A STRUGGLE FOR COMPETENCE: NATIONAL SECURITY, SURVEILLANCE AND THE SCOPE OF EU LAW AT THE COURT OF JUSTICE OF EUROPEAN UNION

MONIKA ZALNIERIUTE

Forthcoming (2022) 85(1) Modern Law Review
[2021] *UNSWLRS* 34

UNSW Law
UNSW Sydney NSW 2052 Australia

Modern Law Review, Vol 85(1) 2022 *forthcoming*

A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union

Monika Zalnieriute*

In *Privacy International* and *Quadrature Du Net,* the Grand Chamber of the Court of Justice of the European Union ('CJEU') ruled that the e-Privacy Directive and EU Charter on Fundamental Rights generally prevent national law from enabling bulk retention and transmission of traffic and location data. However, in *Quadrature Du Net*, the Court clarified that EU law does not preclude indiscriminate data *retention* measures when Member States can prove serious threats to national security. In such cases, bulk data can only be retained during a strictly necessary period and the decision must be subject to review by a court or independent administrative body. The judgments will have serious implications for other data retention and sharing arrangements, such as the PNR, the proposed e-Privacy Regulation and e-Evidence package, international data sharing agreements, and also the third countries seeking adequacy decisions under the GDPR, including post-Brexit UK. The rulings suggest that CJEU has become an important actor in national security landscape, which has been outside the scope of European integration, but has become a ground for political struggle between the EU institutions and Member States. Yet, while *Privacy International* is an unequivocal assertion of CJEU's authority in the area of national security and a victory for data protection, *Quadrature Du Net* does not oppose indiscriminate data retention in principle and is an ambivalent response by the CJEU in the face of political pressure.

* Senior Lecturer and Australian Research Council DECRA Fellow at Faculty of Law and Justice, UNSW Sydney; Lead of 'AI and Law' Research Stream at Allens Hub for Technology, Law & Innovation, UNSW Sydney, Australia, m.zalnieriute@unsw.edu.au. This research has been funded by Australian Research Council Discovery Early Career Research Award (project number DE210101183). I would like to thank anonymous reviewers for constructive feedback and Emily Hunyor for her research assistance.

INTRODUCTION

Balancing the protection of fundamental rights and national security has been one of the greatest challenges for contemporary liberal democracies. That challenge has never been more important than today: the outbreak of global COVID-19 pandemic required governments and citizens to reconsider what 'national security' is, and has triggered an increasing demand for private companies to share data with governments for protecting public health during the times of global health crisis and public emergency.

In this context, on October 6, 2020, the Grand Chamber of the CJEU delivered two long-awaited judgments on surveillance, national security and fundamental rights in Case C-623/17 *Privacy International* ('*Privacy International*'),[1] and Joined Cases C-511/18 *La Quadrature Du Net and Others*, C-512/18 *French Data Network and Others,* and C-520/18 *Ordre des Barreaux Francophones et Germanophone and Others* (one judgment, hereinafter '*Quadrature Du Net*').[2] In both judgments, the Court ruled that the EU Privacy and Electronic Communications Directive (2002/58) ('e-Privacy Directive')[3] and the EUCFR generally prevent national law from enabling indiscriminate *retention* or *transmission* of traffic and location data, even if it is for safeguarding national security. However, in *Quadrature Du Net*, the Court explained that EU law does not preclude indiscriminate data *retention* measures if Member States can prove legitimate and 'serious threats to national security'.[4] In such cases, bulk data can be retained during a strictly necessary period and the decision must be subject to review by a court or independent administrative body.[5]

Privacy International and *Quadrature du Net* have significant implications for the future of data retention and sharing regimes, like Passenger Name Records ('PNR'), the proposed e-Privacy Regulation, e-Evidence package, international data sharing agreements, and also the third countries seeking adequacy

[1] *Case C-623/17 Privacy International* [2020] ECLI:EU:C:2020:790.
[2] *Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others* [2020] ECLI:EU:C:2020:791.
[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 (OJ L 201/37).
[4] *Quadrature Du Net* (n 3) paras 136–139, 168.
[5] ibid 168.

decisions under General Data Protection Regulation (GDPR),[6] including post-Brexit UK. These rulings suggest that the CJEU has become an important actor in the national security landscape, which has traditionally been outside the scope of the European integration but has increasingly become a ground for political struggle between the EU institutions and Member States. Yet, while *Privacy International* is an unequivocal assertion of CJEU authority in the area of national security, *Quadrature Du Net* does not oppose indiscriminate data retention in principle and is an ambivalent response by the CJEU in the face of political pressure.

The first part of this note provides the background to the legal challenges brought in *Privacy International* and *Quadrature Du Net* cases. Part II outlines the three Opinions of the Advocate General, while Part III focuses on the CJEU's two rulings and their reasoning. Part IV focuses on the relationship between national security, surveillance regimes and the scope of EU law. Part V looks at the future of data retention and sharing regimes in EU and beyond.

FACTUAL AND LEGAL BACKGROUND

Data retention regimes date back to the post-9/11 era, when many countries adopted new legislative measures granting novel powers to law enforcement agencies in the fight against the 'war on terror'.[7]

---

[6] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC 2016 1.

[7] See, e.g., 'United Nations Security Council Resolution 1373 (2001)' (*Security Council of Counter-errorism Committee*) <https://www.un.org/sc/ctc/resources/databases/recommended-international-practices-codes-and-standards/united-nations-security-council-resolution-1373-2001/> accessed 12 August 2020; 'The EU Council Counter-Terrorism Strategy of 2005 ("Prevent, Protect, Pursue, Respond")' (*European Council Council of the European Union*) <http://www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy/> accessed 12 August 2020; 'The European Council Stockholm Programme - an Open and Secure Europe Serving and Protecting the Citizens 2010-2014 (OJ 2010/C 115/01)' [2010] Official Journal of the European Union <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF> accessed 12 August 2020; 'Communication of the EU Commission on "An Area of Freedom, Security and Justice."' (2009) COM (2009)262 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:en:PDF>

Numerous governments obliged private companies in telecommunications, transport, financial and other sectors to retain metadata and personal information and make it available to security authorities through national, regional and international agreements, such as PNR,[8] or Terrorist Finance Tracking Programme ('SWIFT').[9] Often, such data was not the content of the communications, but rather 'data about the data', also known as metadata: the location, date, time, duration and form of communications and web browsing activity and other details, which can be used to create a digital picture of individuals' movements, contacts, interests and associations.[10]

While security agencies in some EU Member States, such as in the UK and Ireland, started collecting and intercepting the international e-mail traffic data from Google and Yahoo without a court order,[11] many Member States did not have any data retention mechanism, which was seen as an obstacle in joint EU efforts in the fight against terrorism. Following the terrorist attacks in Madrid in 2004 and London bombings in 2005, the EU adopted the EU

accessed 12 August 2020; Generally, see 'Report of the UN Special Rapporteur on The Promotion and Protection of HR and Fundamental Freedoms While Countering Terrorism' (2009) A/HRC/13/37 and; Claudia Hillebrand, *Counter-Terrorism Networks in the European Union: Maintaining Democratic Legitimacy after 9/11* (OUP Oxford 2012).

[8] See, e.g., Agreement between the United States of America and the European Union of 2012 on the use and transfer of passenger name records to the United States Department of Homeland Security 2012 (OJ L 215); 2007 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (OJ L 204) 18; 2004 Agreement between the European Community and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (OJ L 183).

[9] Agreement between the European Union and The United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program 2010 (L 8/11).

[10] Genna Churches and Monika Zalnieriute, 'A Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA – AUSPUBLAW' (*AUSPUBLAW*, 26 February 2020) <https://auspublaw.org/2020/02/a-window-for-change-why-the-australian-metadata-retention-scheme-lags-behind-the-eu-and-usa/> accessed 19 November 2020.

[11] Joel R Reidenberg, 'The Data Surveillance State in the US and Europe' [2013] Wake Forest Law Review 583, 592; Reidenberg claims that such warrantless wiretapping in the EU was much more prevalent than in the US, see ibid 594.

Directive 2006/24/EC ('Data Retention Directive')[12] which required communications service providers to store traffic and location data for a period between 6 months and 2 years, and maintain a surveillance database for law enforcement purposes.

In 2014, in *Digital Rights Ireland*,[13] the CJEU invalidated the Data Retention Directive for its disproportionate interference with Articles 7 and 8 EUCFR, guaranteeing the rights to private life and data protection respectively. Similarly, national Courts of Member States have scrutinized domestic legislation implementing EU data retention regimes in the Czech Republic, Romania, and Germany, finding them incompatible with the fundamental rights of the citizens in those countries.[14]

Data retention regimes, imposing obligations on electronic communications service providers, also intersect with the e-Privacy Directive, which stipulates that telecommunications providers must erase or anonymise data after communication transmission or billing.[15] However, Article 15(1) of the e-Privacy Directive further allows data retention for a 'limited period' provided it is 'in accordance with the general principles' of EU law and 'necessary, appropriate and proportionate' to the purposes of safeguarding 'national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system'.[16]

In 2016, in *Tele2 Sverige*, the CJEU ruled that data retention for the purposes of combatting serious crime fell under the scope of the

[12] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC 2006 (OJ 2006, L105/54).

[13] *Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General* [2014] ECR -238.

[14] See *The Czech Republic Constitutional Court Judgment In the Name of the Republic of 2011/03/22* [2011]; *Constitutional Court of Romania Decision No 1258* [2009] Off Monit Rom No 798; *Judgment the First Senate of 2 March 2010* [2010] 1 BvR 25608 1 BvR 26308 1BvR 58608; For more details on these judgments and their relation to the Data Retention Directive, see Commission of the European Union, 'Report from the Commission to the Council of the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)' (European Commission 2011).

[15] e-Privacy Directive art 6.

[16] ibid art 15(1).

e-Privacy Directive, and interfered seriously with the fundamental rights under the EUCFR.[17] The CJEU held that *indiscriminate* data retention for the purposes of fighting serious crime was incompatible with the EU law, thus extending the *Digital Rights Ireland* ruling to national data retention regimes in Member States.[18] *Tele2 Sverige* caused unease among some Member States, who felt that the CJEU had deprived them of a useful tool in combatting crime.[19] Member States hesitated to comply with the requirements stipulated in *Tele2 Sverige* judgment and reform their national data retention laws: for example, the EU Fundamental Rights Agency revealed that by 2019, most Member States have still kept data retention legislation in some form.[20]

Article 1(3) of the e-Privacy Directive states that the Directive does not apply to activities that are outside the scope of EU law and to activities concerning, *inter alia,* 'public security' and 'State security'. Under the EU legal framework, organization and oversight of national security, despite extensive European integration, remains 'the responsibility of each EU Member State'. [21] Some Member States thus have relied on these provisions of primary EU law to argue, especially after the *Tele 2 Sverige* ruling, that national data retention legislation is outside of the scope of EU law.

It is against this background that, in 2015, a UK-based civil society organisation, Privacy International, brought proceedings before the Investigatory Powers Tribunal in the UK concerning the lawfulness of the *Telecommunications Act 1984*[22] and *Regulation of Investigatory Powers Act ('RIPA') 2000,*[23] which require private communications service providers to transmit users' traffic and

[17] *Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECLI:EU:C:2016:970 (Court of Justice of the European Union).
[18] ibid 109, 112.
[19] Court of Justice of the European Union, 'Press Release No 123/20, Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature Du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre Des Barreaux Francophones et Germanophone and Others' (2020).
[20] 'Fundamental Rights Report 2019' (European Union Agency for Fundamental Rights 2019) <http://publications.europa.eu/publication/manifestation_identifier/PUB_TKAL19001ENN> accessed 18 December 2020.
[21] Consolidated Version of the Treaty on European Union 2012 (OJ 2012, C 326/15) art 4.
[22] Telecommunications Act 1984 (UK).
[23] Regulation of Investigatory Powers Act 2000 (UK).

location data in bulk to UK security and intelligence agencies.[24] Similarly, in 2016 a Belgian NGO, the Ordre des Barreaux Francophones et Germanophone launched legal action before the Constitutional Court in Belgium regarding the *Law of 29 May 2016,*[25] which imposed obligations on service providers to supply data to authorities for the purposes of ensuring national security, preventing serious crime prevention *and* investigating/prosecuting less serious crime.[26] Soon after, in 2018, several French digital rights NGOs, including Quadrature Du Net, launched a legal challenge before the Conseil d'État (Council of State) regarding the French *Code de la sécurité intérieure* ('Internal Security Code')[27] compelling electronic communications service operators to generally and indiscriminately retain the traffic and location data of all subscribers.[28]

In 2017 and 2018, the three different national courts asked the CJEU for preliminary rulings under Article 267 of the Treaty on the Functioning of the European Union ('TFEU') to clarify whether the e-Privacy Directive applied to the disputed national legislation which established data retention regimes for national security purposes in light of the Article 1(3) of the e-Privacy Directive and Article 4 of TEU. If the e-Privacy Directive *did* apply to the national legislation, the CJEU was asked whether Article 15(1) of the e-Privacy Directive enabled Member States to restrict fundamental rights to safeguard national security. The UK reference focused on the first question regarding scope of EU law, whereas the Belgian and French cases focused on the second question regarding the compatibility of the data retention regimes with the EU law.

---

[24] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service* [2016] HRLR 21 Hum Rights Law Rep 635, 638.

[25] Loi du 19 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [Law on the collection and retention of data in the electronic telecommunications sector] (Belgium) 2016 (2016/09288).

[26] *Grondwettelijk Hof* [Constitutional Court] (Belgium), Rolnummers 6590, 6597, 6599 en 6601 Arrest nr. 96/2018 van 19 juli 2018, https://www.const-court.be/public/n/2018/2018-096n.pdf.

[27] Ord. no 2012-351 du 12 mars 2012, Code de la sécurité intérieure [Code of Internal Security] (France) 2012.

[28] *Conseil d'État, 10ème - 9ème chambres réunies, 26/07/2018, 394922* [2018] Conseil d'État 394922; *Conseil d'État, 10ème - 9ème chambres réunies, 26/07/2018, 393099, Inédit au recueil Lebon* [2018] Conseil d'État 393099, Inéd Au Recl Lebon.

OPINIONS OF THE ADVOCATE GENERAL

On 15 January 2020, the Advocate General ('AG') Manuel Campos Sánchez-Bordona delivered three opinions.[29] The AG first addressed the question of whether the relevant national data retention legislation fell within the scope of the e-Privacy Directive despite Article 1(3) of the e-Privacy Directive and Article 4 of the TEU.[30] In all three cases, he interpreted these provisions to mean that 'activities' for national security purposes, conducted *solely* by state authorities, *without* the assistance of the private actors, are outside the scope of the e-Privacy Directive.[31] On the other hand, he reasoned that national data retention legislation that requires *private parties* such as electronic service providers to cooperate with the state authorities by retaining user data, and that permits state authorities to access the data collected by these private parties, *is* within the scope of the e-Privacy Directive and must comply with its data protection requirements,[32] even if it is to address 'national security concerns'.[33] Since all three countries' national legislation required the cooperation of private parties, the AG concluded that the e-Privacy Directive applied to each of them.[34]

The AG Campos Sánchez-Bordona then turned to the question whether Article 15(1) could justify the disputed national legislation.[35] In all three cases, he stressed the importance of

---

[29] *Opinion of Advocate General Campos Sánchez-Bordona, Joined Cases C-511/18 and C-512/18 La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées (Quadrature du Net, AG)* (Court of Justice of the European Union); *Opinion of Advocate General Campos Sánchez-Bordona, Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (Privacy International, AG)* (Court of Justice of the European Union); *Opinion of Advocate General Campos Sánchez-Bordona, Case C-520/18 Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres, intervener: Child Focus (Ordre des barreaux francophones et germanophone, AG)* (Court of Justice of the European Union).

[30] *Quadrature du Net, AG* (n 30) paras 78–79; *Privacy International, AG* (n 30) paras 19, 78–79.

[31] *Quadrature du Net, AG* (n 30) paras 40–43, 90; *Privacy International, AG* (n 30) para 77.

[32] *Quadrature du Net, AG* (n 30) paras 77–79; *Privacy International, AG* (n 30) para 43; *Ordre des barreaux francophones et germanophone, AG* (n 30) para 155.

[33] *Privacy International, AG* (n 30) para 31.

[34] *Quadrature du Net, AG* (n 30) para 40; *Privacy International, AG* (n 30) para 30; *Ordre des barreaux francophones et germanophone, AG* (n 30) para 26.

[35] *Quadrature du Net, AG* (n 30) paras 77–89; *Privacy International, AG* (n 30) para 89; *Ordre des barreaux francophones et germanophone, AG* (n 30) paras 32–37.

interpreting restrictions on fundamental rights strictly in light of the EUCFR and the precedent set in *Tele2 Sverige*, where the CJEU imposed a general prohibition on indiscriminate retention of traffic and location data.[36]

Therefore, in *Privacy International,* the AG concluded that national legislation compelling electronic communications network providers to indiscriminately transmit data to security and intelligence agencies is incompatible with Article 1(3) of the e-Privacy Directive, read in light of Article 4 of the TEU.[37] He further emphasized that even *if* the UK legislation *was* permissible under EU law, the UK would need to implement the requirements spelled out in *Tele2 Sverige*: access by state agencies to data must authorised by a court or independent authority, and, once access has been authorised, the relevant state agency must notify affected parties if their data is accessed.[38]

The AG similarly opined in *Ordre des barreaux francophones et germanophone* that national law, requiring general and indiscriminate data retention by communications service providers was incompatible with EU law, even though there were safeguards in place regulating authorities' access to the retained data.[39] In addition, the objectives of *Belgian Law of 29 May 2016* went beyond safeguarding national security, including the investigation of less serious offences, which made the general and indiscriminate retention of traffic and location data incompatible with the EUCFR.[40]

Yet, in his opinion on the French case, the AG Campos Sánchez-Bordona recognised an important exception to the general prohibition in *Tele2 Sverige*: that *indiscriminate* data retention may be justified if a Member State is in a 'genuinely exceptional situation', facing an 'imminent security threat' or 'extraordinary security risk'.[41] However, such retention is only permissible if it is a proportionate response that strikes the appropriate balance between national security and citizens' fundamental rights in a democratic society.[42] The AG further reasoned that such measures

[36] *Quadrature du Net, AG* (n 30) para 91; *Privacy International, AG* (n 30) para 25; *Ordre des barreaux francophones et germanophone, AG* (n 30) para 120.
[37] *Privacy International, AG* (n 30) para 45.
[38] ibid 43, 45.
[39] *Ordre des barreaux francophones et germanophone, AG* (n 30) para 155.
[40] ibid.
[41] *Quadrature du Net, AG* (n 30) para 104.
[42] ibid 102.

must first be reviewed by a court or independent administrative body, and must be temporary, carried out only for a strictly necessary period.[43] However, given that the French *Internal Security Code* imposed an indiscriminate data retention requirement, it amounted to a 'particularly serious interference' with fundamental rights, which even France's background of serious terrorist threats did not justify.[44] The AG further noted that Article 15(1) precluded national legislation which does not oblige authorities to inform affected persons about the processing of their personal data, unless this disclosure would undermine the authorities' operations.[45] However, Article 15(1) does *not* preclude national legislation requiring real-time *collection* of individuals' traffic and location data provided that it is retained and/or accessed in accordance with 'established procedures'.[46]

Given these shortcomings, the AG concluded that the obligations imposed by national legislation in all three Member States should be declared incompatible with EU law.

JUDGMENTS OF THE COURT

On 6 October 2020, the Grand Chamber of the CJEU delivered two separate judgments - one in *Privacy International*, and one for joined French and Belgian cases – *Quadrature Du Net.* In both decisions, the Court first rejected the claims by several member states, who have relied on CJEU's earlier caselaw on PNR to argue that e-Privacy Directive does not apply to the national security legislation in the three Member States.[47] According to the Court, Article 15(1) of e-Privacy Directive 'necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.' [48]As the Court explained, 'the mere fact that a

[43] ibid 139.
[44] ibid 150–153, 155.
[45] ibid 155.
[46] ibid.
[47] Arguments by UK, Czech and Estonian Governments, Ireland, and the French, Cypriot, Hungarian, Polish and Swedish Governments, relying on judgment of 30 May 2006, *Joined Cases C-317/04 and C-318/04 Parliament v Council and Commission* [2006] EU:C:2006:346, see paras 32-33 of *Privacy International* judgment and para 89 of *Quadrature Du Net* judgment.
[48] *Privacy International*, paras 35-39, citing judgment of 2 October 2018, Ministerio Fiscal, C 207/16, EU:C:2018:788, paras 32-35; 37.

national measure has been taken for the purpose of protecting national security cannot render the EU law inapplicable and exempt the Member States from their obligation to comply with that law'.[49] The CJEU thus concluded that national legislation which requires electronic communication service providers to retain data (like in *Quadrature Du Net)* and/or transmit it to national authorities (like in *Privacy International*) *is* within the scope of the e-Privacy Directive.[50]

The Court then asserted that the national security exception under Directive should not become the rule,[51] and Member States may only implement data retention measures if they are consistent with EU law,[52] and meet the requirements of Article 15(1) of e-Privacy Directive, read in the light of Articles 7, 8 and 11 and Article 52(1) of the EUCFR,[53] which requires an application of the three-step test of legality, general interest and proportionality.[54] The legality and general interest criteria were met relatively straightforwardly: the interfering national measures were all legislated and the Court accepted the safeguarding of national security as a legitimate objective of 'general interest' that could justify more serious interference with fundamental rights than would be appropriate for other, less significant objectives.[55] Thus, the CJEU focused on the proportionality requirements in both judgments.

In *Privacy International*, the Court explained that legislation requiring service providers to *transmit* data to state authorities must be based on objective criteria determining the conditions of access.[56] General and indiscriminate *transmission* of traffic and location data to security and intelligence agencies is *not* permitted under the e-Privacy Directive and the EUCFR, even if it is for the purpose of safeguarding national security.[57]

However, in *Quadrature Du Net*, the Court held that legislation made in response to a genuine, present or foreseeable 'serious threat to national security' can enable state officials to order service

[49] *Quadrature Du Net* (n 3) para 99; *Privacy International* (n 2) para 44.
[50] *Quadrature Du Net* (n 3) paras 54–56; *Privacy International* (n 2) para 49.
[51] *Privacy International* (n 2) para 59; *Quadrature Du Net* (n 3) para 111.
[52] *Privacy International* (n 2) para 60.
[53] Article 52(1) of the EUCFR provides that limitations of rights must be 'provided for by law', proportionate and necessary, and 'meeting objectives of general interest recognised by the Union'.
[54] *Quadrature Du Net* (n 3) para 121; *Privacy International* (n 2) para 64.
[55] *Privacy International* (n 2) para 75; *Quadrature Du Net* (n 3) para 136.
[56] *Privacy International* (n 2) para 78.
[57] ibid 80–83.

providers to indiscriminately *retain* data.[58] Such orders however must be 'strictly necessary', reviewed by a judicial or administrative body, which must make a binding decision on (a) the existence of a genuine, present or foreseeable 'serious threat to national security' and (b) the existence of 'conditions and safeguards which must be laid down and observed'.[59]

In contrast, the Court held that indiscriminate and general retention of traffic and location data cannot be justified for the purposes of *combating serious crime* and safeguarding *public security*. In such case, the retention must be targeted, 'strictly necessary' and done 'on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion'.[60] However, the Court explained that IP addresses are less intrusive than traffic and location data, and therefore they can be indiscriminately retained for a limited period if strictly necessary for *combatting serious crime*.[61] The CJEU regarded data relating to 'civil identity' of the users, such as their names and surnames, e-mail and postal addresses, as even less intrusive, and therefore, can be retained for an unlimited period for fighting *general* – as opposed to *serious* – crime.[62]

The Court also explained that expedited retention of traffic and location data by service providers is permissible if necessary to shed light on *serious criminal offences* or, *a fortiori,* threats to *national security*. Access to such data by competent authorities must comply with *Tele 2 Sverige* requirements and is not justified for prosecuting and punishing ordinary criminal offences.[63] Finally, indiscriminate automated analysis of traffic and location data can be justified only if Member States are facing 'serious threats to national security' and limited to a strictly necessary duration,[64] subject to effective review[65] and based on non-discriminatory criteria.[66] Individuals do

[58] *Quadrature Du Net* (n 3) para 137.
[59] ibid 138–139.
[60] *Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others* [2020] ECLI:EU:C:2020:791 [140–150].
[61] *Quadrature Du Net* (n 3) paras 152–156.
[62] *Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others* [2020] ECLI:EU:C:2020:791 [157–159].
[63] *Quadrature Du Net* (n 3) paras 160–167.
[64] ibid 172–182, particularly 177-178.
[65] ibid 179.
[66] ibid 18 citing *Opinion 1/15 of the Court (Grand Chamber)* [2017] ECLI:EU:C:2017:592 (Court of Justice of the European Union) para 172.

not have to be notified individually unless their information was matched and their profile further analysed – in that case, individuals must be notified as soon as the notification no longer jeopardises the investigation by competent authorities.[67]

Real-time collection of traffic and location data is only permissible in respect of persons who are reasonably suspected to be involved in terrorist activities; and the legislation authorising real-time collection defines circumstances and conditions for such collection, and decision is subject to a prior review by a national court independent administrative body whose decision is binding, and who has been satisfied that 'real-time collection is authorised only within the limits of what is strictly necessary'.[68] Competent authorities must notify the individuals whose data was collected real-time, as soon as the notification is no longer liable to jeopardise the investigation.[69]

Finally, the Court addressed two issues on the interaction between EU law and national legislation. First, if national legislation is incompatible with EU law, national courts cannot limit the temporal effects of a declaration of illegality in respect of national legislation, because of the primacy of EU law.[70] *(Evidence*) Second, in the context of criminal proceedings, the Court reiterated the long established position that it in the absence of EU rules on the matter, it was for the Member States to assess the admissibility of evidence resulting from indiscriminate data retention. [71] As such, evidence collected in breach of EU law is potentially admissible, with the CJEU emphasizing that under established case law, evidence must be set aside when it contravenes the right to a fair trial.[72]

It will be now for the national courts to judge the legality of national legislation considering the CJEU's ruling.

---

[67] *Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others* [2020] ECLI:EU:C:2020:791 [191].
[68] *Quadrature Du Net* (n 3) 188–189.
[69] ibid 190.
[70] ibid 113–120.
[71] ibid 222–223.
[72] ibid 226–227 citing *Case C-276/01 Joachim Steffensen, Judgment of the Court (Fifth Chamber)* [2003] ECLI:EU:C:2003:228 (Court of Justice of the European Union) paras 76-79.

A STRUGGLE FOR COMPETENCE: NATIONAL SECURITY AND THE SCOPE OF EU LAW

The *Quadrature Du Net* and *Privacy International* decisions suggest that the CJEU has become an important actor in regulating national security and intelligence activities in Europe (and as displeased Americans would say after two *Schrems* cases[73] - in the USA, but more on that below). The emergence of an EU actor capable of seriously influencing national powers of surveillance is relatively new, but is part of a larger historical trend in liberal democracies. Only with the end of the Cold War have the activities of intelligence agencies become gradually regulated by statutory laws, rather than being shielded behind secretive executive decrees with little to no protection for individuals.

This relative novelty is reflected in the EU legal framework which explicitly provides that organization and oversight of national security, despite extensive European integration, remains the responsibility of each EU Member State. Under Article 5 of the TEU , the EU only exercises competence that has been expressly or impliedly delegated to the EU by the Member States. [74] Article 4 of the TEU also provides that 'the Union shall respect the . . . Member States' essential State functions, including safeguarding national security . . . national security remains the sole responsibility of each Member State'.[75]

However, the national security of the Member States intersects and overlaps with the internal EU security, where the EU has shared competence to adopt legislative measures under Title V of the TFEU, which establishes an area of Freedom, Security, and Justice. Articles 87 and 88 of the TFEU provide for EU competence to adopt legislation on police cooperation and fighting organized crime and terrorism; matters closely related to national security. Shared - not exclusive - EU competence under Title V means that the EU Member States can also act in this area, but they have to comply with the EU legal framework. The TFEU further stipulates that the EU's competence in justice and security 'shall not affect the exercise of the responsibilities incumbent upon Member States

[73] *Case C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 (Grand Chamber of the Court of Justice of the European Union); *Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems* [2020] ECLI:EU:C:2020:559 (Grand Chamber of the Court of Justice of the European Union).
[74] TEU art 5.
[75] ibid art 4.

with regard to the maintenance of law and order and the safeguarding of internal security'.[76]

The *Privacy International* and *Quadrature Du Net* judgments emphasised the primacy of EU law over national legislation and gave little weight to the wording of the TEU's designation of national security as the 'sole responsibility of each Member State.' The CJEU' rationale is, following the reasoning of the AG, that because the retention and transmission of personal data to the intelligence agencies is carried by communications service providers, the e-Privacy Directive and the GDPR cannot be circumvented. Therefore, the national security exemption cannot be used to justify mass-surveillance programmes conducted via the communications service providers. Such interpretation can be both supported and contradicted by CJEU's earlier case law stemming from inter-institutional legal disputes in the EU in both retention of communications and traffic data as well as other data sharing regimes.

A History of Data Retention and Sharing: The Blurred Competences

First, the CJEU's reasoning over the involvement of private actors finds support in the earlier disputes over competence in data retention legislation. For example, heated debate between the European Parliament ('EP') and the Council of EU about suitable legal basis took place in the negotiations of what later became Data Retention Directive. Originally, the proposal for harmonised rules concerning the retention, access, and exchange of communications data for law enforcement purposes came from a group of Member States – France, the United Kingdom, Sweden, and Ireland – who, in April 2004, called for the adoption of a wide-ranging Framework Decision under what was then the intergovernmental Third Pillar, called Justice and Home Affairs.[77] In the view of the Council, the matter aimed at resolving issues in the field of Justice and Home Affairs, and had to be decided unanimously in the Council without consent by the EP. However, the Legal Services of the Council and the Commission advised that such an instrument could not be

[76] Treaty on the Functioning of the European Union 2012 (OJ C 3262) art 72.
[77] See Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 - C6-0198/2004 - 2004/0813(CNS)).

legally adopted under the Third Pillar because the proposed Framework Decision would require Member States to impose obligations on telecommunications service providers, and that should be dealt with under 'internal market' legislation on the regulation of telecommunications.[78] In response, the EU Commission prepared an alternative proposal for a Directive, which only sought to harmonise rules imposing data retention obligations on private providers. This way, it could be based on internal market provision, ex-Article 95 TEC (now Article 114 TFEU).[79] The EP, which had opposed the Framework Decision on human rights grounds, eventually backed the proposal for a Directive.[80]

Immediately after the Data Retention Directive was passed in 2006, Ireland, supported by Slovakia, launched legal action against EP and EU Commission before the CJEU claiming that the internal market legal basis of the Data Retention Directive – former Article 95 TEC (now Article 144 TFEU) - was not correct,[81] given that the issue primarily fell under the Justice and Home Affairs. In 2009,

---

[78] Council of the European Union, 'Avis Du Service Juridique (JUR 137 COPEN 62 TELECOM 21) [Council Legal Service Opinion]' (2005) 7688/05 <https://www.statewatch.org/media/documents/news/2005/apr/council-legal-opinion-data-retention.pdf>; Commission of the European Communities, 'Projet de Décision-Cadre Sur La Conservation Des Données – Analyse Juridique [Draft Framework Decision on Data Retention - Legal Analysis]' (2005) SEC(2005) 420 <https://www.statewatch.org/media/documents/news/2005/apr/commission-legal-opinion-data-retention.pdf>. See also 'EU: Data Retention Proposal Partly Illegal, Say Council and Commission Lawyers' (*Statewatch*, 28 March 2012) <https://www.statewatch.org/news/2005/april/eu-data-retention-proposal-partly-illegal-say-council-and-commission-lawyers/> accessed 22 December 2020.

[79] See Commission Staff Working Paper, Projet de décision-cadre sur la conservation des données – Analyse juridique SEC (2005) 420 p. 2

[80] See European Parliament Legislative Resolution on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 – C6-0198/2004–2004/0813(CNS) Official Journal 227 E , 21/09/2006 P. 0045 - 0045; European Parliament Legislative Resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (C6-0293/2005 – 2005/0182(COD)) OJ C 286E , 23.11.2006, p. 264–273.

[81] *C-301/06 Ireland v European Parliament and Council of the European Union* [2009] ECLI:EU:C:2009:68 (Court of Justice of the European Union).

the CJEU rejected the challenge and accepted the use of Article 95, because the Directive imposed data retention obligations on private actors. The reasoning of the CJEU in *Privacy International* and *Quadrature Du Net* about the involvement of the private actors in the national programmes aimed at protecting national security is therefore in line with CJEU's earlier approach on the matter.

However, *Privacy International* and *Quadrature Du Net* can be distinguished from the Irish dispute over Data Retention Directive because these cases concern an exclusive national security competence of the Member States, and not a shared EU competence in the area of Justice and Security (former Justice and Home Affairs third pillar), like it did in the Irish challenge to Data Retention Directive. *Privacy International* and *Quadrature Du Net* are similar to 2006 inter-institutional dispute between the EP and EU Commission on the EU-USA PNR data sharing arrangements, where the CJEU held that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism and other serious crimes did not fall within a scope of the Data Protection Directive 95/46 (now repealed by the GDPR),[82] but rather within a framework established by the public authorities relating to public security and the activities of the State in areas of criminal law and law enforcement.[83] The Court reasoned that the PNR data sharing arrangements could not be covered by the now repealed Directive, because its Article 3(2) excluded 'the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities […] concerning public security, defence, State security and the activities of the State in areas of criminal law.' [84]

Data Processing by State vs Private Actors under the GDPR and Law Enforcement Directive

However, in both *Privacy International* and *Quadrature Du Net*, the Court distinguished the now repealed Data Protection Directive on

[82] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ 1995, L 281/31.
[83] *Joined Cases C-317/04 and C-318/04, European Parliament v Council of the European Union and Commission of the European Communities* [2006] EU:C:2006:346 (Court of Justice of the European Union) [56–59].
[84] ibid 54.

the one hand; and e-Privacy Directive on the other. In particular, the CJEU noted that the Data Protection Directive 'excluded, in a general way, from the scope of that directive "processing operations concerning public security, defence, [and] State security", without drawing any distinction according to who was carrying out the data processing operation concerned'.[85] In contrast, the CJEU reasoned, that 'in the context of interpreting Article 1(3) of Directive 2002/58, it is necessary to draw such a distinction, because e-Privacy Directive explicitly excludes 'activities of State' which the Court defined as activities 'unrelated to the field where individuals are active'.[86]

The Court then made an explicit correlation between the e-Privacy Directive and the GDPR by claiming that the same distinction between the activities of State and individuals is also articulated under the GDPR. The CJEU reasoned that processing carried out by individuals or private actors for the purpose of prevention of criminal offences fell within the scope of the GDPR:

> although Article 2(2)(d) of the GDPR says that it does not apply to processing operations carried out 'by competent authorities' for the purposes of, inter alia, the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security, it is apparent from Article 23(1)(d) and (h) of that regulation that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation.'[87]

It is not, however, clear how Article 23(1) of the GDPR, on which the CJEU relies to make this distinction, supports the Court's position, because that provision simply lists the legitimate aims and circumstances which provide for legitimate restrictions of the obligations and rights of the GDPR, without specifying whether the processing has to be accrued out by State or private actors ('individuals', in CJEU's words).[88]

---

[85] *Quadrature Du Net* (n 3) para 101; *Privacy International* (n 2) para 46.
[86] *Quadrature Du Net* (n 3) para 92 citing Case C-207-16, Ministerio Fiscal [2018] EU:C:2018:788 (Court of Justice of the European Union), para 32; Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis [2016] ECLI:EU:C:2016:970, para 69, Case C-25/17 Jehovan Todistajat [2018] EU:C:2018:551 (Court of Justice of the European Union), para 38.
[87] ibid 102.
[88] Article 32(1) of the GDPR says: '1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure

In contrast, the CJEU reasons that when States do not impose such obligations on private actors, data processing by States is regulated by national law, informed by the Law Enforcement Directive,[89] 'with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.'[90] Law Enforcement Directive was still being negotiated when the CJEU delivered its ruling in *Tele 2 Sverige,*[91] and *Privacy International* and *Quadrature Du Net* were the first opportunity for the Court to clarify the scope of the Law Enforcement Directive.

The CJEU's reasoning that the GDPR applies to private actors, and Law Enforcement Directive applies to public agencies when processing data for national security purposes is, however, not supported by the wording of Law Enforcement Directive. In particular, Article 3(7) of the Law Enforcement Directive, clarifies that 'any entity, whether public or private, entrusted with public power by national law to process data for such purposes, fall under the scope of the Directive.' Moreover, Recital 11 of the Directive

---

the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims.

[89] Directive 2016/680 of the European Parliament and of the Council of 27 April 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 Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA 2016 (OJ 2016, L 119/89).

[90] *Quadrature Du Net* (n 3) para 103.

[91] On the relationship between Tele 2 Sverige and Law Enforcement Directive, see Barbara Grabowska-Moroz, 'Data Retention in the European Union' in Marek Zubik, Jan Podkowik and Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer 2021) <https://eui.idm.oclc.org/login?url=https://doi.org/10.1007/978-3-030-57189-4> accessed 19 December 2020.

says: 'Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive.' Recital 11 further explicitly specifies that, for instance, legal obligations imposed on financial institutions to retain data for the investigation and prosecution of financial crime fall within the scope of the Directive.

The GDPR does not explicitly define 'competent authorities'. Recital 19 says that the GDPR does not apply to '….the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties…<>…'. It adds, similar to how the now amended Data Protection Directive did, that 'This Regulation should not, therefore, apply to processing activities for those purposes.' The emphasis on the *purpose* of processing activities – as opposed to *who* does the processing – remains under the GDPR. However, the Recital 19 continues: 'However, personal data processed by *public* authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council.'

Therefore, CJEU's reasoning is not consistent with wording of the Law Enforcement Directive, and is subject to debate under GDRP. But importantly, because data collected by private actors is important source for national intelligence and security agencies, it is not clear how this model of duty outsourcing to service providers could continue. Is the CJEU is proposing a separation of the private and public data retention, like, e.g. Article 29 Working Party, an independent European advisory body on data protection and privacy, did in their Opinion on the Data Retention Directive?[92] The CJEU does not, at least explicitly, suggest that such separation of the systems is needed, leaving the legality of

[92] Article 29 Data Protection Working Party, 'Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC' (2006) 654/06/EN WP 119 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp119_en.pdf> accessed 15 January 2020.

national intelligence operations, which require private actors, questionable.

CJEU's Ambivalent Direction in the Face of Political Pressure

Moreover, given the same focus on the scope of EU law in *Privacy International* and *Quadrature Du Net* and the above mentioned 2006 PNR case, the CJEU should also have provided an explanation for its decision to prioritize the importance of fundamental rights under EUCFR *vs* TEU and the division of competence between the EU and Member States. While the Court does provide extensive requirements for the national security legislation of Member States in order to satisfy the three-step test under Articles 7, 8, 11 and 52(1) EUCFR, however, these requirements clearly broaden the scope of EU law in relation national security. By asserting that Article 4(2) of the TEU could not be read in a way that would enable Member States to avoid their rights protection obligations under the e-Privacy Directive, the CJEU's decisions in *Quadrature Du Net* and *Privacy International* will shape subsequent tensions between Member States and the CJEU on the appropriate balance between the rights protected under EU law, and the entitlement of Member States to determine their own national security measures.

However, the CJEU sends an ambivalent and somewhat conflicting message. On the one hand, *Privacy International* is arguably more than a strong reiteration of the position articulated in *Tele 2 Sverige*, prohibiting indiscriminate *transmission* and *interception* of personal data even in the context of national security. *Tele 2 Sverige* concerned data *retention* regimes for the purposes of combatting serious crime – as opposed to national security – and therefore, *Privacy International* goes a step further by imposing the same demands as articulated in Tele 2 Sverige, but in the context of national security. It is arguably a step further because, in Court's own words, 'the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives'.[93] Thus, if intelligence agencies are not allowed to demand bulk data transmission from service providers, no other agencies are.

[93] *Privacy International* (n 2) para 75; *Quadrature Du Net* (n 3) para 136.

On the other hand, the CJEU has also been cautious to minimize such wide-ranging implications of the *Privacy International* pronouncement. Therefore, while in *Quadrature Du Net* ruling, the Court demanded procedural safeguards for data *retention*, this approach is very different from that in *Tele2 Sverige* where the CJEU had insisted that to be proportionate, data retention had to be targeted. *Qadradture Du Net*, on the other hand, accepts indiscriminate data retention as, *in principle*, capable of being proportionate.

Such a 'U-turn' in CJEU's jurisprudence, is, however, not surprising, given that the Court was under a lot of pressure to soften its wide-ranging stance developed after the Snowden revelations in 2013. For example, the CJEU's post-Snowden approach has been criticised by US commentators as 'hyper-constitutionalization', and even as a 'largely self-congratulatory exercise that … uses a strategy of "othering" in order to build a specific European identity upon the very idea of privacy'.[94] This is particularly directed at CJEU's rulings in the two *Schrems* cases, in which the Court invalidated the EU-USA data transfers for the lack of safeguards in the US surveillance legislation. US critics argued that it is hypocritical for the CJEU to apply EU law standards to US surveillance frameworks, when it lacks capacity to apply EU legal rules to the national security frameworks of the EU Member States.[95] *Privacy International* and *Quadrature Du Net* however shows that the CJEU is willing to apply the same requirement to national security surveillance frameworks of Member States.

Similar to the concerns of US national security experts, the Council of EU, seeing the CJEU's post-Snowdenian decisions as overreaching and depriving Member States of useful national security tools, has been leading consultations on the data retention in the EU after invalidation of the EU Data Retention Directive.[96]

---

[94] Thomas Wischmeyer, '"Faraway, So Close!" – A Constitutional Perspective on Transatlantic Data Flow Regulation' in Anna-Bettina Kaiser, Niels Petersen and Johannes Saurer (eds), *Obama's Court: Recent Changes in U.S. Constitutional Law in Transatlantic Perspective* (Nomos 2018) 15.

[95] Peter Swire, '"Schrems II" Backs the European Legal Regime into a Corner — How Can It Get Out?' (*IAPP Blog*) <https://iapp.org/news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/> accessed 11 August 2020.

[96] 'Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime' (Council of the European Union 2019) 9663/19 <https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf> accessed 17 October 2020.

Calls for the Council to homogenize data retention instruments in Europe have been supported by organisations such as Europol and the EU Counter-Terrorism Coordinator, who advocate for easier and more coherent data sharing among law enforcement agencies in the EU.[97] Given this political climate, the CJEU's ambivalent response – both asserting its authority over national security, yet at the same time, not opposing indiscriminate data retention *per se* – is not unexpected.

Four cases on data retention and suitable safeguards are currently pending before the CJEU,[98] and one from the German *Bundesverwaltungsgericht* ('Federal Administrative Court') explicitly concerns national security exception in Article 15 of the e-Privacy Directive.[99] It remains to be seen whether the CJEU will reassert the narrow interpretation of national security exception in EU law in that case. Such a narrow interpretation would reinforce the *Privacy International* and *Quadrature Du Net* rulings and solidify Court's position as an EU actor with serious influence over national surveillance powers. While the CJEU could, theoretically, broaden its interpretation of the national security exception and expand the powers of Member States to self-regulate on issues of national security in the forthcoming German case, such an outcome seems less likely after the precedent set in *Privacy International* and *Quadrature Du Net.*

---

[97] Europol, 'Proportionate Data Retention for Law Enforcement Purposes' <https://www.statewatch.org/media/documents/news/2018/feb/eu-council-data-retention-europol-presentation-targeted-data-ret-wk-9957-17.pdf> accessed 23 October 2020; EU Counter-Terrorism Coordinator, 'Data Retention: Contribution by the EU Counter-Terrorism Coordinator' 1 <https://www.statewatch.org/media/documents/news/2017/nov/eu-council-ctc-working-paper-data-retention-possibilities-wk-9699-17.pdf> accessed 23 October 2020.

[98] Request for a preliminary ruling from the Riigikohus (Estonia) lodged on 29 November 2018, *H.K. v Prokuratuur* (Case C-746/18) and *Opinion of Advocate-General Pitruzella, Case C-746/18* [2020] ECLI:EU:C:2020:18 (Court of Justice of the European Union), delivered 20 January 2020; Request for a preliminary ruling from the Bundesverwaltungsgericht (Germany) lodged on 29 October 2019, *Federal Republic of Germany* v *SpaceNet AG* (Case C-793/19); Reference for a preliminary ruling from the Supreme Court (Ireland) made on 25 March 2020 – *G.D. v The Commissioner of the Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General* (Case C-140/20); Request for a preliminary ruling from the Bundesverwaltungsgericht (Germany) lodged on 29 October 2019, *Federal Republic of Germany v Telekom Deutschland GmbH* (Case C-794/19) *('Telekom Deutschland').*

[99] *Telekom Deutschland* n 98.

IMPACT ON FUTURE DATA SHARING REGIMES AND REFORMS

Beyond the struggle for competence in data retention schemes for national security, *Privacy Intenational* and *Qudarture Du Net* rulings will impact other data sharing regimes, where personal data are collected initially for commercial purposes and subsequently processed for law enforcement purposes. For example, the national PNR regimes, implementing the EU PNR Directive 2016/681,[100] are currently challenged in courts in Germany and Belgium, which have requested preliminary rulings from the CJEU.[101] If the Member States are able to claim that PNR regime is crucial in safeguarding national security, then the 5-year retention period of PNR data articulated in the EU PNR Directive, could be held proportionate by the CJEU.

The decisions will also impact the proposed e-Privacy Regulation[102] set to repeal the e-Privacy Directive, the proposed EU e-Evidence package (both Regulation and Directive) and *e-Evidence Digital Exchange System (eEDES)*, aimed at facilitating law enforcement agencies' and judicial authorities' cross-border access to electronic evidence.[103] The EU Commission is also currently

[100] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime 2016 (OJ L 119) 132.

[101] Belgian Constitutional Court, 'Press Release on Judgment 135/2019: The Belgian Constitutional Court Refers Ten Preliminary Questions to the Court of Justice Concerning the Obligation to Transfer Passenger Information' (2019) <https://www.const-court.be/public/e/2019/2019-135e-info.pdf>.
Administrative Court of Hesse, 'Press Release on Decisions of May 13th and 15th, 2020 (Ref .: 6 K 805 / 19.WI and 6 K 806 / 19.WI),: Regulations of the Passenger Data Act on the test bench' (2020) < https://verwaltungsgerichtsbarkeit.hessen.de/pressemitteilungen/vorschriften-des-fluggastdatengesetzes-auf-dem-pr%C3%BCfstand>.

[102] '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)' (European Commission 2017) COM/2017/010 final-2017/03 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> accessed 19 November 2020.

[103] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters' (2018) COM/2018/225 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>; European Commission, 'Proposal for a Directive of the European Parliament and of the

negotiating an EU-US agreement on cross-border access to electronic evidence,[104] while the Second Additional Protocol to the *Council of Europe's Convention on Cybercrime* aim to enhance international cooperation, including provisions on direct cooperation of law enforcement authorities with service providers in other jurisdictions (latest draft of the Protocol was published on 10 November 2020).[105] While *Privacy International* suggests the CJEU has used the opportunity to impose the safeguards for fundamental rights in national security, the compromise judgment in *Quadrature Du Net* strengthens the position of law enforcement agencies in the ongoing negotiations because CJEU's abstract reasoning provides a lot of room to the agencies to claim 'strict necessity' for indiscriminate data retention, automated analysis of it as well as a real-time collection of data, all in the name of national security.

Implications for the EU-UK Data Flows after Brexit

Another important implication of the CJEU's pronouncements concern the national security and surveillance laws in the UK, which is now seeking an adequacy decision under Article 45 of the GDPR. The CJEU's decisions came shortly before the expiry of the Brexit transition period on 31 December 2020, and the adverse ruling in *Privacy International* raises questions about the EU Commission's pending adequacy decision. As of 1 January 2021, data transfers between UK and EU are governed by the interim regime (so-called 'bridging clause') under the *EU-UK Trade and Cooperation Agreement*, agreed by EU and UK negotiators on 24

Council Laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings' (2018) COM/2018/226 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN>; 'Security Union: Commission Facilitates Access to Electronic Evidence' (*European Commission*, 17 April 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343> accessed 22 December 2020.

[104] 'Launch of EU-U.S. Negotiations on Criminal Justice' (*European Commission*, 26 September 2019) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890> accessed 23 December 2020.

[105] Cybercrime Convention Committee (T-CY), 'Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime' (Council of Europe 2020) T-CY (2018)23rev.

December 2020.[106] The interim regime enables continued EU-UK data flows, with no need for companies and public authorities to put in place any special data transfer arrangements. This solution is applicable for a period of maximum six months, and on 19 February 2021, the Commission published two draft adequacy decisions for EU-UK data transfers under the GDPR[107] and the Law Enforcement Directive.[108] An affirmative finding of adequacy of the UK legal system will allow data transfers between the EU and the UK to continue post-Brexit despite the UK's new status as a 'third country'. But this requires an EU Commission finding of an 'essentially equivalent' protection of personal data and fundamental rights in the UK law to that available under EU law. The meaning of 'essential equivalence' was most recently elaborated by the CJEU in the *Schrems II* case, where lack of procedural safeguards in the US surveillance scheme prevented the finding of the 'essential equivalence' for the US, and resulted in the invalidation of the *Privacy Shield*.[109] Given the CJEU's finding in *Privacy International* that UK's data retention and transmission practices under the *Investigatory Powers Act* are incompatible with EU law, such determination by the EU Commission is unlikely and could lead to a potential legal limbo for the post-Brexit data transfers between the UK and EU.[110] The publication of the draft Commission adequacy decisions in February 2021 is only the beginning of a process, which requires obtaining an opinion from the European Data Protection Board (EDPB) and support from a committee composed of representatives of the EU Member States.[111] At the moment, it is unclear how the UK Government

---

[106] *Trade and Cooperation Agreement between The European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part,* OJ L 444, 31.12.2020, p. 14–1462.

[107] *Draft Commission Implementing Decision 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*, 21 February 2021, available at https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf

[108] *Draft Commission Implementing Decision 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, 21 February 2021, available at https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf*

[109] *Schrems II* (n 74).

[110] For more, see Chloé Brière, 'Conditionality in Defining the Future Cooperation in Criminal Matters between the United Kingdom and the European Union' (2020) 21 ERA Forum 515.

[111] European Commission, Brexit – International Dimension of Data Protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_en

could prove the 'essential equivalence' to secure the adequacy decision.

CONCLUSION

At the heart of *Privacy International* and *Quadrature Du Net* is the struggle for competence at the intersection of data retention and national security. The EU institutions, including the CJEU, but also the EU Commission, EP, are institutionally inclined to define 'national security' narrowly, strengthening their own role in the area. The Member States, on the other hand, have an institutional interest in keeping the EU institutions out of their national security business. At the same time, the Member States cannot avoid the growing European interdependence in security matters, so the struggle will continue.

Yet, while *Privacy International* is an unequivocal assertion of CJEU's authority in the area of national security and a welcome victory for privacy advocates, *Quadrature Du Net* does not oppose indiscriminate data retention in principle and is an ambivalent response by the CJEU in the face of political pressure. The CJEU left it up to the Member States to determine when *indiscriminate* data retention is needed for national security purposes, contrasting with the Court's previous unequivocal stance against the indiscriminate data retention in *Tele2 Sverige*. The softening of the CJEU's approach is unfortunate from data protection perspective, but reflects the growing pressure on the Court by other EU institutions and global trading partners, such as the USA. The Court's ambivalent response to this pressure will affect other data sharing regimes, such as the PNR, which are currently being challenged in Germany and Belgium, as well as data sharing beyond the EU.

It remains to be seen whether the Court will further relax its approach on data retention in pending cases from Estonia, Germany and Ireland. Yet, the CJEU's ambivalent response to political pressure in *Quadrature Du Net,* coupled with the efforts by the Council of the EU and Europol to develop a new data retention framework, suggests that the future of data retention in the EU most likely will favour the interests of law enforcement over fundamental rights, in the name of national security.