The EU-US Data Privacy Framework and the *Schrems* Saga: Is there Light at the End of the Tunnel?

Jan Helge Brask Pedersen*

Contents

* LL.M., Associate at Advokatfirmaet Thommessen (Norway), PhD Candidate at Saarland University (Germany), Email: jhp@thommessen.no.

Abstract

The article examines the legal framework for data transfers from the EU to the US. In the judgements known as *Schrems I* and *II*, the CJEU invalidated the two former US adequacy decisions on the grounds that they did not satisfy the requirements in Art. 45 GDPR. On 10 July 2023, the European Commission adopted a new US adequacy decision. The question that is examined in this article is whether the new adequacy decision is compatible with Art. 45 GDPR. According to the CJEU's interpretation of this provision in *Schrems I* and *II*, third countries must provide a level of data protection that is "essentially equivalent" to the EU. This requires the US to comply with all relevant fundamental rights in the Charter and in the ECHR. Based on an assessment of US law, the article concludes that it is doubtful that the latest US adequacy decision fulfils the requirements in Art. 45 GDPR and that it is likely that the CJEU – once it is confronted with the question – will invalidate the adequacy decision of July 2023.

Keywords: International Data Transfers, Extraterritoriality, Adequacy Decision, GDPR, Bulk Interception of Communications, Charter of Fundamental Rights of the European Union, Data Protection, ECHR, The Right to Respect for Private Life, Proportionality

A. Introduction

The *Snowden* disclosures in June 2013 led to strong reactions in Europe. European governments condemned the surveillance conducted by the National Security Agency (NSA), as it became known that European governments had been targeted by the surveillance.[1] Moreover, European citizens' trust in the authorities of the United States (US) dropped following the *Snowden* revelations. According to the survey "Deutschlandtrend", which was conducted in August 2013, only 35 percent of Germans viewed the US as a reliable partner, compared to 76 percent in November 2009.[2] The European Council acknowledged that the Snowden revelations raised "deep concerns" among European citizens.[3] The reactions following the *Snowden* disclosures illustrate the significant cultural differences between the EU and the US in the context of data protection and privacy.

Against the backdrop of the Snowden revelations, the validity of the legal framework for the transfer of personal data from the EU to the US was challenged before

1 *Reuters*, Merkel tells Obama: spying on friends is unacceptable, 24 October 2013, available at: https://www.reuters.com/article/us-eu-summit-merkel-idUSBRE99N0QJ20131024 (2/4/2024); *Rosenbach/Stark*, How America Spies on Europe and the UN, Der Spiegel, 26 August 2013, available at: https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html (2/4/2024).

2 *Deutsche Welle*, Germans lose trust in US, 11 August 2013, available at: https://www.dw.com/en/germans-trust-in-us-plummets-in-wake-of-spying-scandal/a-17213441 (2/4/2024).

3 *BBC*, EU says distrust of US on spying may harm terror fight, 25 October 2013, available at: https://www.bbc.com/news/world-europe-24668286 (2/4/2024).

the Court of Justice of the European Union (CJEU) in the cases known as *Schrems I* and *II*. The Austrian privacy activist *Max Schrems* lodged a complaint to the Irish Data Protection Commissioner, contending that personal data transferred to the US were not sufficiently protected from surveillance under US law. In *Schrems I*, the CJEU invalidated the first US adequacy decision, known as the *Safe Harbour* decision. The CJEU held that the European Commission had not made any formal findings as to the level of protection under US law.[4] After the CJEU handed down its judgement in *Schrems I*, the European Commission adopted another US adequacy decision, known as the Privacy Shield decision. The *Privacy Shield* decision was invalidated by the CJEU in the subsequent *Schrems II* case. In *Schrems II*, the CJEU held that the limitations on the exercise of the right to privacy and data protection imposed under US law were disproportionate,[5] and that US law did not provide an effective remedy.[6]

Under Chapter V of the General Data Protection Regulation (GDPR),[7] the transfer of personal data from the EU to a third country requires a legal basis.[8] Chapter V of the GDPR establishes three alternative legal bases, namely adequacy decisions, appropriate safeguards and derogations.[9] Adequacy decisions are legislative acts that authorise all data transfers to a designated third country and do not necessitate further assessments by the processor or the controller of the level of protection in that country.[10] Appropriate safeguards are measures established by the processor or the controller, which in the absence of an adequacy decision provide an adequate level of protection for personal data transferred from the EU to a third country.[11] In a situation where no adequacy decision has been adopted and no appropriate safeguards have been established, a derogation may be used as legal basis for data transfers from the EU to a third country, provided that the conditions set out in Art. 49 GDPR are fulfilled.[12]

The CJEU's invalidations of the *Safe Harbour* and *Privacy Shield* decisions in *Schrems I* and *II* led to legal uncertainties for processors and controllers transferring personal data from the EU to the US. Although an adequacy decision is per se not required for the transfer of personal data to the US or to other third countries,

4 CJEU, case C-362/14, *Schrems I [GC]*, ECLI:EU:C:2015:650, para. 97.
5 CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, paras. 180–182.
6 Ibid., paras. 191–196.
7 Regulation (EU) No. 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119 of 4/5/2016, p. 1.
8 *Kuner*, in: Kuner/Bygrave/Docksey/Drechsler (eds.), p. 762; *Skullerud/Rønnevik/ Skorstad/Pellerud*, p. 368.
9 *Kuner*, in: Kuner/Bygrave/Docksey/Drechsler (eds.), p. 774; *Skullerud/Rønnevik/ Skorstad/Pellerud*, pp. 371, 377, 389.
10 *Kuner*, in: Kuner/Bygrave/Docksey/Drechsler (eds.), p. 774; *Skullerud/Rønnevik/ Skorstad/Pellerud*, pp. 371, 377, 389.
11 *Kuner*, in: Kuner/Bygrave/Docksey/Drechsler (eds.), p. 815; *Skullerud/Rønnevik/ Skorstad/Pellerud*, p. 377.
12 *Kuner*, in: Kuner/Bygrave/Docksey/Drechsler (eds.), p. 843; *Skullerud/Rønnevik/ Skorstad/Pellerud*, p. 389.

it simplifies the legal aspects. In the absence of an adequacy decision, processors and controllers must assess the level of protection in the third country on their own. There is a risk that processors and controllers make wrongful assessments of the level of protection in the third country, which in turn may impact which safeguards are established to protect the transferred personal data.

The risks related to wrongful assessments of the level of protection in the US is underscored by the high number of processors and controllers that were reliant on the *Safe Harbour* and *Privacy Shield* decisions. According to the Congressional Research Service, 5300 companies relied on *Privacy Shield* as legal basis for data transfers from the EU to the US.[13] The Annual Governance Report 2019 by the International Association of Privacy Professionals further suggests that among the companies that were transferring personal data from the EU to the US, 60 percent used *Privacy Shield* and 88 percent used standard contractual clauses as legal bases.[14]

The latest development is the adoption by the European Commission of a third US adequacy decision on 10 July 2023.[15] The finding that US law provides an adequate level of protection is based on an assessment of Executive Order (E.O.) 14086, which was adopted by the US president on 7 October 2022.[16] E.O. 14086 and the new US adequacy decision are part of a package of measures that are known as the "EU-US Data Privacy Framework".[17] E.O. 14086 is intended to address the problems raised in *Schrems I* and *II* and to implement the measures necessary for US law to provide an adequate level of protection.[18] It is expected that the validity of the new US adequacy decision will be challenged before the CJEU in 2024 or 2025.[19]

The following sections will examine the EU-US data privacy framework. In section B, an analysis of the CJEU's judgement in *Schrems II* is provided. The aim of the analysis is to clarify what it means that third countries must provide a level

13 *Archick/Fefer*, U.S.-EU Privacy Shield and Transatlantic Data Flows, Congressional Research Service, 22 September 2021, available at: https://crsreports.congress.gov/product/pdf/R/R46917 (2/4/2024).

14 *Hughes/Saverice-Rohan*, IAPP-EY Annual Privacy Governance Report 2019, International Association of Privacy Professionals, available at: https://f.hubspotusercontent20.net/hubfs/525875/IAPP_EY_Governance_Report_2019.pdf (2/4/2024).

15 *European Commission*, Commercial sector: adequacy decision on the EU-US Data Privacy Framework, 10 July 2023, available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en#:~:text=On%2010%20July%20the%20European,in%20the%20Data%20Privacy%20Framework (2/4/2024).

16 *The White House*, Fact sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, 07 October 2022, available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ (2/4/2024).

17 See *supra* fn. 15.

18 See *supra* fn. 16.

19 *NOYB*, European Commission gives EU-US data transfers third round at CJEU, 10 July 2023, available at: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (2/4/2024).

of protection of personal data that is "essentially equivalent" to the EU. In section C, it is examined whether US law complies with the requirements set out in *Schrems II*, and in particular, whether E.O. 14086 provides a level of protection of personal data that is "essentially equivalent" to the EU. Finally, in section D, reflections are made on how US authorities can resolve the problems addressed by the CJEU in *Schrems I* and *II*. Alternative measures to those set out in E.O. 14086 are proposed and evaluated in that section.

B. An analysis of the CJEU's judgement in *Schrems II*

I. Introduction

In *Schrems II*, the CJEU clarified the interpretation of Art. 45 GDPR. The CJEU held that Art. 45 (1) GDPR requires third countries to provide a level of protection of personal data that is "essentially equivalent" to the EU.[20] The CJEU examined section 702 of the Foreign Intelligence Surveillance Act (FISA) and E.O. 12333, and concluded that the limitations on the exercise of the right to privacy and data protection were disproportionate,[21] and that an effective remedy was not provided.[22] According to the CJEU, US law did not provide a level of protection of personal data that is "essentially equivalent" to the EU. The expression "essentially equivalent" is unclear and raises questions that are analysed in the following subsections. The purpose of the analysis is to provide a basis for the assessment of E.O. 14086 in section C.

II. What does it mean that US law must provide a protection of personal data that is "essentially equivalent" to the protection provided under EU law?

The expression "essentially equivalent" implies that not all differences in the level of protection of personal data in the EU and a third country would lead to the conclusion that the level of protection provided in the latter is inadequate. At first glance, the level of scrutiny appears to be low. However, the CJEU held in *Schrems I* that the discretion afforded to the European Commission in assessing the level of protection provided by third countries is reduced.[23] Interestingly, in *Schrems II*, the CJEU indulged in detailed assessments of the proportionality of the surveillance programs based on section 702 of FISA and E.O. 12333, without attaching weight to the US authorities' assessments of proportionality.[24] In doing so, the CJEU went far in substituting US authorities' assessments with its own assessments, which leaves an impression of inconsistency.

20 CJEU, case C-362/14, *Schrems I [GC]*, ECLI:EU:C:2015:650, para. 73; CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, para. 162.
21 Ibid., paras. 180–182.
22 Ibid., paras. 191–196.
23 CJEU, case C-362/14, *Schrems I [GC]*, ECLI:EU:C:2015:650, para. 78.
24 CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, paras. 180–182.

Some aspects of the interpretation of Art. 45 (1) GDPR were nevertheless clarified in *Schrems II*. According to the CJEU, the level of protection of personal data provided by the third country must not be "identical" to the level of protection under EU law.[25] Moreover, the means by which a third country protects personal data may differ from the means used by the EU, as long as the means used by the third country are "effective".[26]

In holding that the level of data protection in third countries must be "essentially equivalent" to the EU, the CJEU may have found inspiration in the jurisprudence of national constitutional courts. The expression "essentially equivalent" is for instance similar to the expression "substantially equal", which was used by the German Constitutional Court in the *Solange II* case.[27] The *Solange II* case concerned the principle of primacy of EU law, and it is beyond dispute that a lack of recognition by the German Constitutional Court would have jeopardized the autonomy of EU law.[28] As there is no parallel when the CJEU assesses the data protection and privacy legislation of third countries, the CJEU may apply a higher level of scrutiny than that applied by national constitutional courts when reviewing EU legislation.

A pertinent question is whether it would suffice for the US to comply with the fundamental rights laid down by the Charter of Fundamental Rights (Charter), or whether the US must also comply with the requirements stipulated in the GDPR. The GDPR lays down more specific requirements for the processing of personal data than the Charter. Processors and controllers must, for example, comply with general data protection principles, such as data minimisation and purpose limitation, and provide a legal basis for data processing. In addition, the GDPR provides data subjects with rights, such as the right to information, the right to access and the right to erasure.

Greenleaf assumes that third countries must comply not only with the fundamental rights enshrined in the Charter, but also with the various provisions of the GDPR.[29] However, the CJEU has not applied all the requirements in the GDPR to third countries. In *Google v. CNIL*, the CJEU held that search engines are required to carry out de-referencing on versions of their websites corresponding to the member states of the EU, but not on versions corresponding to third countries. The CJEU held that "numerous third States do not recognise the right to de-referencing or have a different approach to that right".[30] In addition, the CJEU expressed that the EU legislator "has not, to date, struck such a balance as regards the scope of a de-referencing outside the Union".[31] Although Google v. CNIL did not concern

25 Ibid., para. 162; CJEU, case C-362/14, *Schrems I [GC]*, ECLI:EU:C:2015:650, para. 73.
26 Ibid., para. 74.
27 BVerfGe 73, 339 (22 October 1986).
28 *Lenaerts* et al., ZfAÖRuV 2021/2, p. 80; CJEU, case C-6-64, *Costa v E.N.E.L.*, ECLI:EU:C:1964:66.
29 *Greenleaf*, PLBIR 2018/1, pp. 8–10.
30 CJEU, case C-507/17, *Google v. CNIL [GC]*, ECLI:EU:C:2019:772, para. 59.
31 Ibid., para. 61.

the interpretation of Art. 45 GDPR, the reasons provided strongly suggest that the CJEU defers to the priorities made by third countries.

Requiring the US to comply with all the provisions of the GDPR would undermine the efficiency of transatlantic data flows, as there are significant differences between the data protection and privacy laws of the EU and the US.[32] Although not decisive, efficiency is highlighted as an objective in several recitals of the GDPR. For example, it follows from recital 6 of the GDPR that technology should "further facilitate […] the transfer [of data] to third countries and international organisations, while ensuring a high level of the protection of personal data". Moreover, recital 101 of the GDPR highlights that "flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation".

To facilitate for efficient transfers of personal data to the US, the US should be required to comply with the fundamental rights laid down in the Charter, but not with the requirements in the GDPR. The CJEU's interpretation of Art. 45 GDPR in *Schrems II* allows for a distinction between compliance with the fundamental rights in the Charter and with the requirements laid down in the GDPR. As noted above, the CJEU confirmed in *Schrems II* that the level of protection of personal data provided by the third country must not be "identical", but rather "essentially equivalent", to the level of protection under EU law.[33]

Another question is whether differentiations are made between absolute and relative fundamental rights in the assessment of the level of protection of personal data under US law. The distinction between absolute and relative rights recognises that not all rights can be fully realised and that interferences with specific rights may under some circumstances be legitimate. One could assume that the US must respect absolute rights but are free to decide on the permissibility of interferences with relative rights.

Tzanou claims that the CJEU in *Schrems I* limited the extraterritorial application of fundamental rights to situations in which the essence of the right concerned has been compromised.[34] The differentiation between absolute and relative rights proposed by *Tzanou* is worthy of consideration. In principle, neither the CJEU nor the European Commission are in better positions than US authorities to assess the permissibility of interferences with relative rights. A failure to consider the interests and values of the US sends strong signals and discredits the institutions in the US established to secure respect, protection and fulfilment of the right to data protection and privacy. As accurately expressed by Advocate General *Saugmandsgaard Øe*, one must strike a fair balance between "a reasonable degree of pragmatism in order to allow interaction with other parts of the world, and […] the need to assert

32 *Rustad/Koenig*, FLR 2019/2, p. 405.
33 CJEU, case C-362/14, *Schrems I [GC]*, ECLI:EU:C:2015:650, para. 73; CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, para. 162.
34 *Tzanou*, in: Fabbrini et al. (eds.), p. 9.

the fundamental values recognised in the legal orders of the Union and its Member States".[35]

However, a limitation of the extraterritorial application of fundamental rights to situations in which the essence has been compromised is difficult to reconcile with the CJEU's proportionality assessments in *Schrems II*. The CJEU made detailed assessments of the proportionality of the US' bulk interception regime and did not attach weight to the US interest of safeguarding national security and preventing serious crime.[36] If the extraterritorial application of fundamental rights in *Schrems I* and *II* was limited to situations in which the essence of the right concerned has been compromised, it would not make sense for the CJEU to make such detailed assessments of the proportionality of the US' bulk interception regime. When regard is had to the CJEU's reasoning in *Schrems II*, it seems reasonable to conclude that no differentiations are made between absolute and relative fundamental rights in the context of the assessment of the adequacy of US data protection and privacy law.

Another question is whether differentiations are made between the right to data protection and privacy, and other fundamental rights, in the assessment of the level of protection in US law. The transfer of personal data from the EU to the US leads to interferences with fundamental rights other than the right to data protection and privacy. The CJEU expressed in *Digital Rights Ireland* that mass surveillance conducted by EU member states may deter people from using the internet and could have a chilling effect contrary to the freedom of expression in Art. 11 of the Charter.[37] The same is valid in the situation that the communications of European data subjects are intercepted by the US authorities.

Other fundamental rights may also be relevant to the transfer of personal data from the EU to the US. As the US' objective in operating a bulk interception regime is to safeguard national security objectives, it must be assumed that intercepted material may be used as evidence in criminal proceedings. In so far as intercepted material is used as evidence in criminal proceedings, the adversarial and equality of arms principles apply. In addition, the NSA may resort to profiling to identify possible threats to national security before they materialise. Profiling with the aim of identifying possible threats to national security raises problems regarding the prohibition of discrimination. There are also various forms of sensitive information that enjoy protection under the Charter. The communication between a lawyer and his client is protected under Art. 7 of the Charter and the sources of journalists are protected under Art. 11 of the Charter.

The CJEU's assessment in *Schrems II* was limited to the rights enshrined in Art. 7, 8 and 47 of the Charter. As Art. 47 (1) is ancillary and only applicable in so far as another violation of the Charter has occurred, clear conclusions from *Schrems*

35 Opinion of AG Saugmandsgaard Øe, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2019:1145, para. 7.

36 CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, paras. 180–182.

37 *Lock*, in: Kellerbauer/Klamert/Tomkin (eds.), p. 2134; *Woods*, in: Peers/Hervey/Kenner/Ward (eds.), p. 314; CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland [GC]*, ECLI:EU:C:2014:238, para. 28.

II on whether other fundamental rights are relevant under Art. 45 (1) GDPR cannot be drawn. However, there are no compelling reasons for only taking the right to data protection and privacy into account in the assessment of the level of protection under US law. On the contrary, it must be assumed that all relevant fundamental rights may be taken into account in the assessment of whether US law provides a protection of personal data that is "essentially equivalent" to the protection provided under EU law.

This conclusion is supported by the recitals of the GDPR. It follows from recital 104 that "the Commission should, in its assessment of the third country […] take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards". Further, recital 101 of the GDPR provides that "[…] when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined".

III. Should direct access to personal data for US authorities be excluded from the scope of the US adequacy decision?

US authorities can gain access to personal data either directly through their own intelligence activities or indirectly by obliging service providers to provide access to personal data collected from their users. It has been argued by the US government that only the processing of personal data collected indirectly from European data subjects through service providers falls within the scope of the US adequacy decision.[38] According to this view, the processing of personal data collected by US authorities directly from European data subjects falls outside the scope of the US adequacy decision.[39]

This view is supported by the national security exception laid down in Art. 4 (2) TEU. According to this provision, the safeguarding of national security falls outside the scope of EU law. The CJEU clarified in Privacy International and La Quadrature du Net that Art. 4 (2) TEU applies to the activities of national intelligence services, but not to service providers' collection of personal data from their users.[40] According to the CJEU, "all operations processing personal data carried out by providers of electronic communications services fall within the scope of [the e-pri-

38 *The United States*, Feedback from: United States Mission to the European Union, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act-/F1305841_en (2/4/2024); *The United States*, Comments on Proposed EDPB Recommendations 01/2020, available at: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.12.21_-_us_comments_on_edpb_supp_measures_final.pdf (2/4/2024).

39 Ibid.

40 CJEU, case C-623/17, *Privacy International [GC]*, ECLI:EU:C:2020:790, para. 46; CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net [GC]*, ECLI:EU:C:2020:791, para. 101.

vacy directive], including processing operations resulting from obligations imposed on those providers by the public authorities".[41]

These observations are important because the "essentially equivalent" standard requires a comparison to be made between the data protection and privacy laws of the EU and the US. The requirement that the US must provide a level of protection of personal data that is "essentially equivalent" to the protection provided under EU law, presupposes that there is a comparative standard by which the member states of the EU are obliged. If EU member states' direct access to personal data falls outside the scope of EU law, there is no such comparative standard. One may thus argue that US authorities' direct access to the personal data of European data subjects, in lack of a comparative standard by which the EU member states are obliged, falls outside the scope of the US adequacy decision.

In its comments on the proposed Standard Contractual Clauses (SCC) decision submitted on 10 December 2020, the US government recalled the CJEU's judgements in *Privacy International* and *La Quadrature du Net*. The US government made a distinction between direct access to personal data and requiring service providers to provide the authorities with personal data.[42] The US government argued that "[t]he Commission should interpret the *Schrems II* decision in a manner that does not impose a double standard under which non-EU countries' measures are subject to strict EU data protection rules while comparable Member State measures are not subject to EU law at all".[43] Although the statements concerned the proposed SCC decision, they are also valid for the US adequacy decision. It must be assumed that the US government made the same arguments in the negotiations with the European Commission before the adoption of the EU-US data privacy framework.[44]

The CJEU's judgements in *Privacy International* and *La Quadrature du Net* should not lead to exclusion of the US government's direct access to personal data from the scope of the US adequacy decision. Firstly, the CJEU clarified in *Schrems II* that Art. 4 (2) TEU is irrelevant to the transfer of personal data to third countries.[45] According to the CJEU, the GDPR applies to the transfer of personal data from the EU to third countries, irrespective of whether the data is liable to be processed by the authorities in that third country for the purpose of safeguarding national security.[46] The CJEU held that the transfer of personal data from the EU to the US constitutes data processing within the meaning of Art. 2 (1) GDPR also in

41 CJEU, case C-623/17, *Privacy International [GC]*, ECLI:EU:C:2020:790, para. 46; CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net [GC]*, ECLI:EU:C:2020:791, para. 101.

42 See *supra* fn. 38.

43 Ibid.

44 *Christakis*, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1), European Law Blog, 12 April 2021, available at: https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/ (2/4/2024).

45 CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, paras. 81, 85.

46 Ibid., para. 89.

situations where the data is liable to be processed by the authorities for the purpose of safeguarding national security.[47] As there were no applicable exceptions, the GDPR was applicable.[48] These arguments are still valid, in spite of the CJEU's later judgements in *Privacy International* and *La Quadrature du Net*.

Secondly, surveillance of foreign citizens residing abroad may in some situations fall under the territorial scope of application of the European Convention on Human Rights (ECHR). The applicability of the ECHR to international surveillance conducted by its parties is relevant to the assessment of the scope of the US adequacy decision because it may provide a comparative standard by which the parties to the Convention are obliged.

Although the collection of personal data in these situations does not take place on the territory of a party to the ECHR, systematic processing of intercepted material is necessary for threats to national security to be averted and for bulk interception to fulfil its purpose. In the situation that the intercepted material is processed on the territory of a party to the ECHR, the material is arguably protected under the ECHR once it enters the territory of that state. If a party to the ECHR illegitimately processes personal data on the territory of a state that is not a party to the ECHR, there may also in some situations be sufficient basis for claiming that the party has "effective control" over the violation, which would trigger the extraterritorial application of the Convention.

On 12 September 2023, the European Court of Human Rights (ECtHR) adopted its judgement in *Wieder and Guarnieri*. In this judgement, the ECtHR concluded that the United Kingdom's (UK) surveillance of two foreign citizens residing abroad took place on the territory of the UK and thus fell under the territorial scope of application of the ECHR.[49] The Court held that the processing of the collected data was carried out by the UK's intelligence services on the territory of the UK.[50] Interestingly, the ECtHR did not base its findings on an extraterritorial application of the Convention. As to the merits of the case, the Court found that the processing of the collected data constituted a violation of Art. 8 ECHR.[51] This is the first judgement in which the ECtHR has examined the applicability of the ECHR to international surveillance by its parties.[52]

IV. Partial conclusions

The CJEU's judgement in *Schrems II* suggests that the US must comply with the fundamental rights provided by the Charter, but not with all the requirements stipulated in the GDPR. All fundamental rights laid down in the Charter must

47 Ibid., para. 83.
48 Ibid., para. 85.
49 ECtHR, App. nos. 64371/16 and 64407/16, *Wieder and Guarnieri v. The United Kingdom*, para. 95.
50 Ibid., para. 91.
51 Ibid., para. 104.
52 Ibid., para. 88.

be complied with by the US and are relevant in the adequacy assessment. There are no differentiations between fundamental rights on the basis of the protected interests, or on the basis of the possibilities to limit the exercise of the fundamental right. Moreover, there is no basis for excluding the US authorities' direct access to personal data from the scope of the US adequacy decision.

C. An assessment of E.O. 14086: is it essentially equivalent to the protection provided under EU law?

I. Introduction

On 7 October 2022, the US president signed E.O. 14086, which implements the measures intended for US law to provide an adequate level of protection.[53] E.O. 14086 provides that intelligence activities shall be limited to what is "strictly necessary" and "proportionate", and establishes a new judicial redress mechanism, with complaints to the Civil Liberties Protection Officer (CLPO) and appeals to a new Data Protection Review Court (DPRC).[54] The European Commission adopted its long-awaited US adequacy decision on 10 July 2023.[55] The adequacy decision refers to E.O. 14086 and concludes that the US provides an adequate level of protection of personal data. In the following subsections, it is assessed whether E.O. 14086 provides a level of protection of personal data that is "essentially equivalent" to the EU.

II. Does E.O. 14086 satisfy the quality of law requirement?

It has been questioned whether safeguards against surveillance laid down by an executive order can satisfy the quality of law requirement.[56] As executive orders can be amended or revoked by the US president at any time, they do not guarantee the same foreseeability as statutory law. The US government's attempt to exclude the NSA's direct access to personal data from the scope of the US adequacy decision may have been related to the realisation that executive orders as legal bases for surveillance do not satisfy the quality of law requirement.[57] The direct access to personal data by the NSA is based on E.O. 12333, whereas obligating service providers to provide access to the NSA is based on FISA.[58]

53 See *supra* fn. 16.
54 *European Commission*, Questions & Answers: EU-U.S. Data Privacy Framework, 7 October 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 (2/4/2023).
55 See *supra* fn. 15.
56 *Vanebo*, Ny personvernavtale med USA langt fra noen 'quick fix', Dagens Næringsliv, 28 March 2022, available at: https://www.dn.no/innlegg/jus/personvern/eu-domstolen/innlegg-ny-personvernavtale-med-usa-langt-fra-noen-quick-fix/2-1-1191795 (2/4/2024).
57 See *supra* fn. 44.
58 Ibid.

The ECtHR has applied an enhanced foreseeability test for domestic surveillance measures. As surveillance measures are exercised in secret, there is a risk that state authorities will attempt to exceed their own competences. Individuals who are likely to be subjected to surveillance cannot be able to foresee the surveillance measures, as this would often undermine the purpose of the surveillance. However, state authorities are obligated to put in place sufficient guarantees to ensure the public that individuals are not subjected to surveillance, unless the authorities have a legal basis. According to the ECtHR, "domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any [surveillance] measures".[59] In particular, "the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity".[60] The foreseeability test is an aspect of the principle of legal certainty.[61] Legal certainty is a fundamental principle of EU law.[62]

It would be problematic to claim that executive orders as such are incapable of providing sufficient foreseeability to satisfy the quality of law requirement. The US has a longstanding tradition with the use of executive orders.[63] It would arguably discredit the US legal system to find that executive orders as legal bases for surveillance do not satisfy the quality of law requirement. Moreover, the ECtHR has since its judgement in *Sunday Times* held that the expression "law" does not refer to statutory law, as this "would deprive a common-law State which is Party to the Convention of [its protection] and strike at the very roots of that State's legal system".[64] It is safe to say that the use of an executive order as legal basis for surveillance does not as such constitute an infringement of the quality of law requirement.

A pertinent question is whether the competence of the US president to amend the list of legitimate objectives without public announcement is in line with the quality of law requirement. According to section 2(b)(i)(B) of E.O. 14086, changes to the list of legitimate objectives shall be announced publicly, "unless the President determines that doing so would pose a risk to the national security of the United States". *Korf* has held that the US president's competence to secretly amend the list of legitimate objectives under E.O. 14086 is irreconcilable with the quality of law

59 ECtHR, App. nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and Others v. The United Kingdom [GC]*, para. 333; ECtHR, App. no. 35252/08, *Centrum för Rättvisa v. Sweden [GC]*, para. 247.

60 Ibid.; ECtHR, App. nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and Others v. The United Kingdom [GC]*, para. 333.

61 *Steiner/Woods*, p. 169.

62 Ibid., p. 167.

63 *Encyclopaedia Britannica,* "executive order", available at: https://www.britannica.com/topic/executive-order (2/4/2024).

64 ECtHR, App. no. 6538/74, *The Sunday Times v. The United Kingdom (No. 1) [Plenary]*, para. 47.

requirement.[65] A consequence of the US president's competence to amend the list of legitimate objectives under E.O. 14086 without public announcement is that foreign data subjects cannot know for certain the conditions under which they can be subjected to surveillance. General uncertainty as to the conditions for surveillance measures does not satisfy the quality of law requirement. The US president should for this reason consider removing the passage in section 2(b)(i)(B) of E.O. 14086, which allows for the amendment of the list of legitimate objectives without public announcement.

III. Are the legitimate objectives in E.O. 14086 limited to the safeguarding of national security?

The CJEU has made a distinction between national security and serious crime objectives in defining the necessity of bulk interception of communications. Bulk interception of communication can be necessary to safeguard national security,[66] but not to prevent serious crime.[67] National security relates to the primary interests of the state in protecting its essential functions.[68] According to the CJEU, national security "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".[69]

The legitimate objectives in E.O. 14086 are broadly defined.[70] Section 2(c)(ii)(B)(1) sets as a legitimate objective "the taking of hostages, and the holding of individuals captive". As not all takings of hostages and holdings of individuals captive are capable of affecting the national security interests of the US, surveillance under this objective could be exercised in contravention of EU law.[71] Moreover, section 2(c)(ii)(B)(2) holds that the "protecti[on] against espionage, sabotage, assassination, or other intelligence activities conducted by […] a foreign government" is a legitimate objective for surveillance activities. Intelligence activities are part of the activities of every state and are usually legitimate. The US competence to implement bulk interception programs would be too wide to comply with EU law if it would suffice

65 *Korf*, The inadequacy of the October 2022 new US Presidential Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities, Data protection and digital competition, 11 November 2022, available at: https://www.ianbrown.tech/2022/11/11/the-inadequacy-of-the-us-executive-order-on-enhancing-safeguards-for-us-signals-intelligence-activities/ (2/4/2024).

66 CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net [GC]*, ECLI:EU:C:2020:791, para. 137.

67 Ibid., para. 141.

68 Ibid., para. 135.

69 Ibid.

70 *Ruschemeier*, Nothing new in the west? The executive order on US surveillance activities and the GDPR, European Law Blog, 14 November 2022, available at: https://europeanlawblog.eu/2022/11/14/nothing-new-in-the-west-the-executive-order-on-us-surveillance-activities-and-the-gdpr/ (2/4/2024).

71 See *supra* fn. 65.

for the NSA to demonstrate that the interception was executed to protect against intelligence activities of another state. Furthermore, section 2(c)(ii)(B)(6) provides that "protection against transnational criminal threats" is a legitimate objective for surveillance activities. Transnational criminal threats leads thoughts in the direction of serious crime objectives, rather than national security objectives, and gives the NSA wide competence to implement surveillance measures.

The broad wording of the legitimate objectives in E.O. 14086 should not necessarily lead to the finding that US law does not provide a protection of personal data that is "essentially equivalent" to that of EU law. It would suffice for the US authorities to interpret the objectives narrowly and to ensure that bulk interception is not exercised besides where justified by national security objectives. However, it is problematic that surveillance is not always subject to judicial review under US law prior to its execution. In particular, there is no independent mechanism established to review the legality of surveillance undertaken pursuant to E.O. 12333 prior to the execution of the measure. *Korf* has for this reason held that the objectives listed in E.O. 14086 "are clearly not limited to what the EU Court of Justice regards as legitimate national security purposes".[72] Indeed, the US president should consider specifying the legitimate objectives in E.O. 14086 to ensure that bulk interception is only exercised in pursuit of national security objectives.

IV. Does E.O. 14086 authorise surveillance beyond what is necessary and proportionate?

The CJEU applied the "less restrictive means" test in *Schrems II*.[73] The "less restrictive means" test has two aspects: Restrictions on the exercise of fundamental rights must not be overly comprehensive and there must not be other less restrictive measures capable of achieving the objective as efficiently as the measure chosen. In *Schrems II*, the CJEU examined the comprehensiveness of the US bulk interception regime, but did not assess whether there were other less restrictive measures capable of safeguarding national security objectives as efficiently as bulk interception of communications.[74] A possible explanation why the CJEU only assessed the comprehensiveness of the US bulk interception regime is that it may have been constrained by its own institutional limitations in assessing alternative measures. For that same reason, it seems unlikely that the CJEU in a future *Schrems III* will assess whether there are other less restrictive measures capable of safeguarding national security objectives as efficiently as bulk interception of communications. However, the reasoning of the CJEU in *Schrems II* suggests that the CJEU compensates for its inability of assessing alternative measures with a strict assessment of the comprehensiveness of bulk interception regimes.[75]

72 Ibid.
73 CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, para. 176.
74 Ibid.
75 Ibid.

Although E.O. 14086 at first glance appears to be implementing the CJEU's proportionality test in US law, it does not provide necessary clarifications on the elements that shall be taken into consideration by the US authorities when assessing proportionality. Sections 2(a)(ii)(A) and 2(a)(ii)(B) of E.O. 14086 provide that surveillance must be "necessary" and "proportionate" to advance an intelligence priority. The terms "necessary" and "proportionate" are too vague and subjective to give useful guidance on the elements that shall be taken into consideration in the proportionality assessment.[76] In addition, some of the provisions in E.O. 14086 are irreconcilable with the proportionality test applied by the CJEU. Section 2(b)(iii)(A)(3) provides that the CLPO shall provide the director of the NSA with an assessment of whether intelligence priorities were "established after appropriate consideration for the privacy and civil liberties of all persons". Further, sections 2(a)(ii)(A) and 2(c)(i)(A) provide that "signals intelligence does not have to be the sole mean […] available or used for advancing aspects of the validated intelligence priority".

It is also unlikely that the US president intended to bring the US authorities' understanding of proportionality in conformity with that of the CJEU. The Foreign Intelligence Surveillance Court (FISC) has been criticised for granting most of the surveillance requests by the NSA and has been characterised as a "rubber stamp court".[77] Moreover, statements made by the US government after the adoption of E.O. 14086 suggest that the US president did not intend to implement the proportionality test applied by the CJEU. The US Department of Justice issued a regulation stating that "[t]he Executive Order of October 7, 2022 and its terms shall be interpreted […] exclusively in light of United States law and the United States legal tradition, and not any other source of law".[78]

The US authorities can gain access to all forms of communications by means of bulk interception, including sensitive information that enjoys special protection under the Charter. The communication between a lawyer and his clients is protected under Art. 7 of the Charter and the sources of journalistic material are protected under Art. 11 of the Charter. Bulk interception of communications is arguably disproportionate in so far as information protected under the Charter could be included in the material obtained by national surveillance authorities. Although bulk interception under E.O. 14086 is subject to review by the CLPO and DPRC upon complaints, E.O. 14086 does not establish any procedure for prior authorisation or examination of intercepted material before it is released to the NSA. To ensure proportionality, the US authorities should consider establishing a procedure for re-

76 *Goitein*, The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance, Just Security, 31 October 2022, available at: https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/ (2/4/2024).

77 *Ackerman*, US senators push for special privacy advocate in overhauled Fisa court, The Guardian, 1 August 2013, available at: https://www.theguardian.com/law/2013/aug/01/fisa-court-bill-us-senate (2/4/2024).

78 See *supra* fn. 76.

moving sensitive information that enjoys protection under the Charter before it is obtained by the NSA.

V. Are the CLPO and the DPRC independent?

The bodies competent to review complaints relating to the lawfulness of surveillance measures must be independent. The CJEU has held that "[t]he concept of independence presupposes […] that the body concerned exercises its judicial functions wholly autonomously, without being subject to any hierarchical constraint or subordinated to any other body and without taking orders or instructions from any source whatsoever".[79] The right to a hearing by an independent tribunal is intrinsically linked to the respect for the rule of law.[80] The reference made by the CJEU to the respect for the rule of law in *Schrems II* suggests that the CJEU considered the Ombudsman mechanism's lack of independence to be clear and serious.

It is questionable whether the CLPO and the DPRC are independent. Sections 3(c)(iv) and 3(d)(iv) of E.O. 14086 provide that neither the director of the NSA nor the Attorney General shall interfere with the reviews by the CLPO and the DPRC. These provisions imply that the US president is committed to complying with the CJEU's judgement in *Schrems II*. However, both the CLPO and the DPRC are part of the executive branch of the US government and are not institutionally separated from either the NSA or the US president. Although it is not necessarily problematic that the CLPO and the DPRC are institutionally part of the executive branch, there must be safeguards put in place to ensure that the CLPO and the DPRC enjoy actual independence in the exercise of their functions in reviewing complaints pursuant to E.O. 14086.

One may question the sufficiency of the safeguards established by E.O. 14086 to ensure that the CLPO and the DPRC are independent. In particular, the judges of the DPRC are appointed by the Attorney General and their terms are renewable every fourth year.[81] The possibility of renewed terms may indirectly induce pressure on the judges to adopt judgements in favour of the NSA or other parts of the intelligence community.[82] In addition, as E.O. 14086 is the legal basis for the DPRC, the composition and competences of the DPRC can be changed by the US president at any time.[83] In principle, the judges can be fired and the judgements adopted by the DPRC can be overruled by the US president.[84]

79 CJEU, case C-64/16, *Associação Sindical dos Juízes Portugueses [GC]*, ECLI:EU:C:2018:117, para. 44.
80 *Lock/Martin*, in: Kellerbauer/Klamert/Tomkin (eds.), p. 2215; CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, para. 187.
81 *Gorski*, The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance, Just Security, 4 November 2022, available at: https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/ (2/4/2024).
82 Ibid.
83 See *supra* fn. 65.
84 Ibid.

The US Congress should for these reasons consider codifying E.O. 14086 into statutory law. The adoption of the E.O. 14086 suggests that the US president is of the understanding that E.O. 14086 is sufficient for US law to provide an adequate level of protection of personal data. However, a codification of E.O. 14086 into statutory law is necessary to ensure that the CLPO and the DPRC enjoy actual independence in the exercise of their functions in reviewing complaints.

VI. Does E.O. 14086 provide an effective remedy?

It is questionable whether E.O. 14086 complies with the equality of arms and adversarial principles. The CJEU has held that the equality of arms and adversarial principles "impl[y] an obligation to offer each party a reasonable opportunity of presenting its case in conditions that do not place it in a clearly less advantageous position compared with its opponent".[85] The equality of arms and adversarial principles are intrinsically linked together.[86]

The US president should consider amending E.O. 14086 to ensure compliance with the equality of arms and adversarial principles. The special advocate should be involved in the reviews by both the CLPO and the DPRC. According to section 3(d)(i)(C) of E.O. 14086, a special advocate is involved in the review by the DPRC, but not in the review by the CLPO. The lack of involvement of the special advocate in the review by the CLPO results in a purely inquisitorial process at this stage and complainants must apply for review by the DPRC for the NSA's understanding of the facts to be challenged. In addition, the NSA should be required to maintain documentation which demonstrates that the conditions for using surveillance measures have been met in every case. Under section 2(c)(iii)(E) of E.O. 14086, the NSA is required to maintain documentation only "to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected". Incomplete documentation by the NSA would make it difficult for the CLPO and the DPRC to assess whether there has been a violation, which would put the NSA in a more advantageous position than the data subjects.

National surveillance authorities must notify data subjects who have been subject to surveillance, as soon as notification is no longer liable to undermine the objective pursued by the surveillance.[87] According to Advocate General *Saugmandsgaard Øe* "[s]uch notification constitutes a prerequisite to the exercise of the right to a remedy under Art. 47 of the Charter".[88] There is no obligation under E.O. 14086 for the NSA to notify data subjects who have been subject to surveillance.[89] The US president should consider adding a provision to E.O. 14086 clarifying that data subjects

85 CJEU, case C-169/14, *Sánchez Morcillo*, ECLI:EU:C:2014:2099, para. 49.
86 *Lock/Martin*, in: Kellerbauer/Klamert/Tomkin (eds.), p. 2222.
87 See *supra* fn. 81; CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net [GC]*, ECLI:EU:C:2020:791, para. 190.
88 Opinion of AG Saugmandsgaard Øe, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2019:1145, para. 320.
89 See *supra* fn. 65.

who have been subject to surveillance shall be notified as soon as notification is no longer liable to undermine the objective pursued by the surveillance.

VII. Partial conclusions

E.O. 14086 does not provide a level of protection of personal data that is "essentially equivalent" to EU law. The first problem is that the legitimate objectives for surveillance are broadly defined and that the list of legitimate objectives may be amended without public announcement. This problem can be resolved by the US president requiring amendments to the list of legitimate objectives to be announced publicly, concretising the legitimate objectives and involving the special advocate in the reviews by both the CLPO and the DPRC. The second problem is that E.O. 14086 does not provide clarifications on the elements that shall be taken into account by US authorities when assessing proportionality. The US president should clarify that bulk interception of communication can only be exercised in so far as it constitutes a less restrictive mean and establishes a procedure for removing sensitive information before the information is obtained by the NSA. The third problem relates to the independence of the CLPO and the DPRC, as well as the lack of guarantees for data subjects. This problem may be resolved by the US Congress codifying E.O. 14086 into statutory law and imposing stricter documentation and notification requirements on the NSA.

As the US adequacy decision was adopted after E.O. 14086, it must be assumed that the European Commission's assessment is that the level of protection under US law as of July 2023 is adequate. A likely explanation why the findings in this section deviates from the assumed view of the European Commission, is that the European Commission and the US president may have been testing the boundaries set by the CJEU in *Schrems I* and *II*. The CJEU held in *Schrems I* and *II* that the level of protection of personal data provided by third countries does not have to be "identical", but rather "essentially equivalent", to the EU.[90] This suggests that there may be some differences between the level of protection provided by the EU and the US. However, the reasoning in *Schrems I* and *II* suggests that the CJEU is unwilling to compromise on compliance with the fundamental rights in the Charter.

D. Reflections on alternative measures that may ensure a level of protection of personal data that is "essentially equivalent" to the EU

I. Introduction

In this section, reflections are made on how the problems addressed by the CJEU in *Schrems I* and *II* can be resolved. The assumption is that E.O. 14086 does not provide a level of protection of personal data that is "essentially equivalent" to EU

90 CJEU, case C-362/14, *Schrems I [GC]*, ECLI:EU:C:2015:650, para. 73; CJEU, case C-311/18, *Schrems II [GC]*, ECLI:EU:C:2020:559, para. 162.

law. Three structural problems in US law are identified, namely the discrimination of foreign data subjects, the general nature of the surveillance and the lack of sufficient procedural safeguards. Alternative measures to those established by E.O. 14086 are proposed and evaluated.

II. The discrimination of foreign data subjects

Foreign data subjects are not provided with the same data protection and privacy rights as US data subjects under US law. Section 702 of FISA, which sets out the conditions for bulk interception, applies only to foreign nationals assumed to be located outside the territory of the US.[91] The legal bases in FISA that apply to US citizens only permit targeted surveillance.[92] Moreover, foreign data subjects enjoy no protection under the US constitution.[93] The right to be secure against unreasonable searches and seizures except when probable cause is provided, laid down in the fourth amendment to the US Constitution, applies only to US citizens.[94]As regards the status under international law, the US government has since the adoption of ICCPR insisted that the convention does not have extraterritorial application.[95] Although the discrimination of foreign data subjects under US law was not explicitly addressed by the CJEU in *Schrems II*, it is likely that the CJEU's assessment were influenced by this underlying problem.[96]

The discrimination of EU data subjects under US law could be justified by the recognition that also EU law contains elements of discrimination of foreign nationals. Although most of the fundamental rights provided by the Charter apply to both EU and foreign nationals, the prohibition of discrimination applies only to EU nationals.[97] Foreign nationals are excluded from the protection provided by the prohibition of discrimination set out in the Charter.[98] This reflects the fact that states may have legitimate interests in limiting the personal scope of application of fundamental rights to their own citizens or nationals. However, it is not intuitive that bulk interception regimes should target only foreign nationals. Acts of terrorism are also committed by nationals of the states towards which the acts are

91 *Margulies*, FLR 2014/5, p. 2140.
92 *Office Of The Director Of National Intelligence*, Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, April 2023, available at: https://www.intelligence.gov/assets/documents/702%20Documents/statistical-transparency-report/2022_IC_Annual_Statistical_Transparency_Report_cy2021.pdf (2/4/2024).
93 *Margulies*, FLR 2014/5, p. 2137.
94 Ibid.
95 *Nowak*, p. 43; *Margulies*, FLR 2014/5, p. 2143.
96 *Tzanou*, in: Fabbrini et al. (eds.), p. 20.
97 *Martin*, in: Kellerbauer/Klamert/Tomkin (eds.), p. 415; CJEU, joined cases C-22/08 and C-23/08, *Vatsouras,* ECLI:EU:C:2009:344, para. 52; CJEU, case T-452/15, *Petrov and others,* ECLI:EU:T:2017:822, para. 40.
98 *Martin*, in: Kellerbauer/Klamert/Tomkin (eds.), p. 415; CJEU, joined cases C-22/08 and C-23/08, *Vatsouras,* ECLI:EU:C:2009:344, para. 52; CJEU, case T-452/15, *Petrov and others,* ECLI:EU:T:2017:822, para. 40.

committed. This may lead one to question the rationale of targeting only foreign nationals. A straight-forward solution to this problem would be to provide foreign data subjects with the same rights as US data subjects. This is unlikely, as it would not only require amendments to FISA, but also necessitate amendments to the US constitution.

III. The general nature of the surveillance

It is questionable whether there is any reality in the claim that bulk interception can be proportionate. As bulk interception is extensive and intrusive, its permissibility must be construed narrowly. *Goitein* claims that "[t]he CJEU has held that bulk collection, as a general matter, violates international law".[99] However, the CJEU has not expressed itself as categorical as *Goitein*. The CJEU has accepted bulk interception of communications in pursuit of national security objectives.[100] In contrast, bulk interception undertaken to prevent serious crime exceeds what is necessary and proportionate.[101] Because of the extensive nature and intrusiveness of bulk interception, it is nevertheless difficult to imagine how a bulk interception regime could fulfil requirements of proportionality in practice.

Bulk interception allows the NSA to collect personal data without concrete suspicion relating to the possibility that the person will commit a criminal offence. According to the Office of the Director of National Intelligence, approximately 232.432 non-US persons were targeted by orders issued pursuant to section 702 of FISA in 2021.[102] The number of potential targets is sufficient to question whether bulk interception of communications as such can be proportionate. In addition, the number of potential targets makes it difficult to implement effective safeguards and guarantees for subjects whose personal data are processed following bulk interception.

An absolute prohibition of bulk interception of communications under US law is the least complicated and technical alternative that would ensure proportionality. The NSA and other parts of the intelligence community would be required to prove concrete suspicion in all cases surveillance measures are requested. However, requiring US law to lay down an absolute prohibition of bulk interception would risk undermining the sovereignty of the US and would raise questions about consistency and reciprocity.[103] Several EU member states operate their own bulk interception regimes. Among those EU member states, which officially operate systems for gen-

99 See *supra* fn. 76.
100 CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net [GC]*, ECLI:EU:C:2020:791, para. 137.
101 Ibid., para. 141.
102 See *supra* fn. 92.
103 *Gstrein/Beaulieu,* PT 2022/3, p. 1 ff.

eralised surveillance, are Finland, France, Germany, the Netherlands and Sweden.[104] The negotiations on the draft e-privacy regulation further suggest that EU member states wish to maintain their competences in national security, rather than restricting them.[105] Considering the impact of an absolute prohibition, it seems unlikely that the US will be willing to discuss this option. Only taking into account orders issued pursuant to section 702 of FISA, an absolute prohibition of bulk interception would mean that the NSA loses intelligence from more than 200.000 data subjects.[106]

An alternative is to reduce generalised surveillance in the US. As food for thought, it could increase the likelihood of an adequacy finding by the CJEU if generalised surveillance in the US was tied to certain boundary conditions, such as the appearance of a national emergency. Assessing this from a European perspective, Art. 15 ECHR allows the parties to the Convention to derogate from their obligations in times of national emergency. The ECtHR affords the parties a wide margin of appreciation in the interpretation and application of Art. 15 ECHR.[107] Derogations made in accordance with Art. 15 ECHR are in principle also compliant with the Charter.[108] If the use of generalised surveillance by US authorities would be limited to cases of national emergency, this could lead the CJEU in the direction that the level of protection of personal data in US law is "essentially equivalent" to the protection provided under EU law. However, one must bear in mind that the term "national emergency" raises questions around its interpretation,[109] and that generalised surveillance in the US in any event must be reduced drastically if wishing to pass the CJEU's scrutiny.

IV. The lack of sufficient procedural safeguards

The establishment of a special advocate to represent data subjects before FISC has been debated since the *Snowden* disclosures.[110] In August 2013, the US Senators *Blumenthal*, *Wyden* and *Udall* proposed to establish a special advocate to represent data subjects before FISC.[111] It was claimed that, during its 35-year history, FISC rejected only 11 out of more than 34.000 surveillance requests.[112] The special advocate was intended to contribute to adversarial proceedings before FISC.[113]

Proposals to establish a special advocate usually refer to a mechanism that enables the special advocate to participate in proceedings before a court, which is

104 ECtHR, App. nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and Others v. The United Kingdom [GC]*, para. 242; ECtHR, App. no. 35252/08, *Centrum för Rättvisa v. Sweden [GC]*, para. 131.
105 *Rojszczak*, Computer Law & Security Review 2021.
106 See *supra* fn. 92.
107 *Gerards*, p. 170.
108 *Lock*, in: Kellerbauer/Klamert/Tomkin (eds.), p. 2255.
109 ECtHR, App. no. 332/57, *Lawless v. Ireland (No. 3)*, para. 28.
110 *Vladeck*, A&M Law Review 2015.
111 See *supra* fn. 77.
112 Ibid.
113 Ibid.

competent to authorise surveillance, is properly equipped to act as a counter to the government, and has the ability to seek judicial review.[114] Although there is a link between the special advocate mechanism and the adversarial principle, the special advocate can also fulfil other functions. The risk that the NSA can obtain sensitive information protected under the Charter by means of bulk interception can be mitigated by a special advocate. A procedure, in which intercepted material is controlled and sensitive information protected under the Charter, is removed before the rest of the material is released to the NSA, should be considered.

The proposal to establish a special advocate to represent data subjects before FISC is in line with the jurisprudence of the ECtHR.[115] In *Chahal*, the ECtHR referred to the special advocate established under Canadian law.[116] The ECtHR held that "the use of confidential material may be unavoidable where national security is at stake [but that this does not mean] that the national authorities can be free from effective control by the domestic courts whenever they choose to assert that national security and terrorism are involved".[117] The ECtHR claimed that "in Canada a more effective form of judicial control has been developed in cases of this type".[118] The proposal to establish a special advocate in the US was nevertheless rejected and an *amicus curiae* was instead established by section 401 of the US Freedom Act.[119]

The *amicus curiae* in the proceedings before FISC has several weaknesses. First, the obligation to appoint an *amicus curiae* is vaguely formulated. The FISC can decide not to appoint an *amicus curiae* if it finds that the participation in the proceedings is "not appropriate".[120] Second, the *amicus curiae* is not entitled to receive full documentation in the cases in which they appear. It has only access to material "that [FISC] determines [is] relevant to the duties of the amicus curiae".[121] Third, there are constraints as regards the possibilities for judicial review of decisions made by FISC. The *amicus curiae* does not participate in FISC's certification for review by the Foreign Intelligence Surveillance Court of Review (FISCR).[122] Fourth, the *amicus curiae* is only involved in proceedings before FISC. The *amicus curiae* is not involved in the situation that the NSA seeks direct access to personal data through the procedure in E.O. 12333.

An innovation of the E.O. 14086 is the establishment of a special advocate to represent foreign data subjects before the DPRC. According to section 3(d)(i)(C) of E.O. 14086, a special advocate shall be involved in the review by the DPRC. The use of the expression "special advocate" can be understood as nothing less than a reference to the debate initiated by the US Senators *Blumenthal*, *Wyden* and *Udall*

114 *Squitieri*, WJLT 2015/3, pp. 200–201.
115 *Jackson*, JLS, 2019/1, p. 117.
116 ECtHR, App. no. 22414/93, *Chahal v. The United Kingdom [GC]*, para. 131; *Jackson*, JLS, 2019/1, p. 117.
117 ECtHR, App. no. 22414/93, *Chahal v. The United Kingdom [GC]*, para. 131.
118 Ibid.
119 *Squitieri*, WJLT 2015/3, pp. 198–199.
120 Ibid., pp. 204–205.
121 Ibid., p. 207.
122 Ibid., p. 209.

in August 2013.[123] The special advocate established by E.O. 14086 nevertheless has several weaknesses. The special advocate gets involved at a late stage of the complaint procedure and does not participate in the complaint procedure before the CLPO, but only in the procedure before the DPRC. Moreover, the special advocate established by E.O. 14086 is not involved in the fact-finding. In the complaint procedure before the CLPO and the DPRC, the NSA is responsible for the fact-finding in the form of providing documentation of the surveillance it has conducted. In addition, there is no appellate body to hear complaints over determinations made by the DPRC and the special advocate has no possibility of making the determinations of the DPRC subject to review.

The *amicus curiae* under the FISA and the special advocate under E.O. 14086 could with some adjustments contribute to adversarial proceedings and eliminate the possibility that the NSA obtains sensitive information protected under the Charter. For this purpose, the special advocate should take part in all stages of the proceedings and should be involved also where the NSA conducts surveillance by means of direct access pursuant to E.O. 12333. To avoid overburdening the US court system, new review procedures and the special advocate should in any event be accompanied by a significant reduction of generalised surveillance in the US.

V. Partial conclusions

This section has proposed and evaluated alternative measures under US law that may ensure a level of protection of personal data that is "essentially equivalent" to the EU. The first proposal is to provide foreign data subjects with the same rights as US data subjects or reduce the differences between the rights of US and foreign data subjects. The second proposal is to tie the permissibility of generalised surveillance in the US to certain boundary conditions, such as the existence of a national emergency. The third proposal is to provide a special advocate to represent foreign data subjects at all stages of the complaint procedure and in situations where the NSA conducts surveillance by means of direct access pursuant to E.O. 12333.

E. Conclusions

This article examined which changes the US government would have to make for the CJEU to consider the level of protection provided by US law to be adequate in the context of data protection and privacy law. The US would have to comply with the fundamental rights as set out in the Charter, but not with all the requirements as set out in the GDPR. The CJEU is unlikely to find that the failure of the US to provide the same rights as the GDPR, or to impose sanctions of the same severity as the GDPR, would result in the US failing to provide an adequate level of protection. However, the CJEU is likely to assess compliance with the fundamental

123 See *supra* fn. 77.

rights in the Charter with the strictest scrutiny, and this includes compliance with relative rights such as the right to data protection and privacy.

Amendments to E.O. 14086 are necessary to ensure compliance with the fundamental rights set out in the Charter. The most pressing shortcomings of E.O. 14086 are the authority of the US president to amend it without public announcement, the lack of concrete guidance on the meaning of proportionality, and the lack of codification of E.O. 14086 into statutory law. Mutual accommodation is needed to find a compromise if the situation is to be resolved. Otherwise, the future of transatlantic data flows is likely to remain uncertain.

Bibliography

BRINNEN, MARTIN; MAGNUSSON SJÖBERG, CECILIA; TÖRNGREN, DAVID; WESTMAN, DANIEL; ÖMAN, SÖREN, *Dataskyddet 50 år – Historia, aktuella problem och framtid*, Visby, 2023

GERARDS, JANEKE, *General Principles of the European Convention on Human Rights*, Cambridge, 2019

GIEGERICH, THOMAS, *Europäische Vorreiterrolle im Datenschutzrecht: Neue Entwicklungen in der Gesetzgebung, Rechtsprechung und internationalen Praxis der EU*, Zeitschrift für Europarechtliche Studien, 2016, Vol. 19(3), pp. 301–344

GREENLEAF, GRAHAM, *Japan and Korea: Different paths to EU adequacy*, Privacy Laws & Business International Report, 2018, pp. 9–11

GREENLEAF, GRAHAM, *Japan: EU Adequacy Discounted*, Privacy Laws & Business International Report, 2018, pp. 8–10

GREENLEAF, GRAHAM, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, Privacy Laws & Business International Report, 2021, pp. 3–5

GREENLEAF, GRAHAM, *Global Data Privacy Laws 2021: Uncertain paths for international standards*, Privacy Laws & Business International Report, 2021, pp. 23–27

GREENLEAF, GRAHAM, *Global Data Privacy Laws 2021: DPAs joining networks are the rule*, Privacy Laws & Business International Report, 2021, pp. 23–26

GREENLEAF, GRAHAM, *Now 157 countries: Twelve data privacy laws in 2021/22*, Privacy Laws & Business International Report, 2022, pp. 3–8

GSTREIN, OSKAR JOSEF, *Das Recht auf Vergessenwerden als Menschenrecht: Hat Menschenwürde im Informationszeitalter Zukunft?*, Baden-Baden, 2016

GSTREIN, OSKAR JOSEF, *Mapping power and jurisdiction on the internet through the lens of government-led surveillance*, Internet Policy Review, 2020, Vol. 9(3), pp. 1–17

GSTREIN, OSKAR JOSEF; ZWITTER, ANDREJ JANKO, *Extraterritorial application of the GDPR: promoting European values or power?*, Internet Policy Review, 2021, Vol. 10(3), pp. 1–30

GSTREIN, OSKAR JOSEF; BEAULIEU, ANNE, *How to protect privacy in a datafied society? A presentation of multiple legal and contextual approaches*, Philosophy & Technology, 2022, Vol. 35(3), pp. 1–38

JULIUSSEN, BJØRN ASLAK; KOZYRI, ELISAVET; JOHANSEN, DAG; RUI, JON PETTER, *The third country problem under the GDPR: enhancing protection of data transfers with technology*, International Data Privacy Law, 2023, Vol. 13(3), pp. 225–243

KUNER, CHRISTOPHER, *Transborder Data Flows and Data Privacy Law*, 1st edition, Oxford, 2013

KUNER, CHRISTOPHER; BYGRAVE LEE A.; DOCKSEY, CHRISTOPHER; DRECHSLER, LAURA, *The General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2019

KUNER, CHRISTOPHER, *Protecting EU Data Outside EU Borders under the GDPR*, Common Market Law Review, 2023, Vol. 60(1), pp. 77–106

LENAERTS, KOEN, *Exploring the Limits of the EU Charter of Fundamental Rights*, European Constitutional Law Review, 2012, Vol. 8(3), pp. 375–403

LENAERTS, KOEN; GUTIÉRREZ-FONS, JOSÉ A.; ADAM, STANISLAS, *Exploring the Autonomy of the European Union Legal Order*, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, 2021, Vol. 81(1), pp. 47–88

LOCK, TOBIAS, *The ECJ and the ECtHR: The Future Relationship between the Two European Courts*, The Law and Practice of International Courts and Tribunals, 2009, Vol. 8, pp. 375–398

KELLERBAUER, MANUEL; KLAMERT, MARCUS; TOMKIN, JONATHAN, *The EU Treaties and the Charter of Fundamental Rights – A Commentary*, Oxford, 2019

MANTELERO, ALESSANDRO, *The future of data protection: Gold standard vs. global standard*, Computer Law & Security Review, 2021, pp. 1–5

MARGULIES, PETER, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, Fordham Law Review, 2014, Vol. 82(5), pp. 2137–2167

NOWAK, MANFRED, *U.N. Convenant on Civil and Political Rights – CCPR Commentary*, 2nd edition, Kehl, 2005

ROJSZCZAK, MARCIN, *The uncertain future of data retention laws in the EU: Is a legislative reset possible?,* Computer Law & Security Review, 2021

RUSTAD, MICHAEL; KOENIG, THOMAS, *Towards a Global Data Privacy Standard*, Florida Law Review, 2019, Vol. 71(2), pp. 365–454

RYNGAERT, CEDRIC; TAYLOR, MISTALE, *The GDPR as Global Data Protection Regulation?,* American Journal of International Law, 2020, Vol. 114, pp. 5–9

SKULLERUD, ÅSTE MARIE BERGSENG; RØNNEVIK, CECILIE; SKORSTAD, JØRGEN; PELLERUD, MARIUS ENGH, *Personopplysningsloven og personvernforordningen (GDPR) – Kommentarutgave*, Oslo, 2019

SQUITIERI, CHAD, *The Limits of the Freedom Act's Amicus Curiae*, Washington Journal of Law, Technology and Arts, 2015, Vol. 11(3), pp. 198–210

STEINER, JOSEPHINE; WOODS, LORNA, *EU Law*, 10th edition, Oxford, 2020

SVANTESSON, DAN JERKER, *Extraterritoriality in Data Privacy Law,* Copenhagen, 2013

SVANTESSON, DAN JERKER, *The Extraterritoriality of EU Data Privacy Law: Its Theoretical Justification and its Practical Effect on US Businesses*, Stanford Journal of International Law, 2014, Vol. 50(1), pp. 53–103

SVANTESSON, DAN JERKER; KLOZA, DARIUSZ, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Brussels, 2016

SVANTESSON, DAN JERKER, *European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments*, Journal of Intellectual Property, Information Technology and E-Commerce Law, 2018, Vol. 9(2), pp. 113–125

TRACOL, XAVIER, *Schrems II: The return of the Privacy Shield*, Computer Law and Security Review, 2020, Vol. 39, pp. 1–11

TZANOU, MARIA, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter- Terrorism Surveillance*, Oxford, 2016

TZANOU, MARIA, *Schrems I and Schrems II: Assessing the Case for the Extraterritorality of EU Fundamental Rights*, in: Fabbrini, Federico; Celeste, Edoardo; Quinn, John (eds.), Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Oxford, 2021, pp. 99–116

VAN ALSENOY, BRENDAN, *Reconciling the (extra)territorial reach of the GDPR with public international law*, in: Vermeulen, Gert; Lievens, Eva (eds.), Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data, Antwerp, 2017, pp. 77–100

VLADECK, STEPHEN I., *The Case for a FISA "Special Advocate",* Texas. A&M Law Review, 2015

VLADECK, STEPHEN I., *The FISA Court and Article III*, Washington and Lee Law Review, 2015, Vol. 72(3), pp. 1161–1180

PEERS, STEVE; HERVEY, TAMARA; KENNER, JEFF; WARD, ANGELA, *The EU Charter of Fundamental Rights – A Commentary*, Oxford, 2014

POLČÁK, RADIM; SVANTESSON, DAN JERKER, *Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law*, Cheltenham, 2017