or processed in connection with the provisions of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54.

7 C-203/15 *Tele2 Sverige AB v. Post-ochtelestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* ECLI:EU:C:2017:214.

8 Case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788.

9 Maria Tzanou, *European Union Regulation of Transatlantic Data Transfers and Online Surveillance*, Hum. Rts. L. Rev. 545, 546 (2017).

The present contribution aims to critically reflect on the future direction of data retention at the EU and the national level by discussing the lessons arising from *Privacy International* and *Quadrature du Net*. In this respect, it addresses four main themes: (1) the broad reach of EU data privacy law, (2) the detailed typology of permissible data retention models and the conditions applicable to these, (3) the evolving interaction between the CJEU and the European Court of Human Rights (ECtHR) in cases of bulk surveillance, and (4) the relevant legislative developments regarding data retention enshrined in the proposed ePrivacy Regulation.[10]

We advance four main lines of criticism. The first concerns the Court's reasoning regarding the expansive scope of application of EU data protection law that – while anticipated – appears unconvincing. The second regards the shortcomings and weaknesses in the CJEU's analysis laying down a taxonomy of permissible data retention systems. The third line of criticism is broader and concerns the progressive re-legitimisation of bulk as well as other surveillance models that seems to be the path undertaken by both the CJEU and ECtHR. Finally, we criticize the ways the EU legislature is trying to 'circumvent' the CJEU's data retention rulings.

2 THE JUDGMENTS OF THE COURT

Both *Privacy International* and *Quadrature du Net* concerned preliminary questions referred to the CJEU. The *Privacy International* case was about the acquisition and use of bulk communications data by the various security and intelligence agencies in the United Kingdom, namely the Government Communications Headquarters (GCHQ), the Security Service (MI5) and the Secret Intelligence Service (MI6) for national security purposes. Such data, commonly known as traffic location data or 'metadata' concern the 'who', 'when', 'where' and 'how' of the communication, but not its content.

Quadrature du Net concerned several challenges regarding data retention under the French (*La Quadrature du Net*, Cases C-511/18 and C-512/18) and Belgian (*Ordre des barreaux francophones et germanophone* Case C-520/18) national security laws lodged by a number of non-governmental organizations (NGOs) before the Conseil d'État (Council of State, France) and the Cour constitutionnelle (Constitutional Court, Belgium) respectively.

[10] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, ePrivacy Regulation), 10 Feb. 2021, COM/2017/010 final.

Several preliminary questions were referred to the CJEU, which concerned two main issues: (1) the *scope* of the 'ePrivacy Directive'[11]; and (2) the *interpretation* of the ePrivacy Directive with regard to (1) the compatibility with EU law of different types of national legislative measures providing for the preventive retention of electronic communications metadata for the purposes of safeguarding national security, combating crime and safeguarding public security; and (2) the permissibility of automated analysis and real-time collection of metadata.

The Grand Chamber delivered a long judgment that spans in over eighty pages in *Quadrature du Net* and a much briefer decision in *Privacy International*. The CJEU commenced its discussion from an issue heavily contested by the Member States: the *scope* of application of the ePrivacy Directive. In particular, nine Member States (the Czech Republic, Estonia, Ireland, France, Cyprus, Hungary, Poland, Sweden and the United Kingdom) argued that the ePrivacy Directive was not applicable to national legislation whose purpose is the safeguarding of national security[12] as the activities of intelligence services 'are part of the essential functions of the Member States' and, consequently, fall within their 'exclusive competence' in accordance with Article 4(2) Treaty on the European Union (TEU).[13] The Court disagreed with the Member States and held that national legislation which requires electronic communications service providers (ECSPs) to retain metadata for the purposes of protecting national security and combating crime falls within the scope of the ePrivacy Directive.[14]

It then reiterated a general prohibitive rule: national laws that require as a preventive measure, the general and indiscriminate retention of data by telecommunications providers are precluded under EU law.[15] However, the Court distinguished in *Quadrature du Net* other factual circumstances where data retention was found to be permissible. It held that the general and indiscriminate retention of telecommunications' metadata 'in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable' is allowed under the ePrivacy Directive and the EU Charter of Fundamental Rights (EUCFR), provided that certain safeguards are established.[16]

---

11 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11 (ePrivacy Directive).

12 *Quadrature du Net*, *supra* n. 2, para. 89.

13 *Ibid*.

14 *Ibid*., para. 104.

15 *Ibid*., para. 168.

16 *Ibid*.

According to the pronouncements of the Court, also permitted for the purposes of safeguarding national and public security and combating serious crime are: the targeted retention of metadata which is limited on the basis of objective and non-discriminatory factors and undertaken for a limited period; the general and indiscriminate retention of Internet Protocol (IP) addresses assigned to the source of an Internet connection for a limited period; the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and, instructions requiring ECSPs, to undertake for a specified period of time, the expedited retention of metadata in their possession. All these national measures are allowed provided that they ensure that data retention 'is subject to compliance with the applicable substantive and procedural conditions' and that 'the persons concerned have effective safeguards against the risks of abuse'.[17] Finally, the Court dealt with modern methods of counter-terrorism surveillance that employ automated analysis of metadata and require the real-time collection of technical data concerning the location of users' terminal equipment and concluded that both are permissible under a number of strict conditions.

3 ANALYSIS

3.1 The application of EU law to national data retention measures

In *Privacy International* and *Quadrature du Net*, the Court clarified once and for all an issue of particular importance to the Member States: the applicability of EU law to domestic legislation adopted to safeguard national security. The issue had arisen in several cases over the past years (*Tele2, Ministerio Fiscal*), with the Member States insisting that intelligence services' activities relating to the maintenance of public order and the safeguarding of internal security and territorial integrity, are part of their essential functions and, consequently, fall within their exclusive competence, according to the basic principle under Article 4(2) TEU. The CJEU took the opportunity to put the debate to bed by introducing a fundamental distinction: National laws that require ECSPs to retain metadata or grant access to this to national authorities for the purpose of safeguarding national security fall within the scope of the ePrivacy Directive and, therefore, the EUCFR and EU law more broadly. By contrast, national laws that do not impose any obligations on ECSPs, but directly implement national security measures fall outside the scope of the ePrivacy Directive (and EU law) even if these derogate from the principle of confidentiality of electronic communications.[18]

---

17 *Ibid*.

18 *Ibid*., para. 103. The Court recognized, however, that these rules may be subject to the application of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

The crucial aspect of the distinction concerns the involvement of ECSPs and the allocation of data processing obligations to these. Any obligations imposed on ECSPs trigger the application of the ePrivacy Directive no matter the purpose for the access to the data. If, however, the data is directly retained by national authorities without the compelled cooperation of ECSPs, the ePrivacy Directive is not applicable – in this case such measures must comply with national constitutional law requirements and the European Convention on Human Rights (ECHR).

The distinction drawn by the Court is based on the ePrivacy Directive that contains two different provisions: Article 1(3) excludes from its scope 'activities of the State' in the areas of public security, defence and State security (the Advocate General (AG) called this the 'exclusion' clause)[19]; while, Article 15 (1) permits the adoption of national laws that restrict the confidentiality of electronic communications appropriate for national and public security purposes (the AG called this the 'restriction' or 'limitation' clause). The CJEU used here an *effet utile* argument: a different interpretation of the ePrivacy Directive that confounds the two provisions due to the substantial overlap of the public interest objectives under Articles 1(3) and 15(1) would deprive the latter rule of any practical effect.[20]

While the Court's analysis on the application of EU law to national data retention measures appears well-argued, its reasons for departing from its 2006 *Parliament v. Council and Commission (Passenger Name Records [PNR])* judgment,[21] are less convincing. It should be recalled that in *PNR* the CJEU held that the transfer of PNR data by airlines to US public authorities for the purpose of preventing and combating terrorism fell outside the scope of the Data Protection Directive (DPD) because it related to public security.[22] The CJEU's distinction of *Quadrature du Net* from *PNR* is based on a comparison between Article 3(2) of the DPD and Article 1 (3) of the ePrivacy Directive. Pursuant to the Court – which followed the AG on this point – Article 3(2) DPD 'excluded, in a general way' from the scope of the DPD processing operations concerning public security, defence, and State security, 'without drawing any distinction according to *who* was carrying out the data processing operation concerned'.[23] The Court opined that:

---

execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Law Enforcement Directive-LED).

19 *See* Opinion of Advocate General Campos Sánchez-Bordona delivered on 15 Jan. 2020 Joined Cases C 511/18 and C 512/18 *La Quadrature du Net*, para. 48.

20 *Ibid.*, para. 97.

21 Joined Cases C-317/04 and C-318/04, *Parliament v. Council and Commission*, ECLI:EU:C:2006:346.

22 *Ibid.*, paras 56 and 59.

23 *Quadrature du Net*, *supra* n. 2, para. 101. Emphasis added.

> by contrast, […] all operations processing personal data carried out by providers of electronic communications services fall within the scope of [the ePrivacy] directive, including processing operations resulting from obligations imposed on those providers by the public authorities, although those processing operations could, where appropriate, on the contrary, fall within the scope of the exception laid down in … Article 3(2) of Directive 95/46.[24]

The above analysis is circular and introduces a distinction that makes little sense. The CJEU and the AG seem to be based on minor linguistic variations between the texts of the DPD, the ePrivacy Directive and the General Data Protection Regulation (GDPR) to convince that *Quadrature du Net* (and *Tele2*) can be reconciled with the earlier *PNR* judgment. Yet, the linguistic differences between these documents are subtle. More importantly, all the three of them contain both 'exclusion' and 'restriction' clauses as discussed above in the context of the ePrivacy Directive.[25]

What is perhaps more problematic in the CJEU's analysis regarding the application of EU data protection law to national security measures, is its attempt to reconcile this more recent case-law with *PNR*. Indeed, the Court, and the AG, went at great lengths to demonstrate that there has been no departure from the *PNR* judgment. Such an attempt ends up obfuscating the well-reasoned grounds that support the application of EU law to bulk metadata retention for national security purposes. The Court's reluctance to overrule its previous case law is well-known,[26] but a more honest approach that clearly leaves behind the problematic *PNR* judgment would have provided a more solid basis for the application of EU law to national security measures involving private operators. It would have also made a more convincing case to the Member States, which encounter this broad application of EU data protection law with significant skepticism.[27]

Overall, the present cases can be viewed as another confirmation of the broad reach of EU data protection law.[28] Article 4(2) TEU, which provides that 'national security remains the sole responsibility of each Member State' cannot invalidate

---

[24] *Ibid.*, para. 101.

[25] In the GDPR, the exclusion clause is Art. 2(2)(d) and the restriction clause Art. 23(1); in the DPD, the exclusion clause was Art. 3(2) and the restriction clause Art. 13(1). Interestingly the CJEU seemed to entirely forget this provision in its analysis. The Court also considered the interplay between the GDPR and the ePrivacy Directive by acknowledging that the services regarding data relating to the civil identity of persons fall within the latter (para. 195). *See also* EDPB, *Opinion 5/2019 on the Interplay Between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities* (12 Mar. 2019), https://edpb.europa.eu/sites/edpb/files/files/filel/201905_edpb-opinion-eprivacydir-gdpr-interplay-en_0.pdf (accessed 12 Jul. 2021).

[26] Tamás Szabados, *'Precedents' in EU Law – The Problem of Overruling*, ELTE L.J. 125 (2015).

[27] *See* for instance Agence Europe, *La France Monte au Créneau sur la Conservation des Données Personnelles* (4 Mar. 2021), https://agenceurope.eu/fr/bulletin/article/12671/22 (accessed 12 Jul. 2021).

[28] Tzanou, *supra* n. 9, at 549–550.

this conclusion.[29] Indeed, the Court's judicial review expands to the compatibility of national security measures with EU fundamental rights whenever such measures entail a public-private partnership requiring the assisted collaboration of private entities.

3.2 'The exception should not become the rule'[30]: Bulk data retention is (still) prohibited

The most important contribution of *Privacy International* is that it answers the last outstanding question regarding national data retention measures under EU fundamental rights law: Is bulk data retention carried out by intelligence agencies for national security purposes compatible with EU law? *Privacy International* differs from previous cases, such as *Tele2* and the *EU-Canada PNR Agreement* Opinion,[31] because the preliminary questions referred by the Investigatory Powers Tribunal concerned, for the first time, bulk data retention for national security purposes under section 94 of the 1984 Telecommunications Act[32] and not generalized access for any public security purposes.

The Court acknowledged the importance of national security purposes in *Privacy International*, but, nevertheless, maintained the general prohibitory rule of indiscriminate bulk retention even when this is undertaken for national security purposes.[33] It found that the UK's data retention regime under section 94 was problematic for several reasons: it concerned all users of electronic communications; was taking place both in real – and historical time; once transmitted, the data could be subject to bulk automated processing and analysis 'with the aim of discovering unknown threats'[34]; cross-checked with other databases containing different categories of bulk personal data or disclosed outside those agencies and to third countries; and, all those operations did not require prior authorization from a court or independent administrative authority and did not involve notifying the persons concerned in any way.[35]

The Court's judgment in *Privacy International* is significant because it demonstrates that the involvement of national security and intelligence agencies in public-private data surveillance partnerships does not introduce any exception to the basic prohibition of bulk metadata retention. The message to the Member States

---

29 *Quadrature du Net*, *supra* n. 2, para. 99.
30 *See ibid.*, para. 111.
31 Opinion 1/15 (EU-Canada PNR Agreement) of 26 Jul. 2017, EU:C:2017:592.
32 *See also Privacy International*, *supra* n. 1, para. 24 where the IPT draws a distinction between *Tele2* and the present case.
33 *Ibid.*, para. 81.
34 *Ibid.*, para. 25. As the IPT put it, 'the sets of metadata … compiled should be as comprehensive as possible, so as to have a haystack" in order to find the "needle" hidden therein'.
35 *Ibid.*, para. 52.

remains, therefore, clear: general and indiscriminate metadata retention without appropriate safeguards is prohibited under EU law even if this is required by intelligence agencies for national security purposes.

That being said, *Quadrature du Net* established a *hierarchy* of legitimate public interest objectives: at the top of the list comes *national security* which is recognized by the CJEU as a more important objective than the others listed in Article 15(1) ePrivacy Directive. The Court defined national security as:

> the primary interest in protecting the essential functions of the State and the fundamental interests of society [which] encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.[36]

The next level at the hierarchy of objectives includes combating *serious* crime and preventing *serious* threats on public security.[37] The final level includes the objective of *preventing, investigating, detecting and prosecuting criminal offences* – irrespective of seriousness – and safeguarding public security.

This hierarchy of objectives is linked to the seriousness of the interference and corresponds to the permissibility of different types of data retention measures. For instance, national security that ranks at the top of the hierarchy may justify 'measures entailing more serious interferences with fundamental rights than those which might be justified by … other objectives'.[38] This prioritization of national security in the ranking of objectives is also evident in the allowances the Court made in case of serious national security threats.

3.3 A typology of the permissibility of national surveillance measures under EU law

The most significant contribution of *Quadrature du Net* is that it introduces comprehensive guidance on how national surveillance measures can be constructed to comply with EU fundamental rights. The Court had established some broad principles in previous judgments on the (in-)compatibility of different aspects of surveillance measures with the EUCFR,[39] but *Quadrature du Net* is the first case

---

36 *Quadrature du Net*, *supra* n. 2, para. 135.

37 *Ibid.*, paras 140–142.

38 *Ibid.*, para. 139; *Privacy International*, *supra* n. 1, para. 75.

39 *See Digital Rights Ireland*, *supra* n. 5; *Tele2*, *supra* n. 7; *Ministerio Fiscal*, *supra* n. 8; Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner (Schrems I)*, ECLI:EU:C:2015:650; Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II)*, ECLI:EU:C:2020:559. For a commentary *see* Maria Tzanou, *Schrems I* and *Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights*, in *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* 99 (Federico Fabbrini et al. eds, Oxford: Hart 2021).

that develops in a comprehensive manner a typology of permissible national data retention laws.

This list is so prescriptive that at times the Court seems to be assuming a *quasi-legislative* role. Indeed, the CJEU expanded in *Quadrature du Net* its assessment of data retention both *vertically* (entering the Member States' realm) and *horizontally* (entering the legislator's realm). At first glance, one could criticize the CJEU for overstepping its boundaries. However, a deeper analysis of the CJEU's detailed typology in *Quadrature du Net* reveals the complexity of the questions that underpin metadata surveillance: If data retention cannot be harmonized at the EU level, then how would EU fundamental rights be ensured at the national level where data retention measures are fragmented and vary between different Member States? Would a more *laissez-faire* approach not be equally problematic for both fundamental rights and overall legal certainty concerns? The Court chose to adopt a pragmatic approach in *Quadrature du Net* and it would be naïve to criticize it for this.

Pursuant to the CJEU's typology, the compatibility of different data retention regimes with EU fundamental rights depend on several different factors, including (1) the purposes for which surveillance can be undertaken; (2) the conditions under which data retention is allowed; (3) the applicable safeguards; and (4) the possibility of extending the retention laws beyond a certain amount of time. The typology of data retention measures is summarized in Table 1.

Table 1 Compatibility of national data retention measures with EU law

Type of national measure	**Purposes**	**Condition**	**Required Safeguards**	**Extension?**	**Permissibility under EU law**
Preventive, general and indiscriminate retention of metadata					Prohibited
General and indiscriminate retention of metadata	National security	Member State confronted with a serious, genuine and present or foreseeable threat to	Subject to effective review by a court or by an independent administrative body whose decisions are binding For limited period of time	Yes, if the threat persists	Allowed

Type of national measure	Purposes	Condition	Required Safeguards	Extension?	Permissibility under EU law
		national security	Subject to compliance with the applicable substantive and procedural conditions Effective safeguards against the risks of abuse for persons concerned		
Targeted retention of metadata	National security, serious crime, public security		On the basis of objective and non-discriminatory factors According to the categories of persons concerned or using a geographical criterion For limited period of time Subject to compliance with the applicable substantive and procedural conditions Effective safeguards against the risks of abuse for persons concerned	Yes	Allowed
General and indiscriminate retention of IP addresses	National security, serious crime, public security		For limited period of time Subject to compliance with the applicable substantive and procedural conditions Effective safeguards against the		Allowed

Type of national measure	Purposes	Condition	Required Safeguards	Extension?	Permissibility under EU law
			risks of abuse for persons concerned		
General and indiscriminate retention of the civil identity data of users	National security, serious crime, public security		Subject to compliance with the applicable substantive and procedural conditions Effective safeguards against the risks of abuse for persons concerned		Allowed
Expedited retention of metadata	National security, serious crime, public security	For a specified period of time	Subject to effective judicial review Subject to compliance with the applicable substantive and procedural conditions Effective safeguards against the risks of abuse for persons concerned		Allowed
Real-time collection of metadata	Preventing terrorism	In respect of persons to whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities	Based on objective and non-discriminatory criteria provided for in the national legislation Subject to prior review Must be notified to the persons concerned to enable them to exercise their rights		Allowed
Automated analysis of metadata	National security	National laws must	Subject to effective review		Allowed

Type of national measure	**Purposes**	**Condition**	**Required Safeguards**	**Extension?**	**Permissibility under EU law**
		lay down the substantive and procedural conditions governing this	Pre-established models and criteria on which automated analysis is based should be specific, reliable and non-discriminatory Any positive result obtained following automated processing must be subject to an individual re-examination by non-automated means before a measure adversely affecting the persons concerned is adopted Regular re-examination should be undertaken to ensure that the pre-established models and criteria for the automated analysis and the databases used are reliable and up to date Competent national authority obliged to publish information of a general nature relating to automated analysis		

Type of national measure	Purposes	Condition	Required Safeguards	Extension?	Permissibility under EU law
			Person concerned must be notified individually if identified to analyse in greater depth the data concerning them		

3.4 Permissible data retention: An unduly expansive list of surveillance measures?

Notwithstanding the Court's categorical finding in *Privacy International, Quadrature du Net* presents a more nuanced approach to data retention. Indeed, the Court came up with a long list of permissible data retention measures that paints a comprehensive but complex picture of acceptable law enforcement tools and makes several major concessions to Member States' security authorities.[40] The list reflects the hierarchy of public interest objectives discussed above.

3.4[a] *Mass Data Retention Is Allowed in Cases of Serious Threats to National Security*

A first major concession to law enforcement authorities show the Court allowing a general, indiscriminate preventive data retention when Member States are confronted with a 'serious' threat to national security 'which is shown to be genuine and present or foreseeable'.[41]

In *Quadrature du Net*, the Court was asked to consider whether the fundamental right to security enshrined in Article 6 EUCFR[42] imposes on Member States positive obligations to 'take specific measures to prevent and punish certain criminal offences'.[43] It correctly rejected this argument by following the interpretation of Article 5 ECHR by the ECtHR[44] to which Article 6

[40] Juraj Sajfert, *Bulk Data Interception/Retention Judgments of the CJEU – A Victory and a Defeat for Privacy*, European Law Blog (26 Oct. 2020), https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/ (accessed 12 Jul. 2021).

[41] *Quadrature du Net*, *supra* n. 2, para. 136.

[42] Article 6 EUCFR 'Right to liberty and security' provides: 'Everyone has the right to liberty and security of person'.

[43] *Quadrature du Net*, *supra* n. 2, para. 125.

[44] ECtHR, *Ladent v. Poland*, CE:ECHR:2008:0318JUD001103603, paras 45 and 46; *Medvedyev and Others v. France*, CE:ECHR:2010:0329JUD000339403, paras 76 and 77; and *El-Masri v. The former Yugoslav Republic of Macedonia*, CE:ECHR:2012:1213JUD003963009, para. 239.

EUCFR corresponds according to Article 52(3).[45] Pursuant to this, Articles 5 ECHR and 6 EUCFR protect 'personal security, in the sense of a guarantee of the right to physical freedom from arbitrary arrest or detention'[46] and, therefore, apply to 'deprivations of liberty by a public authority'.[47] The clarification of this matter is welcome as both the Commission[48] and the CJEU itself[49] had confusingly (and erroneously) alluded in the past to a free-standing 'right to security' that seems to differ from the Article 6 EUCFR right to liberty and security.[50]

The recognition that serious threats to national security allow for bulk data retention introduces an exception to the general rule confirmed in *Privacy International* and constitutes a clear victory for Member States. Can this signal the beginning of a slippery slope for bulk data retention? The answer seems to be negative as the CJEU laid down a number of conditions and safeguards subject to which mass, preventive data retention for serious national security threats is permitted. Such retention is allowed: (1) for a limited period of time which is strictly necessary and cannot exceed a foreseeable period[51]; (2) only if the Member State concerned is confronted with a 'serious threat' to national security which is shown to be 'genuine and present or foreseeable'[52]; (3) subject to limitations and strict safeguards that protect effectively the personal data of the persons concerned against the risk of abuse.[53] Finally, (4) the decisions giving an instruction to ECSPs to carry out such data retention should be subject to effective review, either by a court or by an independent administrative body (whose decision is binding) that should verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed.[54]

This means, according to the Court, that data retention 'cannot be systematic in nature'. However, some uncertainties remain. For instance, what would constitute 'foreseeable' (rather than present) threat; what would be the strictly necessary maximum retention period (days? weeks? months?) and could this potentially

---

45 *Quadrature du Net*, *supra* n. 2, paras 123–125.
46 Opinion of AG Campos Sánchez-Bordona, *supra* n. 19, para. 98.
47 *Quadrature du Net*, *supra* n. 2, para. 125.
48 *See* for instance Commission Staff Working Document on Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of noncash means of payment and replacing Council Framework Decision 2001/413/JHA, Brussels, 13 Sep. 2017
SWD(2017) 298 final, at 61.
49 *See Digital Rights Ireland*, *supra* n. 5, para. 42 and *Opinion 1/15*, *supra* n. 31, para. 149.
50 For criticism on this *see* Xavier Tracol, *The Two Judgments of the European Court of Justice in the Four Cases of* Privacy International, La Quadrature du Net and Others, French Data Network and Others *and* Ordre des Barreaux francophones et germanophone and Others*: The Grand Chamber Is Trying Hard to Square the Circle of Data Retention*, CLSR 11 (2021).
51 *Quadrature du Net*, *supra* n. 2, paras 137 & 138.
52 *Ibid.*, para. 137.
53 *Ibid.*, para. 138.
54 *Ibid.*, para. 139.

be renewed in perpetuity in light of an ongoing threat? A further interesting question concerns *access* to the data. Can bulk traffic data initially retained by ECSPs for serious national security threats be accessed by law enforcement authorities for other purposes (i.e., public security or combatting crime)? The Court does not appear to provide a clear answer to this, but other parts of the *Quadrature du Net* judgment might offer some guidance. For instance, in its discussion of the expedited retention of metadata for the purpose of combating serious crime, the CJEU notes that 'Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur'[55] and access to such data 'may, in principle, be justified only by the public interest objective *for which those providers were ordered to retain that data*'.[56] An argument can be made, therefore, that the same requirements should apply to data retained for serious national security purposes; access to these can only be justified for the same purposes under which they were retained. In any case, this is an issue that should be subject to review by the national court or the administrative body so that the approach followed in each Member State is at least transparent.

3.4[b] *'Serious' Crime and 'Serious' Threats to Public Security Allow for Targeted Data Retention*

Combating 'serious' crime and preventing 'serious' threats to public security is ranked at the second level of the hierarchy of objectives established by the Court. The CJEU acknowledged that positive obligations arise for Member States in this respect. These regard the protection of minors and other vulnerable persons when interpreting Articles 3, 4 and 7 EUCFR in light of the relevant jurisprudence of the ECtHR regarding the corresponding rights enshrined in Articles 3 and 8 ECHR.[57]

While indiscriminate, mass surveillance affecting all persons using electronic communications services 'without there being a link, at least an indirect one, between the data of the persons concerned and the objective pursued' is unacceptable,[58] the objectives of combating serious crime, preventing serious attacks on public security and, *a fortiori*, safeguarding national security can justify the 'particularly serious interference' entailed by the targeted retention of traffic and location data.[59] The Court defined targeted retention as 'limited' to what is

---

55 *Ibid.*, para. 164.
56 *Ibid.*, para. 166. Emphasis added.
57 *Ibid.*, paras 126 and 128. *See also* C 78/18 *Commission v. Hungary (Transparency of associations)*, EU:C:2020:476, para. 123.
58 *Quadrature du Net*, *supra* n. 2, paras 145 and 143.
59 *Ibid.*, para. 146.

strictly necessary with respect to: (1) the categories of data to be retained, (2) the means of communication affected, (3) the persons concerned[60] and, (4) the retention period[61] (although the CJEU accepted that this can be extended).[62] Targeted retention is also subject to a number of safeguards: (1) it should comply with the applicable substantive and procedural conditions, (2) effective safeguards against the risks of abuse for persons concerned should be in place, and, (3) the data should not be retained systematically and continuously.[63]

Yet, several questions arise regarding both the meaning of 'serious' attacks/risks to public security and the scope of the targeted retention. What would constitute a 'serious' risk to public security? Is a uniform definition of this possible across all the EU Member States? The scope of the targeted retention is also problematic. Persons can be targeted if they have 'been identified beforehand … on the basis of objective evidence',[64] but their link to serious crime or serious risk to public security can be 'indirect',[65] potentially broadening the range of individuals surveilled. The Court accepted that, besides the personal criterion, a geographical criterion can also be used. This would target communications in 'one or more geographical areas' based on 'objective and non-discriminatory factors', demonstrating the existence of 'a situation characterised by a high risk of preparation for or commission of serious criminal offences'.[66]

While the Court provided examples of such geographical areas relating to the commission of those offences (airports, stations, tollbooth areas),[67] its unreserved support for the geographical criterion[68] appears problematic. It ignores – in the year that followed the Black Lives Matter protests – the disproportionate burden of surveillance (and the risk of stigmatization) faced by vulnerable groups in society,[69] such as the poor,[70] the migrants[71] and ethnic minorities[72] that often reside in what

---

60 *Ibid*., paras 148 and 149.
61 *Ibid*., para. 147.
62 *Ibid*., para. 151.
63 *Ibid*., para. 142.
64 *Ibid*., para. 149.
65 *Ibid*., para. 148.
66 *Ibid*., para. 150.
67 It should be noted that all these places relate to the 'commission' rather than the 'preparation' of serious criminal activities.
68 A similar pronouncement was made in *Tele2*, *supra* n. 7, para. 108.
69 Maria Tzanou, *The Future of EU Data Privacy Law: Towards a More Egalitarian Data Privacy*, J. Int'l & Comp. L. 449 (2020). *See also* the 'postcode stereotypes' created from commercial marketing data sources of global data broker Experian's 'Mosaic' tool that is fed into the HART system. Big Brother Watch, *Home Affairs Select Committee: Policing for the Future Inquiry* (2018).
70 Report of the UN Special Rapporteur on extreme poverty and human rights, 11 Oct. 2019, A/74/493; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York, Crown Publishing Group 2016).
71 Valsamis Mitsilegas, *The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law* (Springer 2015).
72 *See* European Union Agency for Fundamental Rights (FRA), *Your Rights Matter: Police Stops, Fundamental Rights Survey* (2021).

can be called 'crime hotspots'.[73] Admittedly, the CJEU stressed the importance of non-discriminatory factors, but the practical consequences of such 'localized' forms of acceptable 'targeted' surveillance are most likely to be felt by the least privileged.[74] In particular, the focus on areas characterized by a high risk of *preparation* of serious criminal activities is very worrying. It reveals a dangerous lack of perception of the social inequalities that arise in the distribution of EU data privacy law outcomes.[75] To put it more bluntly, the relatively more privileged members of the society will be less likely to sustain targeted surveillance compared to the more marginalized ones.

3.4[c] *General and Indiscriminate Retention of IP Addresses and Civil Identities*

Another major concession that the CJEU made to Member States' law enforcement authorities in *Quadrature du Net* was to allow the bulk retention of IP addresses for the purposes of combatting serious crime, preventing serious threats to public security and safeguarding national security.[76] IP addresses are used to identify the natural person who owns the terminal equipment from which an Internet communication is made.[77] While IP addresses are traffic data, the Court accepted that they are less sensitive and could be treated differently from other types of traffic data because 'only the IP addresses of the source of the communication are retained' in email and Internet telephony and 'not the IP addresses of the recipient of the communication', therefore, those addresses do not, 'as such, disclose any information about third parties who were in contact with the person who made the communication'.[78]

Nevertheless, the retention of IP addresses constitutes a *serious interference* with the fundamental rights to privacy and data protection because it can be used to track Internet users' complete clickstream and, therefore, revealing their entire online activity and enabling a detailed profile of the user to be produced.[79] This serious interference is justified by the need to investigate online criminal activities and, more specifically, serious child pornography offences[80] under Directive 2011/93/EU.[81] The retention of IP addresses is subject to safeguards: (1) it cannot be

---

73 *See* Orla Lynskey, *Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing*, Int'l J.L. Context 162, 174 (2019).
74 Tzanou, *supra* n. 69, at 457.
75 *Ibid.*, at 454.
76 *Quadrature du Net*, *supra* n. 2, para. 156.
77 *Ibid.*, para. 152.
78 *Ibid.*
79 *Ibid.*, para. 153.
80 *Ibid.*, para. 154.
81 Directive 2011/93/EU of the European Parliament and of the Council of 13 Dec. 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ 2011, L 335, at 1.

undertaken for a period that exceeds what is strictly necessary in light of the objective pursued, and (2) substantive and procedural conditions regulating the use of that data must be put in place.[82]

The Court also permitted the indiscriminate retention of 'data relating to the civil identity of users of electronic communications systems' for the purposes of preventing and combatting criminal offences and safeguarding public security.[83] According to the CJEU, such data does not provide 'any information on the communications sent and, consequently, on the users' private lives' and, therefore, the interference entailed by the retention of such data cannot be classified as serious.[84]

The concession for indiscriminate retention of IP addresses links to the Court's acknowledgment that Member States have positive obligations to detect online child sexual abuse under Articles 3, 4 and 7 EUCFR deriving from the ECHR. However, it cannot be overstressed that this pronouncement coupled with the retention of the civil identity data of all users essentially signals the *end of anonymity online*: law enforcement authorities are now allowed access to virtually everyone's IP addresses and civil identity data.

It is, therefore, the repercussions of these at first glance 'more nuanced' data retention measures laid down in *Quadrature du Net* that need to be taken seriously rather than the red lines reiterated by the Court regarding bulk surveillance in *Privacy International*.

3.4[d] *Automated Analysis of Traffic and Location Data*

The Court also considered dealt in *Quadrature du Net* the automated analysis of metadata. It found that this presents a 'particularly serious' interference with Articles 7, 8 and 11 of the Charter because it applies to all persons using electronic communication systems and is likely to reveal the nature of the information consulted online.[85] Such interference can meet the requirement of proportionality only in situations in which a Member State is facing a genuine and present or foreseeable threat to national security including terrorism and the automated analysis is implemented for a strictly limited period.[86] Strict conditions are applicable to the automated analysis of metadata: (1) national laws must lay down the substantive and procedural conditions governing that use[87]; (2) the decision authorizing automated analysis must be subject to effective review that will verify that a genuine national security or

---

82 *Quadrature du Net*, *supra* n. 2, para. 156.
83 *Ibid.*, at 159.
84 *Ibid.*, para. 157. *See also Ministerio Fiscal*, *supra* n. 8, paras 59 and 60.
85 *Ibid.*, para. 174.
86 *Ibid.*, paras 177–178.
87 *Ibid.*, para. 176.

counter-terrorism threat exists and the conditions and safeguards that must be laid down are observed[88]; (3) the pre-established models and criteria on which automated analysis is based should be specific, reliable and non-discriminatory[89]; (4) any positive result obtained following automated processing must be subject to an individual re-examination by non-automated means before a measure adversely affecting the persons concerned is adopted[90]; (5) a regular re-examination should be undertaken to ensure that the pre-established models and criteria for the automated analysis and the databases used are reliable and up to date[91]; and, (6) the competent national authority is obliged to publish information of a general nature relating to automated analysis. However, the person must be notified individually 'if the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning him or her'.[92] That notification must, occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible.[93]

Quadrature du Net was the second case where the CJEU was asked to pronounce on the legality of automated decision-making in the context of counter-terrorism. In Opinion 1/15,[94] the Court assessed upon the Parliament's request the compatibility of the proposed agreement for the processing and transfer of PNR data[95] between the EU and Canada. In that case, the CJEU examined automated processing of PNR data used in Canada's border control pre-screening programme[96] and laid down several permissibility conditions. These conditions were reiterated and further clarified in *Quadrature du Net* in the context of telecommunications data retention. The CJEU's discussion in both cases is very

88 *Ibid*., para. 179.
89 *Ibid*., para. 180.
90 *Ibid*., para. 182.
91 *Ibid*.
92 *Ibid*., para. 191.
93 *Ibid*.
94 *Opinion 1/15*, *supra* n. 31, paras 173 and 174. For a commentary *see* inter alia Arianna Vedaschi, *European Court of Justice on the EU-Canada Passenger Name Record Agreement*, 14 Eur. Const. L. Rev. 410 (2018); Monika Zalnieriute, *Developing a European Standard for International Data Transfers After Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, 81(6) MLR 1046 (2018); Christopher Docksey, *Opinion 1/15: Privacy and Security, Finding the Balance*, 24(6) Maastricht J. Eur. & Comp. L. 768 (2017); Arianna Vedaschi, *Privacy and Data Protection Versus National Security in Transnational Flights: The EU–Canada PNR Agreement*, 8(2) Int'l Data Privacy L. 124 (2018).
95 PNR data is information provided by passengers when they book tickets and check-in for flights. For more information on the EU-US PNR saga *see* Yuko Suda, *Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism*, 51 J. Com. Mkt. Stud. 772 (2013); Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* 107 (Hart Publishing 2017); Maria Tzanou, *The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?*, 31(80) Utrecht J. Int'l & Eur. L. 87 (2015).
96 *Opinion 1/15*, *supra* n. 31, paras 168–174.

welcome as it sheds light on the principles governing automated decision-making for counter-terrorism purposes.

That being said, a number of observations are due here. First, the Court noted in *Quadrature du Net* that automated analysis carried out on the basis of models and criteria founded on sensitive data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information about a person's health or sex life would infringe Articles 7 and 8, read in conjunction with Article 21 EUCFR. Thus, such models and criteria used in order to prevent terrorism 'cannot be based on that sensitive data *in isolation*'.[97] This statement is confusing as it is not clear whether it introduces a prohibition of the use of sensitive data in automated decision-making for counter-terrorism purposes.[98] Does this mean that such automated analysis will be allowed for databases which combine sensitive with non-sensitive data? More importantly, the Court's discussion seems to miss out the fact that discriminatory effects may arise *indirectly* from inferences made from the intersection of multiple non-sensitive data and 'proxy attributes'.[99] The issue becomes even more complicated in the big data context where sensitive and non-sensitive data as well as personal and non-personal data can be combined and mixed at different time points.[100] Moreover, the exclusion of sensitive data as input variables has been criticized for contributing to loss of accuracy in the algorithm and for altering the model of the world that an Artificial Intelligence (AI) makes use of, instead of altering how that AI perceives and acts on bias.[101] It has also been argued that in order to avoid algorithmic discrimination it is necessary to use sensitive data in the process of building decision-making models,[102] although it is not clear whether this is applicable in the context of automated analysis for law enforcement purposes that are more rare but raise significantly more fundamental rights issues than automated analysis used in commercial settings.

This brings us to our second point. The automated analysis of metadata for counter-terrorism purposes raises further complexities because it involves a variety of different *actors* (public: law enforcement authorities/private: ECSPs) and sits in between two different *legal frameworks* (ePrivacy/GDPR and the Data Protection Law Enforcement Directive LED). For example, the French law requires that the

---

97 *Quadrature du Net*, *supra* n. 2, para. 181. Emphasis added.

98 The provisions of Art. 22(4) GDPR and 11(3) LED are worded differently.

99 'Proxy attributes' are data strongly correlated with protected characteristics, e.g., postcodes or certain geographical areas might indicate ethnic or racial origin. *See* Xavier Ferrer et al., *Bias and Discrimination in AI: A Cross-Disciplinary Perspective* 3 (2020), arXiv:2008.07309 [cs.CY].

100 Bart Van der Sloot, *Regulating Non-personal Data in the Age of Big Data*, in *Health Data Privacy Under the GDPR: Big Data Challenges and Regulatory Responses* 85 (Maria Tzanou ed., Abingdon, Routledge 2021).

101 Cynthia Dwork et al., *Fairness Through Awareness* 214 (2012), arXiv:1104.3913 [cs.CC].

102 Indrė Žliobaitė & Bart Custers, *Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models*, 24 Artificial Intelligence & L. 183 (2016).

automated screening of all traffic and location data is carried out by ECSPs at the request of the competent authorities[103] applying the parameters set by the latter.[104] While the involvement of the ECSPs brings the matter to the realm of the ePrivacy Directive and, therefore, relates to processing for commercial purposes (GDPR), there are still questions about the issue of the applicable legal framework.[105] This is because there are discrepancies in the relevant safeguards applicable to automated decision-making between the GDPR and the LED.[106] More particularly, Article 22 (3) GDPR provides that in the cases that the prohibition of automated decision-making does not apply,[107] the data subject should have (1) at least the right to obtain human intervention on the part of the controller, (2) to express his or her point of view and (3) to contest the decision. However, Article 11 of the Law Enforcement Directive merely requires that in case the automated processing is permitted (by EU or Member State law), the data subject should be provided 'at least the right to obtain human intervention on the part of the controller' but there is no further mention of the other safeguards included in the GDPR.[108] These discrepancies, such as for instance the absence of a right to contest an automated decision from the LED have been criticized as 'both curious and worrying',[109] but in the context of public-private partnerships for counter-terrorism surveillance they are particularly problematic because they can create further uncertainties when different actors and activities are mixed, rendering it difficult to identify in practice the applicable framework.

It could be argued that the GDPR with its more protective rules should be applicable here, although in *Quadrature du Net* the Court seems to assume quasi-legislative powers to establish a new regime regarding the automated processing of metadata that falls within Article 15 (1) of the ePrivacy Directive. In particular, the

---

[103] Competent authority is defined in Art. 3(7)(a) and (b) LED. *See also* Krzysztof Garstka, *Between Security and Data Protection: Searching for a Model Big Data Surveillance Scheme Within the European Union Data Protection Framework* (2018), https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2018/11/Garstka-Between-Security-and-Data-Projection-November-2018.pdf (accessed 12 Jul. 2021).

[104] Article L. 851 3 of the CSI. *Quadrature du Net*, *supra* n. 2, para. 172.

[105] *See* Lynskey, *supra* n. 73, at 163.

[106] Article 22 GDPR is framed as a right of the data subject, while Art. 11 LED is framed as a prohibition of automated processing. *See* Margot Kaminski, *The Right to Explanation, Explained* (2018), https://ssrn.com/abstract=3196985 (accessed 12 Jul. 2021); Isak Mendoza & Lee Bygrave, *The Right Not to Be Subject to Automated Decisions Based on Profiling*, University of Oslo Faculty of Law Research Paper No. 2017-20 (8 May 2017), https://ssrn.com/abstract=2964855 (accessed 12 Jul. 2021).

[107] The prohibition does not apply according to Art. 22 (2) GDPR if the decision: (1) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (2) is authorized by Union or Member State law; or (3) is based on the data subject's explicit consent.

[108] Such safeguards could be granted at the discretion of the Member States. *See also* Recital 38 LED.

[109] Maja Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, Int'l J.L. & Info. Tech. 91, 109 (2019).

Court laid down a rule of 'individual re-examination' of automated decisions, an *ex-post* obligation for a regular re-examination of the variables and the algorithms in the context of counter terrorism and national security[110] as well as certain transparency conditions that require the publication of information about automated decision-making. These pronouncements go beyond the relevant provisions of the GDPR and the LED. Both these instruments include a qualified prohibition of automated decision-making, however, the requirement for an 'individual re-examination' of the automated assessment of metadata processing for counter-terrorism purposes before a measure adversely affecting the persons concerned is adopted seems to be absolute, with no exceptions recognized by the Court. Moreover, the requirement for an *ex-post* algorithmic auditing in *Quadrature du Net* goes beyond any potential *ex-ante* examination of the algorithm through processes such as Data Protection Impact Assessments (DPIAs) under the GDPR.[111] This is welcome, but further clarification is needed as to how to open the 'black box' or whether an algorithmic 'black box' should exist at all in this context.[112]

Third, while the Court recognized the consequences of automated decisions at the individual level, it failed to pay due attention to the collective harms that these may incur on certain groups that have to sustain the – often uneven – burden of such measures. Automated screening of metadata can be used for both the identification of suspects and to make systemic predictive decisions to discover 'unknown unknowns',[113] by identifying linkages, patterns, associations or behaviours which might demonstrate a serious terrorist threat.[114] The 'data injustices' of such systemic predictive decisions are likely to arise on the collective as much as

---

110 *Quadrature du Net*, *supra* n. 2, para. 182. *See also Opinion 1/15*, *supra* n. 31, paras 173–174.

111 Article 35 GDPR. *See* Bryce Goodman, *Discrimination, Data Sanitisation and Auditing in the European Union's General Data Protection Regulation*, 2(4) EDPLR 493 (2016).

112 *See* inter alia Fundamental Rights Agency (FRA), *Big Data: Discrimination in Data-Supported Decision Making* (2018), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf (accessed 12 Jul. 2021); Tal Zarsky, *The Trouble With Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making*, 41 Sci. Tech. & Hum. Values 118 (2016); Frederik Zuiderveen Borgesius, *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making*, Council of Europe, Directorate General of Democracy (2018), https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73 (accessed 12 Jul. 2021); Jennifer Cobbe & Jatinder Singh, *Reviewable Automated Decision Making*, 39 Computer L. & Sec. Rev. 1 (2020); Ada Lovelace Institute, *Examining the Black-Box: Tools for Assessing Algorithmic Systems* (29 Apr. 2020), https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/ (accessed 12 Jul. 2021); Stefano Civitarese Matteucci, *Public Administration Algorithm Decision-Making and the Rule of Law*, Eur. Pub. L. 103 (2021).

113 *See* ECtHR (Grand Chamber), *Big Brother Watch and others v. United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, para. 422.

114 *See* Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework* (2015), para. 18; Rosamunde van Brakel, *Pre-emptive Big Data Surveillance and Its (dis) empowering Consequences: The Case of Predictive Policing*, in *Exploring the Boundaries of Big Data* 117 (Bart van der Sloot et al. eds, Amsterdam University Press 2016).

the individual level.[115] Admittedly, data protection and privacy are framed as individual rights focusing on addressing harms and providing redress at the individual level, but the CJEU's analysis should no longer miss out on the broader problems regarding predictive automated analysis that might lead to deficits of substantive justice.[116] The CJEU's jurisprudence on data privacy rights has reached a level of maturity that requires now a much more proactive approach from the Court that looks beyond the individual level and is attentive to and strives to deal with data inequalities in order to pursue a more 'egalitarian data protection'[117] and achieve 'data justice'.[118]

Finally, the biggest issue with automated decision-making (and with other forms of data retention and analysis) for law enforcement purposes is whether these technological systems are needed at all[119] for counter-terrorism purposes.-[120] This overarching and pressing issue of necessity goes beyond the 'necessary' requirement of the proportionality criterion that led the Grand Chamber to conclude that such automated processing can be justified only for national security purposes. It essentially asks whether such systems are required in the first place – or whether they should be banned at the outset – and whether the need to have them goes beyond their mere usefulness.[121] There is no discussion of this matter in *Quadrature du Net*, although it is up to the national law enforcement authorities (and not the Court) to provide robust empirical evidence that demonstrates this need.

4 BULK SURVEILLANCE AND THE TWO COURTS: DIVERGENCE OR CONVERGENCE?

On 25 May 2021, the Grand Chamber of the ECtHR delivered its much-awaited judgments in two cases concerning bulk communications surveillance: *Big Brother Watch and Others v. the UK* and *Centrum för rättvisa v. Sweden*.[122] In *Big Brother*

---

115 Linnet Taylor, *What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally*, Big Data & Soc'y 1, 8 (2017).

116 Daniela Caruso & Fernanda Nicola, *Legal Scholarship and External Critique in EU Law*, in *The Transformation or Reconstitution of Europe: The Critical Legal Studies Perspective on the Role of the Courts in the European Union* 221, 230 (Tamara Perišin & Siniša Rodin eds, Hart Publishing, 2018).

117 Tzanou, *supra* n. 69.

118 Taylor, *supra* n. 115.

119 Julia Powles & Helen Nissenbaum, *The Seductive Diversion of 'Solving' Bias in Artificial Intelligence*, The Medium (7 Dec. 2018), https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53 (accessed 12 Jul. 2021).

120 Bruce Schneier, *Data Mining for Terrorists*, *Schneier on Security Blog* 9.3 (2006), https://www.schneier.com/blog/archives/2006/03/data_mining_for.html (accessed 12 Jul. 2021).

121 Opinion of Judge Pinto De Albuquerque in ECtHR (Grand Chamber), *Big Brother Watch and others v. UK*, *supra* n. 113, para. 58.

122 ECtHR (Grand Chamber), *Centrum för rättvisa v. Sweden*, Application no. 35252/08 of 25 May 2021.

Watch, the ECtHR found that the UK's bulk interception and acquisition of communications metadata regimes under the Regulation of Investigatory Powers Act (RIPA) violated Articles 8 and 10 ECHR. Both decisions raise several important issues, but for the purposes of this article, the discussion focuses on the points relevant to the present analysis.

At first glance, there seem to be a few stark differences in the approach of the two Courts regarding bulk surveillance. First, while the CJEU in *Privacy International* maintained in principle a *per se* incompatibility of bulk data retention with fundamental rights (even if such retention is undertaken for national security purposes), the ECtHR's starting point of the analysis was that bulk interception regimes are 'a valuable technological capacity to identify new threats in the digital domain'.[123] Second, the Strasbourg Court introduced a peculiar test that views bulk interception 'as a gradual process in which the degree of interference with individuals' Article 8 ECHR rights increases as the process progresses'[124] considering that there are different stages of the bulk interception process, such as (1) the interception and initial retention of communications; (2) the application of specific selectors to the retained communications data; (3) the examination of selected communications and metadata; and (4) the subsequent retention of data and use of the 'final product', including the sharing of data with third parties. By contrast, the CJEU views each of these types of processing as different, separate interferences with fundamental rights. Third, the ECtHR has not introduced any red lines regarding the generalized access to the content of communications data, which the Luxembourg Court considers a breach of the essence of the right to privacy.[125] Fourth, the ECtHR held that it is appropriate to address 'jointly the "in accordance with the law" and "necessity" requirements' when it examines legislation permitting secret surveillance.[126] The Luxembourg Court tends to address these requirements separately even if secret surveillance is at stake, although there have been cases of secret surveillance measures where the CJEU failed to discuss sufficiently the 'provided for by law' requirement.[127]

The above points signal a divergence between the two Courts regarding bulk surveillance. Nevertheless, a more careful reading of *Quadrature du Net* and *Big Brother Watch* reveals that the CJEU and the ECtHR and are not really walking in different directions. This is evidenced by several reasons. Both Courts have opted for a more nuanced approach to bulk surveillance, which is prescribed by several procedural guarantees regarding authorization, retention,

---

123 *Big Brother Watch*, *supra* n. 113, para. 323.
124 *Ibid.*, para. 325.
125 *Digital Rights Ireland*, *supra* n. 5, para. 58, *Schrems II*, *supra* n. 39, para. 94.
126 *Ibid.*, para. 334.
127 *See* Tzanou, *supra* n. 9, at 556.

access and oversight. Such guarantees, conditions and safeguards demonstrate a trend towards a 're-modulation' of the prohibition of bulk surveillance,[128] with the adoption of a more proceduralized approach. Moreover, the CJEU laid down in *Quadrature du Net* various permissible types of bulk surveillance with significant repercussions.

These signs of convergence between the two Courts might be good news for the Member States and the UK government after Brexit as they present relatively 'easy fixes'[129] to the inherent problems of bulk data retention. However, they also 'fundamentally alter the existing balance in Europe between the right to respect for private life and public security interests'[130] by progressively re-legitimising bulk data retention on the condition that certain safeguards are applicable. In this respect, it is hard to agree with the argument that 'the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe'.[131] Instead, it seems that the two Courts are converging[132] rather than diverging in their recent jurisprudence concerning the data retention saga.

5 AN (IN)ADEQUATE REGIME AFTER BREXIT?

On 19 February 2021 the Commission launched the process for an adequacy finding by issuing two draft adequacy decisions for the transfer of personal data to the UK, under the GDPR[133] and the LED.[134] The European Data Protection Board

---

128 Celeste, *supra* n. 4, at 136.

129 Marko Milanovic, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa* (26 May 2021), EJIL!Talk, https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ (accessed 12 Jul. 2021); Juraj Sajfert, *The Big Brother Watch and Centrum för Rättvisa Judgments of the Grand Chamber of the European Court of Human Rights – The Altamont of Privacy?*, European Law Blog (8 Jun. 2021), https://europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy/ (accessed 12 Jul. 2021).

130 Judge Pinto De Albuquerque, *supra* n. 121, para. 59.

131 *Ibid*.

132 Monika Zalnieriute, *The Future of Data Retention Regimes and National Security in the EU After the Quadrature Du Net and Privacy International Judgments*, ASIL Insights (5 Nov. 2020), https://www.asil.org/insights/volume/24/issue/28/future-data-retention-regimes-and-national-security-eu-after-quadrature#_ednref17 (accessed 12 Jul. 2021).

133 European Commission, *Draft Decision on the Adequate Protection of Personal Data by the United Kingdom – General Data Protection Regulation* (19 Feb. 2021), https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf (accessed 12 Jul. 2021).

134 European Commission, *Draft Decision on the Adequate Protection of Personal Data by the United Kingdom: Law Enforcement Directive* (19 Feb. 2021), https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf (accessed 12 Jul. 2021).

(EDPB),[135] the European Parliament[136] (as well as academics[137] and privacy professionals[138]) expressed concerns regarding the adequacy of the UK's data protection legal framework, focusing inter alia on the access of UK law enforcement and intelligence authorities to data transferred from the EU. More particularly, in a very critical Opinion, the Parliament considered that the Commission's draft adequacy decisions 'fail to take into account the lack of limitations on the use of UK bulk data powers, or the actual use of UK-US surveillance operations'.[139] In this regard, it voiced a number of concerns regarding: the lack of an effective substantive oversight by the Information Commissioner's Office (ICO) or the courts over the use of the national security exemption in UK data protection law; the fact that limitations on the use of UK bulk surveillance powers are not set out in the law itself as required by the CJEU, but are rather left to the discretion of the executive; the lack of meaningful protection of metadata against undue access, bulk collection and AI-based analysis by the UK intelligence agencies; and, the sharing of data among the Five Eyes agencies, in particular the GCHQ and the National Security Agency (NSA).[140]

Nevertheless, on 28 June 2021, the Commission adopted the two adequacy decisions[141] confirming that the UK ensures a level of protection for personal data transferred from the EU that is 'essentially equivalent' to the one guaranteed by EU data protection law.[142] The Commission retains the power to suspend or terminate the adequacy findings and its assessment is time-limited: both adequacy decisions

---

135 EDPB, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, 13 Apr. 2021, paras 9 subseq and Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom, 13 Apr. 2021.

136 European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)), P9_TA(2021)0262.

137 *See* inter alia Douwe Korff & Ian Brown, *The Inadequacy of UK Data Protection Law: Executive Summary*, Data protection and digital competition blog, 4 (30 Nov. 2020), https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf (accessed 12 Jul. 2021); Oliver Patel & Nathan Lea, *EU-UK Data Flows, Brexit and No Deal: Adequacy or Disarray?*, UCL European Institute (Aug. 2019), https://www.ucl.ac.uk/european-institute/sites/european-institute/files/eu-uk_data_flows_brexit_and_no_deal_updated.pdf (accessed 12 Jul. 2021).

138 *See* Georgina Kon & Richard Cumbley, *EU: Data Flows Post-Brexit – Choppy Waters Ahead?*, Linklaters (2 Nov. 2020), https://www.linklaters.com/en/insights/blogs/digilinks/2020/november/eu—data-flows-post-brexit—choppy-waters-ahead (accessed 12 Jul. 2021).

139 Parliament resolution, *supra* n. 136, para. 16.

140 *Ibid.*

141 European Commission, Commission Implementing Decision of 28 Jun. 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4800 final and Commission Implementing Decision of 28 Jun. 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801 final.

142 *Ibid.*, Art. 1.

contain an 'unprecedented'[143] 'sunset clause', which limits the duration of adequacy to four years.[144]

However, the UK's bulk interception and metadata retention regimes continue to present significant concerns for the EU institutions and the Commission undertakes in its adequacy findings to monitor these regularly.[145] The Commission's adequacy decision under the GDPR also mentions several times *Privacy International*. However, as the Commission recognizes, the current UK legal framework, the Investigatory Powers Act 2016 (IPA) replaces the legislation concerning the acquisition of bulk communications data which was the subject of this judgment (the RIPA 2000). According to the Commission, the new regime provides for specific conditions and safeguards under which bulk interception and retention measures can be authorized.[146] The most important of these safeguards is the so-called 'double-lock procedure', which requires that for both national security and law enforcement purposes the decisions of the Secretary of State to issue interception and retention notices must be approved by an independent Judicial Commissioner, who must review in particular whether the notice to retain relevant communications data is necessary and proportionate for one or more of the statutory purposes.[147]

Nevertheless, despite the adequacy finding of the new UK surveillance regime, it is unlikely that the tensions between the EU and the UK regarding government access to personal data have been resolved. A closer look at the adequacy decision under the GDPR shows that the Commission failed to pay due attention to the red lines established by the CJEU in its data retention jurisprudence. A first issue concerns the 'bulk interception' carried out by UK intelligence services.[148] This refers to 'the interception of communications in the course of their transmission sent or received by individuals who are outside the British Islands' and includes both the content of communications as well as metadata. This bulk interception might capture EU originating data, which are considered 'overseas-related communications'.[149] However, the CJEU has held that access to the content of communications breaches the essence of the right to privacy. This pronouncement of the Court that sets out an absolute rule seems to

---

143 European Parliamentary Research Service (EPRS), *EU-UK Private-Sector Data Flows After Brexit: Settling on Adequacy* (Apr. 2021), https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690536/EPRS_IDA(2021)690536_EN.pdf (accessed 12 Jul. 2021).

144 Both decisions will expire on 27 Jun. 2025.

145 UK adequacy decision-GDPR, Recital 281.

146 *Ibid.*, Recital 233.

147 Adequacy decision-GDPR, Recital 209. *See also* UN Special Rapporteur on the Right to Privacy, Joseph Cannataci, *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion of His Mission to the UK and Northern Ireland* (29 Jun. 2018), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E (accessed 12 Jul. 2021).

148 Section 136 of the IPA 2016.

149 *Ibid.*

be ignored by the Commission, which merely goes on to describe in the adequacy finding the different safeguards applicable to bulk interception.[150]

Second, the Commission notes that the 'bulk acquisition of metadata'[151] covers data that is collected by telecommunication operators in the United Kingdom directly from the users of a telecommunication service, and, therefore 'this type of "customer facing" processing typically does not involve … a transfer from a controller/processor in the EU to a controller/processor in the United Kingdom'.[152] While this might be the case, as mentioned above, EU originating metadata can be captured under 'bulk interception' of overseas-related communications. More importantly, the Commission seems to forget here about the prohibition of bulk metadata retention for intelligence purposes laid down in *Privacy International*.[153] Admittedly, now that the UK has left the EU, the CJEU's bite is – unsurprisingly – less powerful, as the UK is only subject to the ECHR for the judicial oversight of its surveillance regime However, it is unclear how the Commission will justify going around the red lines set out by the Court, including in cases concerning third-countries' surveillance as shown in *Schrems I* and *Schrems II*.

In this regard, the assurances made in the adequacy decision that the UK's 'bulk powers' understood as 'the collection and retention of large quantities of data acquired by the Government through various means and which can subsequently be accessed by the authorities' are somehow different to 'mass surveillance' because they incorporate 'limitations and safeguards designed to ensure that access to data is not given on an indiscriminate or unjustified basis'[154] is of little consolation if the CJEU's data retention prohibitory rules are ignored.[155] Such red lines are not going to magically disappear because procedures and limitations exist, so challenges to the Commission's adequacy decisions might be expected in the future.

6 FURTHER COMPLICATIONS AHEAD: THE DRAFT EPRIVACY REGULATION

On 10 February 2021, the Council of the EU agreed its position on the draft ePrivacy Regulation.[156] The proposed legal instrument states that the Regulation

---

150 *See* Adequacy decision-GDPR, Bulk interception and bulk equipment interference, Recitals 218 and subseq.
151 Chapter 2 of Part 6 of the IPA 2016.
152 Adequacy decision-GDPR, Recital 231.
153 *See* Parliament resolution, *supra* n. 136, para. 27.
154 Adequacy decision-GDPR, Recital 216.
155 *See also* EDPB, *Adequacy Referential*, WP 254 rev. 01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 (accessed 12 Jul. 2021).
156 ePrivacy Regulation proposal, *supra* n. 10.

will not apply to the protection of fundamental rights or freedoms related to activities that fall outside the scope of Union Law, 'and in any event measures, processing activities or operations concerning national security and defense, *regardless of who is carrying out these operations, whether it is a public authority or a private operator*'.[157] Moreover, Article 7 (4) of the draft ePrivacy Regulation provides that:

> Union or Member state law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as the safeguarding against and the prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists.

It is noteworthy that both provisions depart considerably from the Council's proposal under the German Presidency,[158] which held that Article 11 of the draft ePrivacy Regulation (Article 15 of the ePrivacy Directive) enabled the EU and its Member States to regulate data retention in conformity with EU law without the need for additional provisions in light of the judgments in *Privacy International* and *Quadrature du Net*.

Nevertheless, both the proposed provisions of the agreed draft – if finally adopted – raise considerable concerns as to their compatibility with the CJEU's case-law. As the EDPB noted, the exclusion of processing activities from the scope of the Regulation may challenge the consistency of the EU data protection legal framework and be incompatible with Articles 7, 8, 11 and 52 EUCFR as interpreted by the Court.[159] According to the EDPB:

> providing a legal basis for anything else other than targeted retention for the purposes of law enforcement and safeguarding national security is not allowed under the Charter, and would anyhow need to be subject to strict temporal and material limitations as well as review by a Court or by an independent authority.[160]

Besides the significant fundamental rights concerns, circumventing – or indeed abolishing – the CJEU's jurisprudence on data retention in the ePrivacy Regulation would also set a dangerous precedent for the Court's assessment of third countries metadata retention laws and practices, such as the US, in light of

---

[157] Article 2 (2) (a) and recital 7a Draft ePrivacy Regulation. Emphasis added.

[158] Presidency compromise text on the proposal for the ePrivacy Regulation, 9931/20 as of 4 Nov. 2020, https://data.consilium.europa.eu/doc/document/ST-9931-2020-INIT/en/pdf (accessed 12 Jul. 2021). *See also* Christina Etteldorf, *A New Wind in the Sails of the EU ePrivacy-Regulation or Hot Air Only? On an Updated Input from the Council of the EU Under German Presidency*, 4 Eur. Data Prot. L. Rev. 570 (2020).

[159] EDPB, *Statement 3/2021 on the ePrivacy Regulation* (9 Mar. 2021).

[160] *Ibid*.

Schrems I and *Schrems II*. Double standards in this regard risk rendering the CJEU's case law meaningless and cannot be accepted.

Finally, the margin of discretion given to the Member States under Article 7 (4) of the draft ePrivacy Regulation is extremely large and could prove disruptive for the purposes of consistency[161] that is considered the 'name of the game'[162] of the EU data protection regime. Ensuring consistency for natural and legal persons, economic operators, controllers, processors, and supervisory authorities is a huge task given that the ePrivacy Regulation aims to regulate communications' technologies that allow the tracking of end-users' online behaviour, such as the so-called over-the-top (OTT) services. With the massive uptake in the use of applications such as Skype, WhatsApp, Facebook Messenger and Viber for sending messages or making audio calls, these OTT services will now fall within the scope of the Regulation and will need to comply with its requirements on data protection, privacy and security.[163] Following the invalidation by the CJEU of the Data Retention Directive which attempted to harmonize mandatory data retention in the EU, Article 15(1) of the ePrivacy Directive has provided the legal basis for data retention for law enforcement purposes. In this context, MS either maintained, repealed or amended their national laws.[164] However, there is no EU or national legal framework imposing a general data-retention obligation on OTTs for law enforcement purposes[165] and this is likely to raise uncertainties. The introduction of 5G will also bring about new challenges, as its service-based architecture will make it harder for ECSPs to collect certain types of data that are currently retained, such as international mobile subscriber identity (IMSI) numbers. All the more, the cross-border provision of communication services is expected to further increase with the implementation of 5G-enabled Internet of Things (IoT) applications.[166]

7 CONCLUSION

Privacy International and *Quadrature du Net* undoubtedly constitute landmark constitutional decisions that signify the judicial protection of fundamental rights in the context of national security and counterterrorism. While the two judgments

---

[161] *See* Recital 6 draft ePrivacy Regulation.
[162] Opinion of AG Bobek in Case C – 645/19 *Facebook Ireland and Others*, 13 Jan. 2021 para. 76.
[163] Handbook on European data protection law | European Union Agency for Fundamental Rights, https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed 12 Jul. 2021), at 34.
[164] Study on the retention of electronic communications non-content data for law enforcement purposes final report (EU 2020).
[165] *Ibid*.
[166] *Ibid*.

should be read together, they are also distinct. *Privacy International* continues the established peremptory rejection by the Court of mass, indiscriminate data retention even if this is undertaken for national security purposes. *Quadrature du Net* marks the beginning of a more nuanced approach to surveillance that opens the door for even bulk data retention measures when these are required for counter-terrorism purposes.

This re-evaluation of data retention models seems to be based on what this article referred to as the 'proceduralisation of surveillance'. Instead of red lines and prohibitive rules, data retention measures are now gradually permitted on the basis of a set of procedures, criteria, and safeguards under which they should operate. This is a significant departure from previous case-law that signals a progressive re-alignment of the CJEU with the ECtHR, especially following the latter's recent *Big Brother Watch* judgment.

Overall, in *Quadrature du Net*, the CJEU attempted to find a compromise between intelligence services' requirements and fundamental rights. It is, therefore, little surprising that the judgment has angered both Member States and privacy advocates and the legislature is considering taking the matter of the scope of application of EU law in its own hands. The future will show whether *Quadrature du Net* 'opened the gates for an electronic "Big Brother" in Europe'[167] or led the way towards a less-absolute, more pragmatic (and perhaps less naïve) approach to surveillance. What is for sure is that the EU data retention saga is not over yet.

[167] *Ibid.*, para. 60.