Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 79

National Security, Privacy, and Possible Alterations in the Court of Justice of the European Union's Case Law in Response to the Spyware Surveillance Crisis

David Mollenkamp

2023

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

David Mollenkamp is a first-year law student at Stanford Law School. Prior to attending law school, David worked as a secondary school educator in the United States and the United Kingdom. At Stanford, his research focuses primarily on national security and comparative public law and procedure.

General Note about the Content

The opinions expressed in this student paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum, or any of TTLF's partner institutions, or the other sponsors of this research project.

Suggested Citation

This European Union Law Working Paper should be cited as:
David Mollenkamp, National Security, Privacy, and Possible Alterations in the Court of Justice of the European Union's Case Law in Response to the Spyware Surveillance Crisis, Stanford-Vienna European Union Law Working Paper No. 79, http://ttlf.stanford.edu.

Copyright

Abstract

Since 2017, individual EU Member States have used spyware surveillance software to evade the privacy rights of individual citizens. Without citizens' knowledge, Member States access individuals' tracking data, messages, and phone calls. While no legal challenges have emerged from individual citizens against states, the Court of Justice of the European Union's current data privacy jurisprudence is woefully unprepared to hold states accountable for what appear to be the plain security rights of individual citizens.

This paper seeks to define the current state of the Court of Justice of the European Union's current jurisprudence and offer two critiques to its jurisprudence. First, this paper argues that the lack of a substantive definition of "national security" allows states to invoke the term to circumvent the European Union's privacy requirements. Secondly, this paper argues that the Court of Justice of the European Union should replace the "independence" test when assessing reviewing courts for the "established by law" test. Doing so, this paper argues, it would more meaningfully constrain Member States from violating individual citizen's privacy rights with a perfunctory referral to "national security."

Finally, this paper briefly analyses current proposals made by the European Parliament's Task Force and considers why those proposals would not be as effective as the European Parliament suggests they might be.

Table of Contents

Introduction

At the turn of the millennium, the European Union ("EU") passed the Charter of the Fundamental Rights of the EU ("Charter") in an attempt to codify and guarantee the rights of European citizens. The seven titles of the Charter provide "dignity," "freedoms," "equality," "solidarity," "citizens' rights," and "justice."[1] Two provisions in the "freedoms" title have had major implications for Member States that have sought to ensure national security by retaining, accessing, and sharing their citizens' telecommunications data. The first provision, Title II, Article 6 notes that "Everyone has the right to respect for his or her private and family life, home and *communications*."[2] In addition to this broad protection of communication, Title II, Article 7 adds that "[e]veryone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[3] Generally, the two provisions are referred to as the "right to a private life" and the "right to privacy."

Member States and EU institutions alike have sought to reconcile the "right to a private life" and the "right to privacy" with Article 4(2) in the Treaty on the EU ("TEU") providing that "[the EU] shall respect [Member States'] essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. *In particular, national security remains the sole responsibility of each Member State*."[4] In the context of retaining and accessing user data, providing an appropriate balance between these two sources of primary EU law has proven nearly impossible.

---

[1] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
[2] *Id.*, Chapter II, Art. 6, (emphasis added).
[3] *Id.*, Chapter II, Art. 7.
[4] Consolidated Version of the Treaty on the European Union art. 4(2), Oct. 26, 2012, 2012 O.J. (C 326) 13 [hereinafter TEU].

Indeed, Member States argue that the Court of Justice of the European Union's ("CJEU") attempts to resolve the issue has aggravated Member States' efforts to thwart genuine national security threats. At the same time, human rights advocates worry that the CJEU's rulings may not adequately protect individuals from Member States' abuse of data in the long run.[5]

In light of the CJEU's recent rulings, Member States have tacked a new course. Rather than implementing legislation that requires telecommunications providers to present users' data, Member States have hired surveillance software companies operating outside of the CJEU's jurisdiction to retain users' data on their behalf. Member States justify these data retention schemes by making a perfunctory reference to national security and claiming absolute authority under Article 4 TEU. So far, this tactic has enabled Member States to circumvent the requirements established in recent CJEU jurisprudence and evade the protections guaranteed to EU residents in the Charter. To resolve this issue and more adequately protect individuals' fundamental rights as they pertain to data privacy within the EU, the CJEU should more clearly define "national security" and establish a more robust process of judicial review to validate whether a Member State's data retention scheme actually seeks to protect the Member State.

The Privacy Landscape

In 2002, the EU passed Directive 2002/58 ("ePrivacy Directive") in part urging Member States to issue new legislation regarding data access, data retention, and data sharing.[6] Article 15 of the ePrivacy Directive permitted Member States to "restrict [users'] rights" regarding data privacy to "safeguard national security (i.e., State security), defence, public security, and the

[5] *See, e.g.*, EDRI, DATA RETENTION? ADVOCATE GENERAL SAYS 'ASKED AND ANSWERED'," https://edri.org/our-work/data-retention-advocate-general-says-asked-and-answered/

[6] Directive 2002/58/processing of personal data and the protection of privacy in the electronic communications sector.

prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system."[7]

In 2006, the European Parliament and the Council of the European Union attempted to strengthen the article by adopting the Data Retention Directive 2006/24/EC ("Data Retention Directive").[8] The Data Retention Directive sought to create EU-wide retention standards that could combat serious crime. It required telecommunication companies that obtain users' data to do so for a minimum of six months and a maximum of twenty-four months in case any such data could be useful in combatting crime or providing for national security.[9]

While the national security exception in the ePrivacy Directive and the additional Data Retention Directive seemed sensible at the time of their passage, human rights groups and telecommunication providers have since contested their legality, arguing that they conflict with the right to privacy and communication guaranteed by the Charter.

***Digital Rights Ireland* and Limitations on Data Retention**

The CJEU first considered the legality of the Data Retention Directive in 2014. Digital Rights Ireland, a human rights group, argued that the Data Retention Directive violated the right to privacy guaranteed by Articles 7 and 8 of the Charter by allowing Member States to surveil their residents on a massive scale without even the pretense of harm to national security.[10]

The CJEU agreed. The Court weighed the Data Retention Directive's interest in curtailing criminal activity against the Charter's provisions advancing privacy.[11] EU legislators

---

[7] Article 15, Directive 2002/58/processing of personal data and the protection of privacy in the electronic communications sector.
[8] Directive 2006/24/EC, Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
[9] *Id.*
[10] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* ECLI:EU:C:2014:238., ¶ 65-66 (Apr. 8, 2014).
[11] *Id.*, par. 38.

could only justify limiting rights established by the Charter when they respected the essence of the rights provided and ensured the limitations were proportionate to the aim pursued.[12]

Even though the Data Retention Directive had a valid aim in fighting crime, it failed the proportionality test by permitting indiscriminate data retention.[13] In so doing, the Data Retention Directive allowed Member States to disrespect the essence of the rights established by the Charter. Thus, the Court deemed the Data Rights Directive invalid. The European Parliament could not request that Member States pass legislation which facially violated citizens' rights codified in EU primary law.

The ruling was sensible enough. EU legislators did not assert that they approved the Data Retention Directive in furtherance of Article 4(2) of the TEU as they could not. Per the article, only Member States have power over national security. Future cases though exposed the conflict between the TEU and the Charter.

Tele2Sverige and the Subjection of the National Security Defense

Shortly after the Court's finding in *Digital Rights Ireland*, the Swedish company Tele2 Sverige stopped retaining user data in compliance with the Swedish government's data retention laws.[14] The company argued that the Swedish laws were unenforceable since they required telecommunication providers to retain all telecommunications users' data indiscriminately without any time constraints.[15] The CJEU considered whether the Swedish government's data retention regime could be deemed valid under Article 15 of the ePrivacy Directive. It could not,

---

[12] *Id.*, par. 63-64.
[13] *Id.*, par. 64.
[14] COLUMBIA UNIVERSITY GLOBAL FREEDOM OF EXPRESSION, JOINED CASES TELE2 SVERIGE AB V. POST-OCH TELESTYRELSEN AND SECRETARY OF STATE FOR THE HOME DEPARTMENT OF WATSON, https://globalfreedomofexpression.columbia.edu/cases/the-cases-of-privacy-international-la-quadrature-du-net-and-others/.
[15] Joined Cases C-203/15 and C-689/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others* [hereinafter *Tele2Sverige*], ECLI:EU:C:2016:970, ¶ 46.

the CJEU reasoned, because Article 15 of the ePrivacy Directive, like the Data Retention Directive, violated the fundamental rights under Articles 7 and 8 of the Charter. [16]

In *Tele2 Sverige*, the CJEU first addressed the national security argument offered by Member States. The Court noted that the Charter's protection of the freedom of expression "constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded."[17] The CJEU then equated the fundamental freedoms guaranteed by the Charter with the freedoms guaranteed by the Member States.[18] Implicitly then, the Court adopted the view that a Member State's right to protect national security under Article 4 TEU is limited to when it conflicts with the Charter's protections.[19]

After indicating that any data retention scheme may only be implemented if the data retained is "strictly proportional" to a demonstrated need for the data, the Court made its first attempt to define national security in relation to privacy rights. The Court stated that "[i]n particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities."[20] The Court specifically referred to terrorist activities in defining national security but failed to distinguish

[16] *Id.*, ¶ 91.
[17] *Id.*, ¶ 93.
[18] The CJEU's decision to read the Charter as an element into the founding treaties is somewhat surprising given the political debate that preceded the passage of the Charter and the Charter's applicability to all countries within the EU. Note that, at the time of its passage, both the United Kingdom and Poland requested a protocol indicating that the Charter would not have force in their respective countries. At the same time, the Czech Republic sought an equivalent protocol but abandoned it before the Charter obtained legal effect. While the debate about the significance of the Poland Protocol continues, it is plausible that the CJEU's rulings on Data Privacy reignite some discussion of its applicability.
[19] *Tele2 Sverige*, ¶ 122.
[20] *Id.*, ¶ 119.

what type of terrorist activities might be deemed a national security concern as opposed to a public security concern. The distinction is important since the CJEU's later jurisprudence would permit variable levels of responses according to whether an activity was a national security concern or a public security concern, claiming that Article 4 TEU gives states plenary authority over the former but not the latter.

Privacy International* and the Reaffirmation of *Tele2 Sverige

In June of 2015, Privacy International, a human rights group in the United Kingdom ("UK"), filed a claim before the UK's Investigatory Powers Tribunal, alleging that the UK's national security agencies' acquisition and retention of massive amounts of data contravened EU law.[21] The agencies alleged that their power to retain user data came not from Article 15 of the ePrivacy Directive, but rather from Article 4 TEU itself. As an executive body of a Member State, the agencies claimed, any attempt to protect national security need not comply with other rights guaranteed by EU law since national security matters were beyond the scope of EU institutions.

In *Privacy International*, the Court reaffirmed the position it laid out in *Tele2 Sverige*, arguing that a Member State's rights under Article 4 TEU were restricted to the principles of primary EU law.[22] Because the EU was founded on the fundamental principles enumerated in the Charter, Member States who belonged to the EU must comply with those principles.[23] Namely, Member States could not indiscriminately retain data because doing so constituted a breach of

---

[21] COLUMBIA UNIVERSITY GLOBAL FREEDOM OF EXPRESSION, THE CASES OF PRIVACY INTERNATIONAL, LA QUADRATURE DU NET AND OTHERS [hereinafter COLUMBIA REPORT ON PRIVACY INTERNATIONAL, LA QUADRATURE DU NET AND OTHERS], https://globalfreedomofexpression.columbia.edu/cases/the-cases-of-privacy-international-la-quadrature-du-net-and-others/
v. Secretary of State for Foreign and Commonwealth Affairs and Others ECLI:EU:C:2020:790.
[22] Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790 ¶ 91.
[23] *Privacy International* ¶¶ 66-68.

privacy and confidentiality.[24] Additionally, the sheer amount of data collected increased the possibility that a party would unlawfully access it or otherwise abuse it. The CJEU functionally expanded the reach of EU law in *Privacy International* by announcing that national security matters, while remaining under the sole authority of the States, must still comply with EU law. In so doing, the *Privacy International* court expanded *Tele2 Sverige* by foreclosing the possibility that national security agencies could require telecommunication providers to give users' traffic and location data to Member States' agencies.

***La Quadrature du Net* and a New Balance between Security and Privacy**

The CJEU reversed course in *La Quadrature du Net*, which expanded the scope of permissible data retention by Member States, while the Court's previous three rulings limited Member States' ability to retain data.

A few months after Privacy International requested the CJEU to hear its case, French human rights groups sought to annul a decree by the Conseil d'État requiring telecommunication providers to process data indiscriminately to determine if any such data might constitute national security threats.[25] Like the UK's Investigatory Powers Tribunal, the French government also claimed authority under Article 4 TEU, alleging that its activities were not subject to EU law.

While the CJEU announced that the French legislature's delegation of authority to national security agencies still fell within the bounds of EU law, the Court took a different approach to defining Member States' surveillance rights within the EU. The CJEU first identified three different types of threats a Member State might face.[26] A Member State may first face "a

[24] *Id.* ¶ 50.
[25] COLUMBIA REPORT ON PRIVACY INTERNATIONAL, LA QUADRATURE DU NET AND OTHERS, https://globalfreedomofexpression.columbia.edu/cases/the-cases-of-privacy-international-la-quadrature-du-net-and-others/

[26] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v. Premier Ministre and Others* [hereinafter *La Quadrature du Net*], ECLI:EU:C:2020:791, ¶ 136 (Oct. 6, 2020).

genuine and present or foreseeable," "serious threat" against *national security*.[27] Second, a Member State may face "serious threats" or "serious attacks" on *public security*.[28] And finally, a Member State may face general crimes against *public security*.[29] In response to each of these different types of state interests, the CJEU announced that Member States may retain and access different types of data—subject to review by an independent court.[30]

The CJEU gave Member States a great degree of latitude when facing national security threats. The Court noted that Member States may respond to national security threats with any of the following tools: preventive mass data retention of traffic and location data, automated analysis of traffic and location data, preventive targeted retention of traffic and location data, real-time collection of traffic and location data, expedited retention, and preventive mass retention of civil identity data.[31] Under *Privacy International* and the Court's earlier jurisprudence, Member States could not have employed any of the preventive retention schemes. Thus, these tactics expanded Member States' data retention tools allowable under EU law. In combatting "serious threats" against public security, Member States were provided a slightly lesser degree of latitude, and then very limited latitude when facing general threats against public security. While the Court gave the distinction between national security, which permits the use of preventive measures, and public security, which generally does not, greater force, the Court did not adequately define either.

Distinguishing National Security and Public Security

[27] *Id.* ¶ 137.
[28] *Id.* ¶ 146.
[29] *Id.* Note that the CJEU does not understand general crimes as a valid justification for the use of data retention methods.
[30] *Id.*
[31] *Id.* ¶ 134-139.

The CJEU's case law regarding data privacy has largely defined national security in the negative. That is, the Court has often identified what national security is not to suggest what it might be. In *Digital Rights Ireland*, the Court first distinguished between national security and public security, contending that the Data Retention Directive was largely concerned with public security—the prosecution of criminals within a Member State's borders.[32] Criminal prosecutions, the Court suggested, did not rise to the level of national security concerns because they did not involve essential state functions.[33] Commentators and the TEU itself agree that national security does not include the State's attempts to prosecute criminals.[34]

The Court has provided only two distinct examples of what might constitute a national security concern. In *Tele2 Sverige*, the Court, in dictum, pointed to "organised crime" and "terrorism" as specific examples of what constitutes national security.[35] The Court also provided its singular positive definition of national security in the context of data retention in *Privacy International*. There, the Court opined that national security includes "the primary interest in protecting the essential functions of the State and the fundamental interests of society and 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] This definition, though vague, identifies the outer limits of Article 4 TEU in the context of data privacy. The Court suggested that if an activity does not seek to prevent

[32] *Digital Rights Ireland* ¶ 41.
[33] *Id.*
[34] *See* ORLA LYNSKEY, EUROPEAN LAW BLOG, JOINED CASES C-293-12 AND 594/12 DIGITAL RIGHTS IRELAND AND SEITLINGER AND OTHERS: THE GOOD, THE BAD, AND THE UGLY (Apr. 8, 2014), https://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/; TFEU, art. 4(2)
[35] *Tele2 Sverige* ¶ 103.
[36] *Privacy International* ¶ 74.

destabilizing the fundamental constitutional, political, economic, or social structures of a country, then it cannot be defined as national security. Accordingly, the line between national security and public security depends on whether a potential threat impacts one of the "essential functions of the State." While the definition sounds sensible, the limit, in reality, is so poorly defined as to be meaningless.

This is so in part because the CJEU does not subject Member States' decisions regarding what amounts to a national security concern to judicial review outside of the Member States' borders. In *La Quadrature du Net*, the CJEU specified only that decisions must be subject to "effective judicial review."[37] In using that expression, the CJEU imposed on the Member States the requirements of effective judicial review that it established in its previous jurisprudence and would reinforce in *HK v. Prokuratuur*. In *HK*, the Court ruled that effective judicial review must be accommodated by either a domestic court or an administrative body that has all the powers necessary to review claims presented to it.[38] Moreover, *HK* held that the domestic court or tribunal must be free from influence from other parties and, in criminal investigations, must be able to strike a fair balance between national security and the fundamental right to privacy.[39] Accordingly, the domestic court or tribunal cannot be involved in any investigation and must be neutral with respect to the parties.[40]

By imposing these restrictions on domestic courts and tribunals adjudicating matters relating to data retention regimes within Member States, the CJEU sought to eliminate the

[37] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, ECLI:EU:C:2020:791, ¶ 163 (Oct. 6, 2020).
[38] Case C-746/18, *HK v. Prokuratuur*, ECLI:EU:C:2021:152 ¶ 51 (Mar. 2, 2021).
[39] *Id.*, ¶ 53.
[40] *Id.*, ¶ 54.

possibility that Member States might evade EU law with passing references to national security. But the CJEU did not succeed.

By making Member States' decisions about what constitutes a national security threat subject only to domestic courts and administrative tribunals, *La Quadrature du Net* simply encouraged Member States to ensure that domestic courts and tribunals are staffed by judges that are likely to rule in favor of Member State when presented with data retention claims involving national security. Member States' attempts to staff courts with judges disposed toward national security does not contravene the elements of effective judicial review as defined in *HK*.[41]

Even though *HK*'s requirement that courts be able to strike a balance between national security and the fundamental right to privacy seems to prevent this tactic, the CJEU has not clarified what it means to "strike a fair balance" and no case law suggests that selecting judges who, on balance, favor national security claims would disable a judge from being able to "strike a fair balance." Indeed, additional case law suggests that the legislature's attempt to hire judges partial to national security when presented with data privacy concerns is valid. In *A.K. and others*, the CJEU noted that the inquiry regarding the independence of a court has two aspects. First, the CJEU asks whether the court is free from external influence when deciding case law, and second, whether the court "has an equal distance . . . from the parties to the proceeding and their respective interests."[42] Indeed, a judge may only be said not to be acting impartially if "the judge gave any indication of personal prejudice or bias in a given case" or if "there are ascertainable facts which may raise doubts as to his or her impartiality."[43] However, the fact that

[41] *See HK v. Prokuratuur*, specifying that the elements of judicial review requires independence but that independence does not include exemption from the inherently political process of selection to the bench.
[42] Joined Cases C-585/18, C-624/18 and C-625/18, *A.K. and others v. Prokurator Generalny* (hereinafter *A.K.*), ECLI:EU:C:2019:982 ¶ 122 (Nov. 19, 2019).
[43] *Id.*, ¶ 128.

a judge was appointed by an executive does not give rise to a reason to doubt a judge's impartiality.[44]

Accordingly, staffing courts with judges that favor national security claims on balance does not make courts dependent or partial as prohibited by *HK* and *La Quadrature du Net*.[45] While domestic courts must be independent from political branches, nominating judges through the normal political processes, so long as they are qualified, does not violate the independence test. Rather, nominating friendly judges is the primary legitimate political tool that European lawmakers use to control domestic courts.

Accordingly, the CJEU's recent jurisprudence has expanded the meaning of Article 4 TEU while claiming to limit it by inviting Member States to create indiscriminate data retention regimes with passing references to national security and to subsequently make their regimes subject to tribunals with judges who are nominated by the governing parties because they favor national security, on balance, over personal privacy. Thus, Member States may obtain favorable rulings from domestic courts all while remaining within the confines of the CJEU's current jurisprudence.

The CJEU's attempt to restrict Member States also fails for a political reason—that is, the interplay between judicial bodies on the one hand, and the legislature and executive on the other, makes it practically impossible for courts to be independent notwithstanding the judicial standards established in *HK*. Existing studies on Member States' national security services

---

[44] *Id.*, par. 133.

[45] Note though that the European Court of Human Rights (ECHR) imposes a different definition of judicial review. Rather than relying on the independence test set forth by the CJEU, the ECHR relies on the establishment test. That is, the ECHR considers whether the court was "established by law." The establishment test considers more factors than the independence test. *See* Filipek, Paweł. *Only a Court Established by Law Can Be an Independent Court: The ECJ's Independence Test as an Incomplete Tool to Assess the Lawfulness of Domestic Courts,* VerfBlog, 2020/1/23, https://verfassungsblog.de/only-a-court-established-by-law-can-be-an-independent-court/, DOI: 10.17176/20200123-181754-0.

indicate that only a few judicial bodies across the EU comply with the standards the CJEU imposes on Member States in the context of data privacy.[46] While Member States in theory must implement new laws to comply with the judgment, the CJEU cannot practically prohibit a Member State from implementing a new data retention scheme on the grounds that its judicial review is insufficient until a tribunal refers such a case to the CJEU. Tribunals that are not in compliance with effective judicial review requirements are unlikely to refer a case to the CJEU. Despite their legal obligation to update laws to provide for effective judicial review, Member States will instead continue to assert that their data retention schemes are valid by referring to national security in the abstract. Setting this argument aside though, even those Member States whose domestic courts comply with the CJEU's jurisprudence may routinely rule in favor of the Member States because the political branches nominate the judges and the CJEU has not prohibited politicians from nominating judges who favor national security claims over claims of privacy.

The Logic in *La Quadrature du Net* Creates Scenarios Antithetical to the Purposes of EU Law

La Quadrature du Net allows for the possibility of scenarios that are antithetical to the intent behind the CJEU's privacy jurisprudence. Imagine that the elected legislators of Member State A view political adversaries as a threat to the political structure of Member State A. In an effort to limit their political adversaries' activities, Member State A's legislators seek to retain data regarding their adversaries' whereabouts, the length of their conversations, and the people

[46]EU Agency for Fundamental Rights (FRA), 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Mapping Member States' Legal Frameworks' (6 November 2015), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf, 52

with whom they communicate. To accomplish this end, legislators purchase surveillance software that retains data on their political adversaries.

In line with *La Quadrature du Net*, the legislators' decision deeming their political adversaries a threat to the political structure of Member State A is reviewable by a court or administrative body within the State. The court conducts a fair trial, but because of the judge's sympathy for national security claims, the court determines that the existence of the political adversary poses a threat to the political structure of Member State A. Thus, the court upholds the legislators' data retention regime, and the political adversaries are subject to data retention without a guarantee to privacy.

Do the political adversaries' activities constitute a legitimate national security concern? If the political adversaries threaten violence against the legislators or executive members, then yes. Absent any such threat, the mere existence of a political adversary would likely not be a legitimate national security to most judges. Yet, the domestic court in this hypothetical, though functionally independent from the executive, may have been nominated by the political party imposing the new data retention scheme specifically because of his sensitivity to national security matters.

While this hypothetical may seem like a distant fantasy, some Member States have made it a reality in recent years—in part as a result of the CJEU's jurisprudence on data retention and lack of a concrete definition of national security or adequate system of judicial review.

The Spyware Surveillance Software Crisis Illuminates Why the CJEU Should Attempt to More Concretely Define National Security

Between 2015-17, a handful of EU member states, including Poland, Hungary, Greece, Spain, and Cyprus, allegedly purchased spyware from private surveillance software companies.[47] Human rights groups thereafter accused each country of retaining and accessing data in the same manner as outlined in the hypothetical above. Indeed, a Committee of Inquiry ("Committee") launched by the European Parliament revealed that Poland, Hungary, Greece, Cyprus, and Spain have used surveillance software to hack the telecommunication records of journalists, political adversaries, and supporters of separatist movements.

Poland announced that it purchased surveillance software in 2017. After purchasing the software, researchers discovered that the country had used it to gain access to and retain data on at least three high-profile individuals, namely Senator Krzysztof Brejza, attorney Roman Giertych, and prosecutor Ewa Wrzosek.[48] Each of the three have frustrated the governing parties' political aims. Senator Brejza, a campaign leader of the opposition party Civic Platform, suffered from spyware attacks until a few days after the end of a national election.[49] Giertych served as Donald Tusk's lawyer during the 2019 campaign when Polish authorities accessed telecommunication data from his phone.[50] Finally, Wrzosek investigated the safety of Presidential elections during COVID when Polish authorities used surveillance software against her.[51]

In Hungary, the government surveilled journalists including Szabolcs Panyi, a journalist at Direkt36, and Zoltan Varga, the CEO of 24.hu, the largest of Hungary's independent news

[47] Draft Report of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware (Nov. 8, 2022) [hereinafter Committee Report], https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf.
[48] *Id.*, par. 49.
[49] *Id.*, par. 51.
[50] *Id.*, par. 56.
[51] *Id.*, par. 59.

sites.[52] Greek officials have used surveillance software against both journalists and opposition politicians—including Thanasis Koukakis, a journalist investigating financial scandals involving the Greek government, and Nikos Androulakis, leader of the minority PASOK-KINAL party.[53] The Committee's report further alleges that Cypriot officials have investigated Makarios Drousiotis, whose inquiries into President Anastasiades' connections with Russian officials may have aroused the Cypriot government's suspicion.[54] In Spain, research by North American nonprofits suggests that the government has used surveillance software to investigate supporters of the Catalan separatist movement.[55]

Notably, the surveillance software crisis is not limited to just these Member States. Evidence suggests that the governments of the Netherlands, Belgium, Germany, Malta, and France may have also used surveillance software against their citizens, but the information available about each Member State's use is less apparent than about those above.[56]

The Committee's draft report largely focuses on whether the Member States' use of surveillance software at present violates EU law. The Committee claims it does.[57] As the CJEU before it, the Committee argues that Member States continuously violate the Charter by retaining, and in some cases, accessing, telecommunications data on political opposition parties.[58] The Committee also argues that any Member State using these software services should

[52] *Id.*, par. 100-101, 104.
[53] *Id.*, par. 175-183, 184-195.
[54] *Id.*, par. 254.
[55] *Id.*, par. 280-282.
[56] *Id.*, par. 306, 310, 312, 318, 324-326.
[57] *Id.*, par. 426-486. The Committee argues that the use of Pegasus software by Member States may violate a host of legal obligations imposed on the Member States including the fundamental rights guaranteed by the Charter, the TEU itself, data and privacy protection laws (discussed in greater detail below), the Law Enforcement Directive (LED), the obligations imposed by the European Convention on Human Rights and the European Court of Human Rights which fall outside the scope of this paper, the Budapest Convention on Cybercrime, and EU procurement laws. Some of the arguments presented, for instance the argument that the use of surveillance software violates the LED is a rather weak argument, and therefore is not addressed here.
[58] *Id.*, par. 427.

point to a "legal act clearly indicating the circumstances under which [spyware surveillance software] may be used and how its use is necessary" to protect national security.[59] This, the Committee argues, would assure Member States' use of such tools complies with the Law Enforcement Directive ("LED").[60] However, this is not necessary for Member States since the CJEU's data privacy jurisprudence has not provided a precise definition of national security and furthermore allows Member States to present claims of national security to domestic courts staffed by judges that favor claims of national security over those of data privacy, thereby operating within the confines of the CJEU's jurisprudence.

The Response to the Surveillance Spyware Crisis

In response to all of the allegations above, Member States contest that, even if they were using surveillance software against individuals—which every state denies—that is their prerogative under Article 4 TEU.[61] As *La Quadrature du Net* declares, this is not so. All decisions regarding data retention are reviewable under EU law.[62] If Member States' decisions are challenged, they must contend that their activities protect national security and then present their arguments to domestic courts meeting the criteria established in *HK*.[63]

---

[59] *Id.*, par. 438

[60] The EU passed the Law Enforcement Directive (LED) parallel to the General Data Privacy Regulation (GDPR). The LED stipulates the requirements that law enforcement officers must meet when processing personal data for purposes of law enforcement which fall outside of the scope of the GDPR.

[61] *See* Shaun Walker, *Viktor Orbán using NSO Spyware in assault on media, data suggests,* THE GUARDIAN, Jul. 18, 2021; *Hungarian prosecutors drop probe into Pegasus spyware*, DAILY NEWS HUNGARY, Jun. 15, 2022; Michalis Hariatis, *ND for investigation: The opposition's complaint collapsed*, IEIDISEIS, Oct. 10, 2022. Importantly, in the context of the surveillance spyware crisis, Member States do not cede that they have spied on particular civilians.

[62] *La Quadrature du Net*, ¶ 67. The CJEU notes that the referring court indicates the reviewability of any action taken by a state that retains data over its civilians.

[63] *Id.*, ¶ 120. *See also* Valsamis Mitsilegas, Elspeth Guild, Elif Kuskonmaz, Niovi Vavoula, *Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks*, EUR. LAW J. 1, 15 (2022) (discussing the requirements that *La Quadrature du Net* imposed on domestic courts and tribunals and how they extend to *HK*).

If a Member State were sued for its alleged used of spyware surveillance, it might plausibly argue that retaining data about specific political adversaries is necessary because such adversaries' activities constitute a genuine and imminent threat to the "essential functions of the state."[64] A Member State might support this argument by contending that political adversaries pose a legitimate threat to the essential elements of a Member State by creating political disarray within the Member State. While this is a colorable argument, a judge that did not favor national security claims over privacy claims would likely reject it. However, *La Quadrature du Net* incentivizes Member States to select judges that are sensitive to national security who very well may defer to this line of reasoning.

Even if courts within the Member States were not staffed by judges that favored national security claims over privacy claims, the current intra-State referral system established by *La Quadrature du Net* would lead to the development of twenty seven different definitions of what constitutes national security as opposed to public security. While the Court could refine that definition over time, it would be impracticable in the short-term.

Toward the Future

Despite its well-intentioned efforts, the CJEU's current jurisprudence regarding data retention cannot adequately respond to the surveillance software crisis.

While the requirements the CJEU imposed on Member States in *La Quadrature du Net* seem like an adequate compromise at first glance, in practice, they provide Member States with plenary power to use the term national security as a justification for almost any data retention scheme given the broad definition of national security advanced in *Privacy International*, the blurry line between that which constitutes national security and that which constitutes public

[64] *Privacy International* ¶ 74.

security, and the weak standards imposed on domestic courts in *HK* regarding what amounts to effective judicial review. While the *Privacy International* and *La Quadrature du Net* judgments sought to chart a middle course to protect individuals' privacy and Member States' sovereignty, that course is ineffective in light of the developing surveillance software crisis.

Instead of insisting on compliance with the system of judicial review set forth in its previous jurisprudence, the CJEU should adopt a new system of judicial review. There are two conceivable ways that the CJEU could change its current system of judicial review. First, it could require a supernational court to review whether a particular concern is indeed a matter of national security rather than public security. Second, the CJEU could change the definition regarding what amounts to effective judicial review.

While Article 4(2) TEU states that "national security remains the sole responsibility of each Member State," it does not bestow upon Member States the ability to decide what constitutes a national security concern when doing so would conflict with the fundamental rights guaranteed to persons within the EU.[65] Indeed, the CJEU states as much in *Privacy International* and *La Quadrature du Net*.[66]

The first proposal, that the CJEU require a supernational court to review whether a particular matter is one of national security or public security, is untenable without political support from the legislative bodies of the EU. Article 257 TFEU stipulates that "[t]he European Parliament and the Council . . . may establish specialised courts attached to the General Court to hear and determine at first instance certain classes of action."[67] This plain statement strips the CJEU the ability to create a court *sua sponte* and instead gives that power to the EU legislature.

---

[65] TEU art. 4(2).
[66] *La Quadrature du Net* ¶ 96; *Privacy International* ¶ 39.
[67] Consolidated Version of the Treaty on the Functioning of the European Union, art. 257, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter TFEU].

This is almost always true as a constitutional matter—almost no court has the ability to create inferior courts of its own volition. However, Article 257 does provide the CJEU some rights with respect to creating inferior courts.

Article 257 specifically contemplates that the CJEU may request the EU Commission create specialized courts "to hear and determine at first instance certain classes of action or proceeding brought in specific areas" requiring that the CJEU consult with the EU Commission to propose a court.[68] Theoretically, it would not be difficult for the CJEU and the EU Commissioners to create a new independent court to determine whether Member States' concerns regarding national security are valid since the EU Commissioners, by oath at least, must operate for the benefit of the EU, not their respective Member States. However, Article 257 further notes that "[t]he European Parliament and the Council shall act by means of regulations" on any proposal made by the CJEU and the EU Commissioners. This provision requires the creation of any specialized court to undergo the inherently political legislative process before being established. Given the European Parliament and the Council's inability to pass a new regulation regarding ePrivacy, it seems unlikely that either body would ultimately agree to create such a court.[69] While judicial panels may now be established under the Treaty of Lisbon, those too can only be created by EU legislators. Thus, the CJEU cannot practically require Member States to hear claims before a newly established EU court on its own—and certainly not through its own jurisprudence.

This does not foreclose the CJEU from requiring data retention cases involving Member States to be heard by a pre-existing EU court; however, no preexisting supernational, EU court

[68] *Id.*
[69] JENNIFER BAKER, IAPP, HOW THE EPRIVACY REGULATION TALKS FAILED . . . AGAIN (NOV. 26, 2019) https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/ (explaining how the EU failed to pass the ePrivacy Regulation).

exists whose jurisdiction the CJEU might expand. While the CJEU might try to expand the General Court, the TFEU limits the jurisdiction of the General Court such that it may only hear four types of claims: the legality of acts passed by the EU's legislative bodies and EU agencies, any case brought by a Member State against the EU, disputes between "servants" of the EU and the EU, and any claim arising from an arbitration clause.[70] However, according to the treaty, the General Court does not have original jurisdiction to hear a dispute against a Member State. Moreover, any amendments to the General Court's original jurisdiction must be made by statute from the EU legislative bodies, and not from the CJEU.[71]

Accordingly, the first proposition is untenable without EU legislators' aid. However, the CJEU could instead alter its definition of "effective judicial review." As argued earlier, the "independence test" used by the CJEU is ultimately ineffective, at least in response to the spyware surveillance crisis because it does not meaningfully impose restrictions on states regarding who may be elected as domestic judges. It also does not foreclose Member States from elevating judges to the bench who are biased in favor of finding national security concerns. However, there are other plausible definitions of judicial review. The most obvious contender is that proposed by the European Court of Human Rights ("ECHR")—the establishment test.

The establishment test considers a host of different factors that are not considered by the CJEU's independence test. Rather than looking to external and internal indicia of independence in a particular trial, the establishment test considers whether the court was independent at the moment of the court's establishment. Surprisingly, the CJEU has not adopted this line of reasoning even though it referenced the possibility in *A.K. and others.*[72] Should the CJEU adopt

[70] TFEU, art. 256.
[71] *Id.*
[72] *A.K. and others* ¶ 126.

this test in relation to domestic courts considering data privacy matters, it would allow the CJEU to determine that a court does not comply with EU law if the judge, when appointed, expressed any personal prejudice or bias regarding the subject matter of the dispute. In this way, the CJEU could find that a judge who favored the Member State routinely in data retention matters even before being elevated to an appropriate domestic court, was not in compliant with EU law.

Finally, the CJEU could adopt a more particularized definition of national security. While the CJEU made a first effort at defining national security in the context of data privacy in *Privacy International*—the definition offered does not practically restrict Member States. Rather than claiming that national security only concerns activities that threaten the essential functions of the state, the CJEU might take the next step of describing what those activities might be. While the court has already specified that terrorist activities might constitute national security concerns, it could add the other most common types of threats that nations refer to as national security threats. In the context of data privacy, which would include widespread financial fraud, threat of deadly force against a state official, and protection against foreign threats. By imposing a limited definition, the EU might plausibly reduce Member State's capacity to argue that using spyware surveillance technology against individual prosecutors is intended to protect national security.

Criticisms

Member States have critiqued all of these proposals in CJEU case law before by urging that they have an unparalleled right to protect national security under Article 4(2) TFEU. Of course, the CJEU has rejected this argument. However, Member States might also argue that implicit in that right is the ability to decide what threatens national security. Yet, the veracity of the latter statement has not been clarified by the CJEU's case law. *Tele2 Sverige* indicated that

the Member States' rights in determining national security generally were limited when it held that the EU's right to practice national security was constrained by the Charter, which underpins the structure of the EU itself.[73] As indicated above, the *La Quadrature du Net* court further implied that Member States might not be able to decide what may be deemed national security as opposed to public security by indicating that Member States have different rights depending on the nature of the conflict concerned. Accordingly, even though the case law is silent as to this particular issue, the most recent cases in the CJEU's jurisprudence suggest that the Court may inhibit the Member States' ability to determine what amounts to a national security concern in the context of data privacy.

Nevertheless, there might be deleterious political consequences if the CJEU were to institute such a ruling. Indeed, some academics suggest that one of the reasons the CJEU reversed course in *La Quadrature du Net* is because the restrictive rulings in its previous case law proved too politically onerous. Whether that is true or not, and whether the CJEU would consider those consequences in future holdings or not, political consequences resulting from a Court's decision would exist—and, if severe, could threaten the EU itself. That said, limiting Member States' use of national security to justify broad data retention methods probably would not be so severe as to institute a crisis for the European Union. Instead, the most recent EU-wide political crises have stemmed not from data regulation policies, but rather from a general disdain for the EU as an institution[74] and a failure in EU monetary policy.[75]

Other Proposals for Reform

[73] *Tele2 Sverige* ¶ 92.
[74] *See generally* Czech, Sławomir, and Monika Krakowiak-Drzewiecka. "The rationale of Brexit and the theories of European integration." Oeconomia Copernicana 10, no. 4 (2019): 589-602 (describing that Brexit resulted from a failure to integrate the UK into the EU and a growing frustration amongst the UK populace)
[75] *See generally* Arghyrou, Michael G., and John D. Tsoukalas. "The Greek debt crisis: Likely causes, mechanics and outcomes." The World Economy 34, no. 2 (2011): 173-191.

There are of course other proposals for reform. The Committee advances numerous suggestions when recommending EU-wide action to curtail the use of spyware surveillance. Key among these suggestions, the Committee argues that national security services should adopt common standards and a legal framework for the use of spyware.[76] The Committee also argues that a new "ePrivacy Regulation should be adopted as soon as possible and should fully reflect the case law on the restrictions for national security as well as the need to prevent abuse of surveillance technologies"[77] adding that "the new ePrivacy Regulation should strengthen the fundamental right to privacy and its scope for surveillance should not go beyond the ePrivacy Directive."[78]

Commentary Re: Common Standards and Legal Framework for Use of Spyware

The Committee spends several paragraphs arguing in favor of the development of common standards and a unitary legal framework governing the use of spyware. In part, the Committee relies on the European Commission for Democracy through Law's Report on the Democratic Oversight of the Security Services ("Venice Commission Report"). In both the Committee Report and the Venice Commission Report, legislators argue that national security services should be subjected to greater democratic control since those security services at present have no generally agreed upon limitations regarding which authorities may use spyware, for which crimes they may use such spyware, *ex ante* and *ex post* judicial review before using such spyware, and transparency.

While the national security agencies lack limitations, the CJEU has attempted to impose some requirements in its data retention jurisprudence. Yet, even in *La Quadrature du Net*, the

[76] Committee Report, par. 588.
[77] *Id.*, par. 608.
[78] *Id.*

Court recognized its own institutional limitations by only imposing meaningful restrictions on state security services when the activity the agency engages in does not fall within the category of national security.[79] Of course, the Court is not the only body to impose standards on national security services' data retention schemes. Alternatively, EU legislators might seek to draft legislation or Member States could agree to adopt new regulations.

However, these possibilities are also unfeasible. If the Council presented legislation to the European Parliament, few parliamentary members would have an interest in passing legislation that limited Member State's use of spyware and potentially conflicted with the right to national security. Most efforts to curtail national security services has generated fierce criticism from the Member States.[80] For the same reason, Member States are determined not to develop their own standards. Since national security is solely the responsibility of the Member States and curtailing any powers belonging to national security would *ipso facto* curtail State authority, Member States have exhibited no interest in creating standards that restrict them. Accordingly, the development of common standards in response to the surveillance crisis is simply unfeasible.

Commentary Re: ePrivacy Regulation

Since 2017, European legislators have attempted to adopt a new ePrivacy Regulation to act in conjunction with the General Data Privacy Regulation.[81] Like the 2002 ePrivacy Directive,

[79] *La Quadrature du Net* ¶¶ 142-144.
[80] This is particularly true with regards to the proposed ePrivacy Regulation (discussed in greater detail below). The proposed ePrivacy Regulation, which has been inactive since 2017 has not been passed precisely because of Member States' refusal to legislate away what they perceive as fundamental elements of State sovereignty. The debate has shown no sign of abating anytime soon. Indeed, discussion of the ePrivacy Regulation has all but vanished in Brussels' halls.
[81] The General Data Privacy Regulation (GDPR) governs data processing with respect to personal data whereas the ePrivacy Directive and proposed ePrivacy Regulation would govern electronic communications that do not include personal data collection. While the GDPR has a provision relating to national security—Article 48—that Article only pertains to personal data and is not at issue here. That said, the language in Article 48 illustrates the challenges that EU legislators consistently face when trying to hold Member States accountable for concerns regarding national security.

the regulation seeks to increase data protections for individuals and businesses while limiting the exemptions that states might employ.[82] In sum, it would likely make the ePrivacy Directive and elements of the CJEU's case law moot by restricting States' ability to retain data on individuals or persons.[83]

However, actually passing such a regulation that comports with the CJEU's previous caselaw has proven nearly impossible.[84] In 2019, the Council of the EU reported that "[a]fter two years of work in the [Working Party on Information Exchange and Data Protection], no solution has yet been found on how to implement a targeted/restricted retention."[85] While the Council made this statement prior to the CJEU's decisions in *Privacy International* and *La Quadrature du Net*, little has changed since. Indeed, the ePrivacy Regulation still sits in committee with the Council of the EU.

Despite the CJEU's recent rulings, the ePrivacy Regulation remains in a political quagmire. As argued above, most Member States think the proposed regulations far too restrictive, but a few leaders deem its provisions not restrictive enough. The German Federal Commissioner for Data Protection and Freedom of Information ("BfDI"), Professor Ulrich, views the proposed ePrivacy Regulation as a failure by virtue of the fact that it permits "cookie walls" and continues to allow Member States to access data without users' consent. Professor Ulrich argued that "if the ePrivacy Regulation remains as the EU Council decided on it [on

[82] Note that, unlike the ePrivacy Directive, the proposed regulation would not require the States to pass implementing legislation.
[83] EUROPEAN DATA PROTECTION BOARD, STATEMENT OF THE EDPB ON THE REVISION OF THE EPRIVACY REGULATION AND ITS IMPACT ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PRIVACY AND CONFIDENTIALITY OF THEIR COMMUNICATIONS, https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf
[84] 'The issue of data retention in the proposal for ePrivacy Regulation - discussion paper', Council of the European Union (14 February 2019), 6358/19.
[85] *Id.* p. 3.

February 10, 2021], that would be a serious blow to data protection."[86] He added that "If there are no significant improvements to the regulation during the trilogue negotiations, several red lines would be crossed simultaneously in the area of data protection."[87] It seems that the proposed ePrivacy Regulation, in the end, pleases no one.

Conclusion

The surveillance spyware crisis exposes some of the flaws inherent in the logic that the CJEU presented in its data privacy jurisprudence. Notably, the surveillance spyware crisis demonstrates that *La Quadrature du Net* and its predecessors provide Member States with plenary power to use the term national security as a justification for almost any data retention scheme because the definition of national security advanced in *Privacy International* is overly broad. Moreover, the blurry line between that which constitutes national security and that which constitutes public security makes it easy for Member States to claim that they seek to protect the former whenever they choose. Finally, the relaxed standards imposed on domestic courts in *HK* regarding what amounts to effective judicial review allow Member States to refer cases weighing data privacy and national security to courts that are partial to the latter.

Even though the surveillance spyware crisis has not created any litigation before the CJEU yet, it very well may, given the public's interest in the case, the details known about victims of the surveillance spyware crisis, and the impending litigation before national courts. Already, at least six lawsuits have been filed by plaintiffs allegedly harmed by spyware surveillance software, namely Pegasus, in Spain alone.[88] In France, Poland, and Hungary,

[86] Der Bundesbeauftragte für den Datenschutz unc die Informationsfreiheit Pressemitteilung, 3/2021, BfDI kritisiert Position des Rats zur ePrivacy-Verordnung (February 10, 2021).
[87] *Id.*
[88] SIENA ANSTIS, THE CITIZEN LAB, LITIGATION AND OTHER FORMAL COMPLAINTS CONCERNING TARGETED DIGITAL SURVEILLANCE AND THE DIGITAL SURVEILLANCE INDUSTRY (database updated on Dec. 7, 2022).

another seven lawsuits have been filed claiming that plaintiffs have been injured by their respective Member States' use of spyware.[89] While these mattesr have been filed against the software companies themselves, its plausible that future litigation will involve the Member States themselves. If any such cases are presented to the CJEU, the Court must alter its existing jurisprudence so as to better protect civilians operating under EU law.

[89] *Id.*