Stanford – Vienna
Transatlantic Technology Law Forum

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

TTLF Working Papers

No. 99

Key Legal Issues of the EU's New U.S. Data Protection Adequacy Decision

Mikołaj Barczentewicz

2023

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work 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 TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

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

Dr Mikołaj Barczentewicz is a Senior Lecturer (Associate Professor) in Public Law and Legal Theory at the University of Surrey School of Law (UK), as well as the Research Director of the Surrey Law and Technology Hub. He is also a Research Associate at the University of Oxford (UK), a Fellow of the Stanford Law School and University of Vienna Transatlantic Technology Law Forum, as well as a Senior Scholar at the International Center for Law & Economics.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Mikołaj Barczentewicz, Key Legal Issues of the EU's New U.S. Data Protection Adequacy Decision, Stanford-Vienna TTLF Working Paper No. 99, http://ttlf.stanford.edu.

Copyright

Abstract

Since the *Schrems II* decision of the EU Court of Justice (CJEU), lawfulness of transfers of personal data from the EU to the U.S. has been in a precarious position. Aiming to address this situation, the U.S. adopted a new data protection framework for its intelligence collection activities. The European Commission responded by preparing a draft "Adequacy Decision" for the U.S. under Article 45(3) of the General Data Protection Regulation (GDPR). The purpose of this paper is to present and discuss the key legal issues of the European Commission's draft Adequacy Decision, which are likely to be the subject of litigation, if the Commission adopts the Decision. I begin, in Section 2, by problematizing the issue of the applicable legal standard of an "adequate level of protection" of personal data in a third country, noting that this issue remains largely open for the CJEU to address. This makes it more difficult to assess the chances of the draft Adequacy Decision before the Court and suggests that the conclusive tone adopted by some commentators is premature. I then turn, in Section 3, to the question of proportionality in relation to bulk data collection by the U.S. government. I consider the question whether the objectives for which U.S. intelligence agencies collect personal data may constitute "legitimate objectives" under EU law. Secondly, I discuss whether bulk collection of personal data may be done in a way that does not jeopardize adequacy under the GDPR. Section 4 is devoted to the problem of effective redress, which was the key issue that the Court relied on in making its *Schrems II* decision. I note some confusion among the commentators about the precise role of Article 47 of the EU Charter of Fundamental Rights for a third-country adequacy assessment under the GDPR. I then outline the disagreement between the Commission and some of the commentators on the question whether the new U.S. data protection framework provides redress through an independent and impartial tribunal with binding powers. Finally, I discuss the issue of access to information about data processing by U.S. intelligence agencies.

TABLE OF CONTENTS

1. Introduction[1]

Since the *Schrems II* decision of the EU Court of Justice (CJEU),[2] lawfulness of transfers of personal data from the EU to the U.S. has been in a precarious position. True, there have been changes in U.S. intelligence collection rules and practice since the state of the matter in 2016 which was the basis of the European Commission's assessment in the "Privacy Shield Decision" and to which facts the CJEU limited its reasoning. However, there has also been a vocal movement among NGOs, European politicians and - recently - national data protection authorities, to treat *Schrems II* as if it conclusively decided that exports of personal data to the U.S. cannot be justified through standard contractual clauses ("SCC") in most contexts (i.e., when data can be accessed in the U.S.). The latter interpretation has now led to a series of

[1] This paper builds on the author's previous short form publications published on *Truth on the Market*.

[2] Case C-311/18, Data Protection Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, ECLI:EU:C:2019:1145 (CJ, Jul. 16, 2020), *available at* http://curia.europa.eu/juris/liste.jsf?num=C-311/18 [hereinafter "Shrems II"].

enforcement actions by national authorities in Austria, France and likely in several other member states ("Google Analytics" cases).[3]

Aiming to address this precarious situation, the U.S. adopted a new data protection framework for its intelligence collection activities. On Oct. 7, 2022, President Biden signed a new Executive Order[4] which had been awaited since March 2022, when U.S. and EU officials reached an agreement in principle on a new data privacy framework.[5] The European Commission responded by preparing a draft "Adequacy Decision" for the U.S. under Article 45(3) of the General Data Protection Regulation (GDPR), which was released on Dec. 13, 2022.[6] An adequacy decision will remove the need for the current workarounds (especially the SCC-s) used by businesses to be able to transfer personal data between the EU and the U.S. Like the previous U.S.-EU arrangements, this one is nearly certain to be challenged before the EU courts.

The purpose of this paper is to present and discuss the key legal issues of the European Commission's draft Adequacy Decision, which are likely to be the subject of litigation, if the Commission adopts the Decision. I begin, in Section 2, by problematizing the issue of the applicable legal standard of an "adequate level of protection" of personal data in a third country, noting that this issue remains largely open for the CJEU to address. This makes it more difficult to assess the chances of the draft Adequacy Decision before the Court and suggests that the

[3] *See, e.g.,* Caitlin Fennessy, "The Austrian Google Analytics decision: The race is on", IAPP PRIVACY PERSPECTIVES (Feb. 7, 2022) https://iapp.org/news/a/the-austrian-google-analytics-decision-the-race-is-on/; "Italian SA bans use of Google Analytics: No adequate safeguards for data transfers to the USA" (Jun. 23, 2022), https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782874.

[4] Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, (2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

[5] "European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework" (Mar. 25, 2022), https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087.

[6] European Commission, *Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, (2022), https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf.

conclusive tone adopted by some commentators is premature. I then turn, in Section 3, to the question of proportionality in relation to bulk data collection by the U.S. government. I consider the question whether the objectives for which U.S. intelligence agencies collect personal data may constitute "legitimate objectives" under EU law. Secondly, I discuss whether bulk collection of personal data may be done in a way that does not jeopardize adequacy under the GDPR. Section 4 is devoted to the problem of effective redress, which was the key issue that the Court relied on in making its *Schrems II* decision. I note some confusion among the commentators about the precise role of Article 47 of the EU Charter of Fundamental Rights for a third-country adequacy assessment under the GDPR. I then outline the disagreement between the Commission and some of the commentators on the question whether the new U.S. data protection framework provides redress through an independent and impartial tribunal with binding powers. Finally, I discuss the issue of access to information about data processing by U.S. intelligence agencies.

2. The Applicable Legal Standard: What Does "Adequacy" Mean?

The overarching legal question that the CJEU will likely need to answer is whether the United States "ensures an adequate level of protection for personal data essentially equivalent to that guaranteed in the European Union by the GDPR, read in the light of Articles 7 and 8 of the [EU Charter of Fundamental Rights]."[7] The words "essentially equivalent" are not to be found in the GDPR's provision on adequacy decisions, i.e. in its Article 45, which merely refers to an "adequate level of protection" of personal data in a third country. Instead, we find them in the GDPR's recital 104: "[t]he third country should offer guarantees ensuring an adequate level

[7] *Shrems II* [178].

of protection essentially equivalent to that ensured within the Union (…)". This phrasing goes back to the CJEU's *Schrems I* decision,[8] where the Court interpreted the old Data Protection Directive (Directive 95/46).[9] In *Schrems I*, the Court stated:

> The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.[10]

As Christakis, Propp, and Swire note,[11] the key point that "a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order" was also accepted by the Advocate General Øe in *Schrems II*.[12]

The European Data Protection Board issued Recommendations "on the European Essential Guarantees for surveillance measures".[13] The aim of the Recommendations is to "form part of

[8] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, EU:C:2015:650 (CJEU judgment of 6 October 2015) [hereinafter: "Schrems I"].

[9] 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 ("Data Protection Directive").

[10] *Schrems I* [73].

[11] Theodore Christakis, Kenneth Propp & Peter Swire, *EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an "Essentially Equivalent" Solution*, EUROPEAN LAW BLOG (2022), https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution/.

[12] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2019:1145 [248].

[13] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (hereinafter: "EDPB Recommendations").

the assessment to conduct in order to determine whether a third country provides a level of protection essentially equivalent to that guaranteed within the EU."[14] The EDPB's document is, of course, not a source of law binding the Court of Justice, but it attempts to interpret the law in the light of the CJEU's jurisprudence. The Court is free to disregard the EDPB's legal interpretation and thus the importance of the Recommendations should not be overstated, neither in favour, nor against the draft Adequacy Decision.

Though we know that the "adequate level" and "essential equivalence" of protection do not necessarily mean identical protection, the precise degree of flexibility remains an open question, and one that the EU Court may need to clarify to a much greater extent.

3. Proportionality and Bulk Data Collection

Under Article 52(1) of the EU Charter of Fundamental Rights, restrictions of the right to privacy must meet several conditions. They must be "provided for by law" and "respect the essence" of the right. Moreover, "subject to the principle of proportionality, limitations may be made only if they are necessary" and meet one of the objectives recognized by EU law or "the need to protect the rights and freedoms of others."

The new U.S. executive order supplemented the phrasing "as tailored as possible" present in 2014's Presidential Policy Directive on Signals Intelligence Activities (PPD-28) with language explicitly drawn from EU law: mentions of the "necessity" and "proportionality" of signals-intelligence activities related to "validated intelligence priorities." The executive order expressly states that:

[14] EDPB Recommendations [8].

> … signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.[15]

However, doubts have been raised as to whether this is sufficient. In this section, I consider two potential issues. First, whether the objectives for which U.S. intelligence agencies collect personal data may constitute "legitimate objectives" under EU law. Second, whether bulk collection of personal data may be done in a way that does not jeopardise adequacy under the GDPR.

3.1. Legitimate objectives

In his analysis of the adequacy of the new U.S. data protection framework with EU law, Douwe Korff argued that:

> The purposes for which the Presidential Executive Order allows the use of signal intelligence and bulk data collection capabilities are clearly not limited to what the EU Court of Justice regards as legitimate national security purposes.[16]

Korff's concern is that the legitimate objectives listed in the executive order are too broad and that they could be interpreted to include, e.g., criminal or economic threats, which do not rise to the level of "national security" as defined by the CJEU.[17] Korff refers here to the EDPB

[15] Executive Order, *supra* note 4, Sec. 2(a)(ii)(B).

[16] Douwe Korff, *The inadequacy of the October 2022 new US Presidential Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities*, 13 (2022), https://www.ianbrown.tech/2022/11/11/the-inadequacy-of-the-us-executive-order-on-enhancing-safeguards-for-us-signals-intelligence-activities/.

[17] *Id.* at 10–13.

Recommendations, which in turn reference CJEU decisions in *La Quadrature du Net* and *Privacy International*. However, unlike Korff, the EDPB stresses that those CJEU decisions were given "in relation to the law of a Member State and not to a third country law."[18] In contrast, in *Schrems II*, the Court did not consider the question what objectives can be legitimate when assessing whether a third country provides adequate protection. In its Recommendations, the EDPB discussed the legal material that was available, i.e., the CJEU decisions on intra-EU matters, but this approach can be taken too far if not done with sufficient care. In other words, there is a risk of falling prey to a kind of a legal version of an "availability bias." However, just because some guidance is available (on intra-EU matters), it does not follow that this guidance is applicable in this foreign context. It is instructive to consider in this context what Advocate General Øe said in *Schrems II*:

> It also follows from that judgment [*Schrems I* – MB], in my view, that the law of the third State of destination may reflect its own scale of values according to which the respective weight of the various interests involved may diverge from that attributed to them in the EU legal order. Moreover, the protection of personal data that prevails within the European Union meets a particularly high standard by comparison with the level of protection in force in the rest of the world. The 'essential equivalence' test should therefore in my view be applied in such a way as to preserve a certain flexibility in order to take the various legal and cultural traditions into account. That test implies, however, if it is not to be deprived of its substance, that certain minimum safeguards and general requirements for the protection of fundamental rights that follow from the Charter and the ECHR have an equivalent in the legal order of the third country of destination.[19]

[18] EDPB Recommendations [34].

[19] Opinion of Advocate General Saugmandsgaard Øe in *Schrems II* [249].

The right approach under Article 45 GDPR is not to focus exclusively on what the EU law requires *within the EU*, however convenient this method may be, given the existence of legal material to draw on.

Aside from the lack of direct guidance on how to approach the question of legitimate objectives under Article 45 GDPR, there is a second reason not to be too quick to conclude that the U.S. framework fails on this point. As the Commission noted in the draft Adequacy Decision:

> (…) the legitimate objectives laid down in EO 14086 cannot by themselves be relied upon by intelligence agencies to justify signals intelligence collection but must be further substantiated, for operational purposes, into more concrete priorities for which signals intelligence may be collected. In other words, actual collection can only take place to advance a more specific priority. Such priorities are established through a dedicated process aimed at ensuring compliance with the applicable legal requirements, including those relating to privacy and civil liberties.[20]

It may be a formalistic mistake to consider the list of "legitimate objectives" in isolation from such additional requirements and process. The assessment of third country adequacy cannot be constrained by the mere choice of words, even if they seem to correspond to an established concept in EU law. (Note that this applies also to "necessity" and "proportionality" as used in the Executive Order.)

[20] European Commission, *supra* note 6 at [129].

3.2. Can bulk collection be "adequate"?

As Max Schrems' organisation NOYB stated in response to the publication of the executive order:

> (…) there is no indication that US mass surveillance will change in practice. So-called "bulk surveillance" will continue under the new Executive Order (see Section 2 (c)(ii)) and any data sent to US providers will still end up in programs like PRISM or Upstream, despite of the CJEU declaring US surveillance laws and practices as not "proportionate" (under the European understanding of the word) twice.[21]

Korff echoed this view, noting e.g.:

> (…) - the EO [executive order – MB] does not stand in the way of the indiscriminate bulk collection of e- communications content data that the EU Court held does not respect the "essence" of data protection and privacy and that therefore, under EU law, must always be prohibited, even in relation to national security issues (as narrowly defined);
>
> - the EO allows for indiscriminate bulk collection of e-communications metadata outside of the extreme scenarios in which the EU Court only, exceptionally, allows it in Europe; and

[21] NOYB, "New US Executive Order unlikely to satisfy EU law" (Oct. 7, 2022), https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law.

> - the EO allows for indiscriminate bulk collection of those and other data for broadly defined not national security-related purposes in relation to which such collection is regarded as clearly not "necessary" or "proportionate" under EU law.[22]

It is true that the *Schrems II* Court held that U.S. law and practices do not "[correlate] to the minimum safeguards resulting, under EU law, from the principle of proportionality."[23] But it is important to note the specific reasons the Court gave for that conclusion. The reasons were that "PPD-28 does not grant data subjects actionable rights before the courts against the US authorities"[24] and that, under Executive Order 12333, "access to data in transit to the United States [is possible] without that access being subject to any judicial review."[25] The issue of bulk collection was not among those reasons.

However, as Korff noted, the CJEU has considered the question of bulk collection of electronic communication data, in an intra-EU context, in cases like *Digital Rights Ireland*[26] and *La Quadrature du Net*.[27] In *Schrems I*, the Court referenced *Digital Rights Ireland* while stating:

> (…) legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (…)[28]

This is potentially important, because the Court concluded the discussion including this paragraph by saying that "a level of protection of fundamental rights essentially equivalent to

---

[22] Korff, *supra* note 16 at 19.

[23] *Schrems II* [184].

[24] *Schrems II* [181].

[25] *Schrems II* [183].

[26] Digital Rights Ireland and Others, Cases C-293/12 and C-594/12, EU:C:2014:238.

[27] La Quadrature du Net and Others v Premier ministre and Others, Case C-511/18, ECLI:EU:C:2020:791.

[28] *Schrems I* [94].

that guaranteed in the EU legal order" is "apparent in particular from the preceding paragraphs".[29] This could suggest that, like under the Data Protection Directive in *Schrems I*, the Court may see the issue of bulk collection of *contents* of electronic communication as a serious problem for adequacy under Article 45 GDPR.

The Commission addressed this in the draft Adequacy Decision in the following way:

> (…) collection of data within the United States, which is the most relevant for the present adequacy finding as it concerns data that has been transferred to organisations in the U.S., must always be targeted (…) 'Bulk collection' may only apply to data collection that takes place outside the United States, on the basis of EO 12333.[30]

The Commission relies on a distinction between data collection that the U.S. government does *within* the United States and *outside* of the U.S. This likely refers to an argument, discussed e.g. by Christakis,[31] that adequacy assessment should only concern the processing of personal data that takes place due to a data transfer to the country in question. In other words, that it should only concern domestic surveillance, not international surveillance (assuming that personal data transferred from the EU would fall under domestic surveillance in that third country).

The Commission also made a second relevant point:

---

[29] *Schrems I* [96].

[30] European Commission, *supra* note 6 at [134].

[31] Theodore Christakis, *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1)*, EUROPEAN LAW BLOG (2021), https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/; Theodore Christakis, *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)*, EUROPEAN LAW BLOG (2021), https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/.

> (…) bulk collection under EO 12333 takes place only when necessary to advance specific validated intelligence priorities and is subject to a number of limitations and safeguards designed to ensure that data is not accessed on an indiscriminate basis. **Bulk collection is therefore to be contrasted to collection taking place on a generalised and indiscriminate basis ('mass surveillance') without limitations and safeguards**.[32]

On the Commission's view, there is a categorical distinction between "bulk collection" as practiced by the U.S. and the kind of "generalised and indiscriminate" mass surveillance that the CJEU scrutinised in *Digital Rights Ireland* and other cases. This may seem like an unnatural reading of "generalised and indiscriminate", given that it is meant *not* to apply to "the collection of large quantities of signals intelligence that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms)."[33] However, there may be analogies in EU law that could lead the Court to agree with the Commission on this point.

Consider the Court's interpretation of the prohibition on "general monitoring" obligations from Article 15(1) of the eCommerce Directive.[34] In *Glawischnig-Piesczek*, the Court interpreted this rule as not precluding Member States to require hosting providers to monitor all the content they host in order to identify content identical to "the content of information which was previously declared to be unlawful."[35] In other words, "general monitoring", was interpreted as *not* covering indiscriminate processing of all data

[32] European Commission, *supra* note 6 at [134] footnote 223 (emphasis added).

[33] *Id.* at [134] footnote 223.

[34] Directive (EU) 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1.

[35] Case C-18/18, Eva Glawischnig-Piesczek v Facebook [2019] ECLI:EU:C:2019:821. *See also* Daphne Keller, *Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling*, 69 GRUR INTERNATIONAL 616 (2020).

stored by a hosting provider in order to find content identical to some other content.[36] The Court adopted an analogous approach in respect to Article 17 of the Copyright Directive.[37] This suggests that, in somewhat similar contexts, the Court is willing to see activities that may technically seem general, as not general if some procedural or substantive limitations are present.

4. Effective Redress

The issue of the lack of effective redress available to EU citizens against potential restrictions of their right to privacy from U.S. intelligence activities was central to the *Schrems II* decision. As I noted earlier, the Court's key findings were that "PPD-28 does not grant data subjects actionable rights before the courts against the US authorities"[38] and that, under Executive Order 12333, "access to data in transit to the United States [is possible] without that access being subject to any judicial review."[39]

The new executive order introduced redress mechanisms that include creating a civil-liberties-protection officer in the Office of the Director of National Intelligence (DNI), as well as a new Data Protection Review Court (DPRC). The DPRC is proposed as an independent review body that will make decisions that are binding on U.S. intelligence agencies. The old framework had sparked concerns about the independence of the DNI's ombudsperson, and what was seen as

[36] As Keller puts it: "Instead of defining prohibited 'general' monitoring as *monitoring that affects every user*, the Court effectively defines it as *monitoring for content that was not specified in advance by a court*." *Id.* at 620.

[37] Case C-401/19, Poland v Parliament and Council [2022] ECLI:EU:C:2022:297; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ 2019 L 130, p. 92). For the background, *see* Christophe Geiger & Bernd Justin Jütte, *Platform Liability Under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match*, 70 GRUR INTERNATIONAL 517 (2021).

[38] *Schrems II* [181].

[39] *Schrems II* [183].

insufficient safeguards against external pressures that individual could face, including the threat of removal. Under the new framework, the independence and binding powers of the DPRC are grounded in regulations issued by the U.S. Attorney General.

In a comment pre-dating the executive order, Max Schrems argued that:

> It is hard to see how this new body would fulfill the formal requirements of a court or tribunal under Article 47 CFR, especially when compared to ongoing cases and standards applied within the EU (for example in Poland and Hungary).[40]

4.1. Article 47 of the Charter "contributes" to the benchmark level of protection

Schrems' comment raises two distinct issues. First, Schrems seems to suggest that an adequacy decision can only be granted if the available redress mechanism *satisfies* the requirements of Article 47 of the Charter of Fundamental Rights.[41] But this is a hasty conclusion. The CJEU's phrasing in *Schrems II* is more cautious:

> …Article 47 of the Charter, which also contributes to the required level of protection in the European Union, compliance with which must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of the GDPR.[42]

---

[40] Max Schrems, „Open Letter on the Future of EU-US Data Transfers" (May 23, 2022), https://noyb.eu/en/open-letter-future-eu-us-data-transfers.

[41] Similar phrasing can be found in Ashley Gorski, *The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance*, JUST SECURITY (2022), https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/. Gorski's text shows well how easy it is to elide, even unintentionally, the distinction between the Article 47 being a standard that must be *satisfied* by a third country, and it merely *contributing* to the level of protection that constitutes a benchmark for an adequacy assessment. At one point she notes that "the CJEU held that U.S. law failed to provide an avenue of redress 'essentially equivalent' to that required by Article 47". However, in other places she adopts the phrasing of "satisfying" Article 47.

[42] *Schrems II* [186].

In arguing that Article 47 "also contributes to the required level of protection," the Court is not saying that it *determines* the required level of protection. This is potentially significant, given that the standard of adequacy is "essential equivalence," not that it be procedurally and substantively identical. Moreover, the Court did not say that the Commission must determine compliance with Article 47 itself, but with the "required level of protection" (which, again, must be "essentially equivalent"). Hence, contrary to the certainty exhibited by some of the commentators, it is far from clear how the CJEU's jurisprudence interpreting Article 47 is to be applied in the context of an adequacy assessment under Article 45 GDPR.

4.2. Is there an independent and impartial tribunal with binding powers?

Second, there is the related but distinct question of whether the redress mechanism is effective under the applicable standard of "required level of protection." Christakis, Propp, and Swire offered a helpful analysis suggesting that it is, considering the proposed DPRC's independence, effective investigative powers, and authority to issue binding determinations.[43] Gorski and Korff argued that this is not the case, because the DPRC is not "wholly autonomous" and "free from hierarchical constraint."[44]

The Commission stated in the draft Adequacy Decision that the available avenues of redress "allow individuals to have access to their personal data, to have the lawfulness of government access to their data reviewed and, if a violation is found, to have such violation remedied, including through the rectification or erasure of their personal data."[45] Moreover:

[43] Theodore Christakis, Kenneth Propp & Peter Swire, *The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC*, IAPP.ORG (2022), https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/.

[44] Gorski, *supra* note 41; Korff, *supra* note 16 at 21.

[45] European Commission, *supra* note 6 at [167].

> (…) the executive branch (the Attorney General and intelligence agencies) are barred from interfering with or improperly influencing the DPRC's review. The DPRC itself is required to impartially adjudicate cases and operates according to its own rules of procedure (adopted by majority vote) (…)[46]

Likely the most serious objection to this assessment raised by Gorski is that:

> (…) the court's decisions can be overruled by the President. Indeed, the President could presumably overrule these decisions in secret, since the court's opinions are not issued publicly.[47]

Given that Christakis, Propp, and Swire seem to disagree,[48] this question of U.S. law may require further scrutiny. However, even if the scenario sketched by Gorski is theoretically possible, the CJEU may take a view that it would not be appropriate to rule based on an assumption that the U.S. government would act to mislead the EU. And without that assumption, then the possibility of a future change of U.S. law seems to be adequately addressed by the adequacy monitoring process (Article 45(4) GDPR).

4.3. Access to information about data processing

Finally, Schrems' NOYB raised a concern that "judgment by 'Court' [is] already spelled out in Executive Order."[49] This concern seems to be based on the view that a decision of the DPRC ("the judgment") and what the DPRC communicates to the complainant are the same thing. Or

---

[46] *Id.* at [179].

[47] Gorski, *supra* note 41.

[48] According to them: "(…) key U.S. Supreme Court decisions have affirmed the binding force of a DOJ regulation and the legal conclusion that all of the executive branch, including the president and the attorney general, are bound by it." Christakis, Propp, and Swire, *supra* note 43.

[49] NOYB, *New US Executive Order unlikely to satisfy EU law* (Oct. 7, 2022), https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law.

in other words, that legal effects of a DPRC decision are exhausted by providing the individual with the neither-confirm-nor-deny statement set out in Section 3 of the executive order. This is clearly incorrect: the DPRC has power to issue binding directions to intelligence agencies. The actual binding determinations of the DPRC are not predetermined by the executive order, only the information to be provided to the complainant is. Relatedly, Korff argued that:

> (…) the meaningless "boilerplate" responses that are spelled out in the rules also violate the principle, enshrined in the ECHR and therefore also applicable under the Charter, that any judgment of a court must be "pronounced publicly". The "boilerplate" responses, in my opinion, do not constitute the "judgment" reached (…)[50]

Here, like before, Korff seems to elide the issue raised by the question of the legal standard of "adequacy", directly applying to a third country what he argues is required under the European Convention of Human Rights and thus under the EU Charter.

However, the issues of access to information and data may call for closer consideration. For example, in *La Quadrature du Net,* the CJEU looked at the difficult problem of notification of persons whose data has been subject to state surveillance, requiring individual notification "only to the extent that and as soon as it is no longer liable to jeopardise" the law-enforcement tasks in question.[51] Given the "essential equivalence" standard applicable to third-country adequacy assessments, however, it does not automatically follow that individual notification is required in that context.

Moreover, it also does not necessarily follow that adequacy requires that EU citizens have a right to access the data processed by foreign government agencies. The fact that there are

[50] Korff, *supra* note 16 at 25.

[51] Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, ECLI:EU:C:2020:791 [191].

significant restrictions on rights to information and to access in some EU member states,[52] though not definitive (after all, those countries may be violating EU law), may be instructive for the purposes of assessing the adequacy of data protection in a third country, where EU law requires only "essential equivalence."

5. Conclusion

With the draft Adequacy Decision, the European Commission announced it has favorably assessed the executive order's changes to the U.S. data-protection framework, which apply to foreigners from friendly jurisdictions (presumed to include the EU). If the Commission formally adopts an adequacy decision, however, the decision is certain to be challenged before the CJEU by privacy advocates. As I discussed it above, the key legal concerns are likely to be proportionality of data collection and availability of effective redress.

Opponents of granting an adequacy decision tend to rely on an assumption that a finding of adequacy requires virtually identical substantive and procedural privacy safeguards as required within the EU. As noted by the European Commission in the draft decision, this position is not well-supported by CJEU case law, which clearly recognizes that only "adequate level" and "essential equivalence" of protection are required from third-party countries under the GDPR. To date, the CJEU has not had to specify in greater detail precisely what, in their view, these provisions mean. Instead, the Court has been able simply to point to certain features of U.S. law and practice that were significantly below the GDPR standard (*e.g.*, that the official

[52] European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update* (2017) https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu.

responsible for providing individual redress was not guaranteed to be independent from political pressure). Future legal challenges to a new Adequacy Decision will most likely require the CJEU to provide more guidance on what "adequate" and "essentially equivalent" mean.

In the draft decision, the Commission carefully considered the features of U.S. law and practice that the Court previously found inadequate under the GDPR. Nearly half of the explanatory part of the decision is devoted to "access and use of personal data transferred from the [EU] by public authorities in the" United States, with the analysis grounded in CJEU's *Schrems II* decision. The Commission concludes that, collectively, all U.S. redress mechanisms available to EU persons:

> …allow individuals to have access to their personal data, to have the lawfulness of government access to their data reviewed and, if a violation is found, to have such violation remedied, including through the rectification or erasure of their personal data.

The Commission accepts that individuals have access to their personal data processed by U.S. public authorities, but clarifies that this access may be legitimately limited—*e.g.*, by national-security considerations. Unlike some of the critics of the new executive order, the Commission does not take the simplistic view that access to personal data must be guaranteed by the same procedure that provides binding redress, including the Data Protection Review Court. Instead, the Commission accepts that other avenues, like requests under the Freedom of Information Act, may perform that function.

Overall, the Commission presents a sophisticated, yet uncynical, picture of U.S. law and practice. The lack of cynicism, *e.g.*, about the independence of the DPRC adjudicative process, will undoubtedly be seen by some as naïve and unrealistic, even if the "realism" in this case is based on speculations of what might happen (*e.g.*, secret changes to U.S. policy), rather than evidence. The CJEU will likely be invited by litigants to assume that the U.S. government

cannot be trusted and that it will attempt to mislead the European Commission and thus undermine the adequacy monitoring process (Article 45(3) GDPR). However, it is not clear that the Court will be willing to go that way, not least due to respect for the principle of comity in international law.