International Center for Law & Economics

Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States

Mikołaj Barczentewicz

ICLE Issue Brief 2023-09-25

laweconcenter.org | icle@laweconcenter.org
1104 NW 15th Ave. Ste 300 Portland, OR 97209

@laweconcenter
503.770.0076

Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States

September 2023

Mikołaj Barczentewicz[1]

Executive Summary

The EU Court of Justice's (CJEU) July 2020 *Schrems II* decision generated significant uncertainty, as well as enforcement actions in various EU countries, as it questioned the lawfulness of transferring

[1] Mikołaj Barczentewicz is a senior scholar with the International Center for Law & Economics (ICLE); associate professor of law and research director of the Law and Technology Hub at the University of Surrey School of Law; and a research associate at the University of Oxford. This text builds on and updates the earlier working paper, *Key Legal Issues of the EU's New U.S. Data Protection Adequacy Decision*, STANFORD LAW SCHOOL TTLF WORKING PAPERS (2023), https://law.stanford.edu/publications/no-99-key-legal-issues-of-the-eus-new-u-s-data-protection-adequacy-decision.

data to the United States under the General Data Protection Regulation (GDPR)[2] while relying on "standard contractual clauses."

President Joe Biden signed an executive order in October 2022 establishing a new data-protection framework to address this uncertainty. The European Commission responded in July 2023 by adopting an "Adequacy Decision" under Article 45(3) of the GDPR, formally deeming U.S. data-protection commitments to be adequate.

A member of the French Parliament has already filed the first legal challenge to the Adequacy Decision and another from Austrian privacy activist Max Schrems is expected soon.

This paper discusses key legal issues likely to be litigated:

1. The legal standard of an "adequate level of protection" for personal data. Although 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 that the EU Court may need to clarify to a much greater extent.

2. The issue of proportionality of "bulk" data collection by the U.S. government. It examines whether the objectives pursued can be considered legitimate under EU law and, if so, whether the existing CJEU precedents preclude such collection from being considered proportionate under the GDPR.

3. The problem of effective redress—a cornerstone of the *Schrems II* decision. This paper explores debates around Article 47 of the EU Charter of Fundamental Rights, whether the new U.S. framework offers redress through an impartial tribunal, and whether EU persons can effectively access the redress procedure.

4. The issue of access to information about U.S. intelligence agencies' data-processing activities.

I. Introduction

Since the EU Court of Justice's (CJEU) *Schrems II* decision,[3] it has been precarious whether transfers of personal data from the EU to the United States are lawful. It's true that U.S. intelligence-collection rules and practices have changed since 2016, when the European Commission issued its

[2] Regulation (EU) 2016/679 (General Data Protection Regulation).

[3] 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 "*Schrems II*"].

assessment in the "Privacy Shield Decision" and to which facts the CJEU limited its reasoning. There has, however, 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 United States could not be justified through standard contractual clauses ("SCC") in most contexts (*i.e.*, when data can be accessed in the United States). This interpretation has now led to a series of enforcement actions by national authorities in Austria, France, and likely in several other member states (notably in the "Google Analytics" cases, as well as the French "Doctolib/Amazon Web Services" case).[4]

Aiming to address this precarious situation, the White House adopted a new data-protection framework for intelligence-collection activities. On Oct. 7, 2022, President Joe Biden signed an executive order codifying that framework,[5] which had been awaited since U.S. and EU officials reached an agreement in principle on a new data-privacy framework in March 2022.[6] The European Commission responded by preparing a draft "Adequacy Decision" for the United States under Article 45(3) of the General Data Protection Regulation (GDPR), which was released in December 2022.[7] In July 2023, the European Commission formally adopted the Adequacy Decision.[8]

---

[4] *See, e.g.*, Ariane Mole, Willy Mikalef, & Juliette Terrioux, *Why This French Court Decision Has Far-Reaching Consequences for Many Businesses*, IAPP.ORG (Mar. 15, 2021), https://iapp.org/news/a/why-this-french-court-decision-has-far-reaching-consequences-for-many-businesses; Gabriela Zanfir-Fortuna, *Understanding Why the First Pieces Fell in the Transatlantic Transfers Domino*, THE FUTURE OF PRIVACY FORUM (2022), https://fpf.org/blog/understanding-why-the-first-pieces-fell-in-the-transatlantic-transfers-domino; 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.

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

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

[7] *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*, EUROPEAN COMMISSION (2022), *available at* https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf.

[8] *Commission Implementing Decision EU 2023/1795 of 10 July 2023 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*, OJ L 231, 20.9.2023, EUROPEAN COMMISSION (2023), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023D1795 (hereinafter "Adequacy Decision").

The first legal challenge to the decision has already been filed by Philippe Latombe, a member of the French Parliament and a commissioner of the French Data Protection Authority (CNIL).[9] Latombe is acting in his personal capacity, not as a French MP or a member of CNIL. He chose a direct action for annulment under Article 263 of the Treaty on the Functioning of the European Union (TFEU), which means that his case faces strict admissibility conditions. Based on precedent, it would not be surprising if the EU courts refuse to consider its merits.[10] Regarding the substance of Latombe's action, he described it in very general terms in his press release (working translation from French):

> The text resulting from these negotiations violates the Charter of Fundamental Rights of the Union, due to the insufficient guarantees of respect for private and family life with regard to the bulk collection of personal data, and the General Data Protection Regulation (GDPR), due to the absence of guarantees of a right to an effective remedy and access to an impartial tribunal, the absence of a framework for automated decisions or lack of guarantees relating to the security of the data processed: all violations of our law which I develop in the 33-page brief (+ 283 pages of annexes) filed with the TJUE yesterday.[11]

Latombe also complained about the Adequacy Decision being published only in English.[12] Irrespective of the legal merits of that complaint, however, it is already moot because the Adequacy Decision was subsequently published in the *Official Journal of the European Union* in all official EU languages.[13]

Reportedly, Max Schrems also plans to bring a legal challenge against the Adequacy Decision,[14] as he has successfully done with the two predecessors of the current EU-US framework.[15] This time,

---

[9] *See* Patrice Navarro & Julie Schwartz, *Member of French Parliament Lodges First Request for Annulment of EU-US Data Privacy Framework*, HOGAN LOVELLS ENGAGE (Sep. 8, 2023), https://www.engage.hoganlovells.com/knowledgeservices/news/member-of-french-parliament-lodges-first-request-for-annulment-of-eu-us-data-privacy-framework; Philippe Latombe, *Communiqué de Presse* (Sep. 7, 2023), *available at* https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf.

[10] *See, e.g.*, Joe Jones, *EU-US Data Adequacy Litigation Negins*, IAPP.ORG (Sep. 8, 2023), https://iapp.org/news/a/eu-u-s-data-adequacy-litigation-begins.

[11] Latombe, *supra* note 9.

[12] *Id.*

[13] *See supra* note 8.

[14] Mark Scott, *We Don't Talk About Fixing Social Media*, DIGITAL BRIDGE FROM POLITICO (Aug. 3, 2023), https://www.politico.eu/newsletter/digital-bridge/we-dont-talk-about-fixing-social-media. *See also New Trans-Atlantic Data Privacy Framework Largely a Copy of "Privacy Shield". NOYB Will Challenge the Decision*, NOYB.EU (2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

[15] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, *available at* https://curia.europa.eu/juris/liste.jsf?num=C-362/14 [hereinafter "*Schrems I*"].

however, Schrems plans to begin the suit in the Austrian courts, hoping for a speedy preliminary reference to the EU Court of Justice ("CJEU").[16]

This paper aims to present and discuss the key legal issues surrounding the European Commission's Adequacy Decision, which are likely to be the subject of litigation. In Section II, I begin by problematizing the applicable legal standard of an "adequate level of protection" of personal data in a third country, noting that this issue remains open for the CJEU to address. This makes it more challenging to assess the Adequacy Decision's chances before the Court and suggests that the conclusive tone adopted by some commentators is premature.

I then turn, in Section III, to the question of proportionality of bulk data collection by the U.S. government. I consider 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.

The second part of Section III is devoted to the problem of effective redress, which was the critical issue on which the CJEU relied 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 commentators on 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 U.S. intelligence agencies' data-processing activities.

II. 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]."[17]

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

---

[16] Scott, *supra* note 13.

[17] *Schrems II* [178].

offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union (...)." This phrasing goes back to the CJEU's *Schrems I* decision,[18] where the Court interpreted the old Data Protection Directive (Directive 95/46).[19] 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.[20]

As Christakis, Propp, & have Swire noted,[21] the critical 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*.[22]

In 2020, the European Data Protection Board (EDPB) issued recommendations "on the European Essential Guarantees for surveillance measures."[23] The recommendations aim to "form part of 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."[24] 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 light of the CJEU's jurisprudence. The Court is free not to follow the EDPB's legal interpretation, and thus the

---

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

[19] 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").

[20] *Schrems I* [73].

[21] 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.

[22] 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].

[23] European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, *available at* https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (hereinafter: "EDPB Recommendations on surveillance measures").

[24] EDPB Recommendations on surveillance measures [8].

importance of the recommendations should not be overstated, either in favor or against the Adequacy Decision.

While 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.

III. Arguments Likely to Be Made Against the Adequacy Decision

A. Proportionality and Bulk Data Collection

Under Article 52(1) of the EU Charter of Fundamental Rights, restrictions on the right to privacy and the protection of personal data 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 October 2022 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."[25]

Doubts have been raised, however, as to whether this is sufficient. 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 the bulk collection of personal data may be done in a way that does not jeopardize adequacy under the GDPR.

[25] Executive Order, *supra* note 5, Sec. 2(a)(ii)(B).

1. Legitimate objectives

In his analysis of the adequacy under EU law of the new U.S. data-protection framework, Douwe Korff argues 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.[26]

Korff's concern is that the legitimate objectives listed in the executive order are too broad and 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.[27] Korff referred to the EDPB Recommendations, which reference CJEU decisions in *La Quadrature du Net* and *Privacy International*. Unlike Korff, however, the EDPB stresses that those CJEU decisions were "in relation to the law of a Member State and not to a third country law."[28]

In contrast, in *Schrems II*, the Court did not consider legitimate objectives 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. Still, this approach can be taken too far without sufficient care. Just because *some* guidance is available (on intra-EU issues), it does not follow that it applies to data transfers outside the EU. 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

---

[26] 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.

[27] *Id.* at 10–13.

[28] EDPB Recommendations on surveillance measures [34].

> 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.[29]

Hence, exclusive focus on what the EU law requires *within the EU*—however convenient this method may be—may be misleading in assessing the adequacy of a third country under Article 45.

Aside from the lack of direct guidance on 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 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.[30]

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 also applies to "necessity" and "proportionality" as used in the executive order.)

2. *Can bulk collection be 'adequate'?*

As Max Schrems' organization NOYB stated in response to the executive order's publication:

> (…) 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.[31]

Korff echoed this view, noting, *e.g.*:

---

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

[30] European Commission, *supra* note 8, Recital 135.

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

> (...) - 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
>
> - 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.[32]

The Schrems II Court indeed held that U.S. law and practices do not "[correlate] to the minimum safeguards resulting, under EU law, from the principle of proportionality."[33] As, however, the EDPB noted in its opinion on a draft of the Adequacy Decision:

> ... the CJEU did not exclude, by principle, bulk collection, but considered in its Schrems II decision that for such bulk collection to take place lawfully, sufficiently clear and precise limits must be in place to delimit the scope of such bulk collection. (...)
>
> The EDPB also recognizes that while replacing the PPD-28, the EO 14086 provides for new safeguards and limits to the collection and use of data collected outside the U.S., as the limitations of FISA or other more specific U.S. laws do not apply.[34]

As Korff observed, the CJEU has considered the question of bulk collection of electronic communication data, in an intra-EU context, in cases like *Digital Rights Ireland*[35] and *La Quadrature du Net*.[36] 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

---

[32] Korff, *supra* note 25 at 19.

[33] *Schrems II* [184].

[34] European Data Protection Supervisor, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data Under the EU-US Data Privacy Framework*, [134]-[135] (2023), https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en. *See also* Alex Joel, *Necessity, Proportionality, and Executive Order 14086*, JOINT PIJIP/TLS RESEARCH PAPER SERIES (2023), https://digitalcommons.wcl.american.edu/research/99.

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

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

> essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (…)[37]

This is potentially important, because the Court concluded the discussion included in this paragraph by saying that "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order" is "apparent in particular from the preceding paragraphs."[38] This could suggest that, as under the Data Protection Directive in *Schrems I*, the Court may see the issue of bulk collection of the *contents* of electronic communications as a serious problem for adequacy under Article 45 GDPR.

The Commission addressed this in the Adequacy Decision as follows:

> (…) 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 be carried out outside the United States, on the basis of EO 12333.[39]

The Commission relies on a distinction between data collection that the U.S. government does *within* the United States and *outside* of the United States. This likely refers to an argument—discussed by, *e.g.*, Christakis[40] —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, it should only concern domestic surveillance, not international surveillance (if personal data transferred from the EU would fall under domestic surveillance in that third country).

The Commission also made a second relevant point:

> (…) 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**

---

[37] *Schrems I* [94].

[38] *Schrems I* [96].

[39] European Commission, *supra* note 8, Recitals 140-141 (footnotes omitted).

[40] 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.

> **is therefore to be contrasted to collection taking place on a generalised and indiscriminate basis ('mass surveillance') without limitations and safeguards.**[41]

In the Commission's view, there is a categorical distinction between "bulk collection" as practiced by the United States and the "generalized and indiscriminate" mass surveillance that the CJEU scrutinized in *Digital Rights Ireland* and other cases. This may seem like an unnatural reading of "generalized 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)."[42] There may, however, 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.[43] In *Glawischnig-Piesczek*, the Court interpreted this rule as not precluding member states from requiring 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."[44] In other words, "general monitoring" was interpreted as *not* covering indiscriminate processing of all data stored by a hosting provider in order to find content identical to some other content.[45] The Court adopted an analogous approach with respect to Article 17 of the Copyright Directive.[46] This suggests that, in somewhat similar contexts, the Court is willing to see activities that may technically appear to be "general" as "not general," if some procedural or substantive limitations are present.

---

[41] European Commission, *supra* note 8, Recital 141, footnote 250 (emphasis added).

[42] *Id.*, Recital 141, footnote 250.

[43] 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.

[44] 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).

[45] 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.

[46] 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 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).

B. Effective Redress

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. Among the Court's key findings were that "PPD-28 does not grant data subjects actionable rights before the courts against the US authorities"[47] 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."[48]

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 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 insufficient safeguards against external pressures, 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 recent public debate, Max Schrems argued that the CJEU would have a difficult time finding that this judicial procedure satisfies Article 47 of the EU Charter, while at the same time holding that some courts in Poland and Hungary do not satisfy it.[49]

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.[50] But this is a hasty conclusion. The CJEU's phrasing in *Schrems II* is more cautious:

---

[47] *Schrems II* [181].

[48] *Schrems II* [183].

[49] @MBarczentewicz, TWITTER (Aug. 24, 2023, 9:43 AM), https://twitter.com/MBarczentewicz/status/1694707035659813023. *See also* 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.

[50] 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." In other places, however, she adopts the phrasing of "satisfying" Article 47.

> ...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.[51]

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, it is far from clear how the CJEU's jurisprudence interpreting Article 47 of the Charter is to be applied in the context of an adequacy assessment under Article 45 GDPR.

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, & Swire offer helpful analysis suggesting that it is, considering the proposed DPRC's independence, effective investigative powers, and authority to issue binding determinations.[52] Gorski & Korff argue that this is not the case, because the DPRC is not "wholly autonomous" and "free from hierarchical constraint."[53]

The Commission stated in the 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."[54] Moreover:

> (...) 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) (...)[55]

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

---

[51] *Schrems II* [186].

[52] 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.

[53] Gorski, *supra* note 49; Korff, *supra* note 25 at 21.

[54] European Commission, *supra* note 8, Recital 175.

[55] *Id.*, Recital 187 (footnotes omitted).

> (…) 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.[56]

Given that Christakis, Propp, & Swire appear to disagree,[57] this question of U.S. law may require further scrutiny. Even if the scenario sketched by Gorski is theoretically possible, however, the CJEU may take the view that it would not be appropriate to rule based on the assumption that the U.S. government would act to mislead the EU. And without that assumption, then the possibility of future changes to U.S. law appear to be adequately addressed by the adequacy-monitoring process (Article 45(4) GDPR).

3. Do EU persons have effective access to the redress mechanism?

In the already-cited public debate, Max Schrems argued that it may be practically impossible for EU persons to benefit from the new redress mechanism, due to the requirements imposed on "qualifying complaints" under the executive order.[58] Presumably, Schrems implicitly refers to the requirements that a complaint:

> (i) "alleges a covered violation has occurred that pertains to personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the United States from a qualifying state after" the official designation of that country by the Attorney General;
>
> (ii) includes "information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant's data has in fact been subject to United States signals intelligence activities; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the United States; the identities of the United States Government entities believed to be involved in the alleged violation (if known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures;"
>
> (iii) "is not frivolous, vexatious, or made in bad faith"[59]

---

[56] Gorski, *supra* note 49.

[57] 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, & Swire, *supra* note 51.

[58] @MBarczentewicz, TWITTER (Aug. 24, 2023, 9:43 AM), https://twitter.com/MBarczentewicz/status/1694707035659813023.

[59] Executive Order, section 5(k)(i)-(iv).

Given the qualifications that a complaint need only to "allege" a violation and "need not demonstrate that the complainant's data has in fact been subject to United States signals intelligence activities," it is unclear what Schrems' basis for suggesting that it will not be possible for EU persons to benefit from this redress mechanism is.

C. Access to Information About Data Processing

Finally, Schrems' NOYB raised a concern that "judgment by 'Court' [is] already spelled out in Executive Order."[60] 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. In other words, the 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 the 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 argues 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 (...)[61]

Here, as before, Korff appears to elide 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.

The issues of access to information and data may, however, call for closer consideration. For example, in *La Quadrature du Net,* the CJEU looked at the difficult problem of notifying 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.[62] Nevertheless, given the "essential equivalence" standard applicable to third-country adequacy assessments, it does not automatically follow that individual notification is at all required in that context.

---

[60] 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. *See also* NOYB, *supra* note 13.

[61] Korff, *supra* note 25 at 25.

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

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 significant restrictions on rights to information and access in some EU member states,[63] 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."

The Commission's Adequacy Decision accepted that individuals would 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.[64] The Commission did not take the simplistic view that access to personal data must be guaranteed by the same procedure that provides binding redress, including through the Data Protection Review Court. Instead, the Commission accepts that other avenues, such as requests under the Freedom of Information Act, may perform that function.

IV. Conclusion

With the Adequacy Decision, the European Commission announced that it has favorably assessed the October 2022 executive order's changes to the U.S. data-protection framework, which apply to foreigners from friendly jurisdictions (presumed to include the EU). The Adequacy Decision is certain to be challenged before the CJEU by privacy advocates. As discussed above, the key legal concerns will likely be the proportionality of data collection and the availability of effective redress.

Opponents of granting an adequacy decision tend to rely on the 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 its 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 to point to certain features of U.S. law and practice that were significantly below the GDPR standard (*e.g.*, that the official responsible for providing individual redress was not guaranteed to be independent of political pressure). Future legal challenges to a new Adequacy Decision will

---

[63] 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.

[64] European Commission, *supra* note 8, Recitals 199-200.

most likely require the CJEU to provide more guidance on what "adequate" and "essentially equivalent" mean.

In the Adequacy 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.

Overall, the Commission presents a sophisticated, yet uncynical, picture of U.S. law and practice. The lack of cynicism about, *e.g.*, 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. Litigants will likely invite the CJEU 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). It is not clear, however, that the Court will be willing to go that way—not least due to respect for comity in international law.