The inadequacy of the October 2022 new US Presidential Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities

by

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

November 2022

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

About the author:

Douwe Korff is a Dutch comparative and international lawyer specialising in human and digital rights. He is emeritus professor of international law at London Metropolitan University and visiting professor at the universities of Zagreb and Rijeka in Croatia; an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin.

He has carried out many studies relating to digital rights, data protection and surveillance for the EU, the Council of Europe, the UN (ITU), the British Commonwealth, and the UK authorities. This includes a 2021 study with Ian Brown for the European Parliament's civil liberties (LIBE) committee, Exchanges of personal data after the Schrems II judgment, that he draws on in this note (see footnote 6 for reference).

He works closely with civil society and digital rights groups including European Digital Rights (EDRi) and the Foundation for Information Policy Research (FIPR) in the UK.

Acknowledgment:

Just as I had started writing this note, I noticed the excellent two-part analysis of the new US Presidential Executive Order by Elizabeth Goitein and Ashley Gorski at:
https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/
https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/

I have taken the liberty to draw extensively on their summaries and analyses, merely expanding on specifically European issues. My conclusions fully chime with theirs.

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

CONTENTS

- o – O – o -

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

The inadequacy of the October 2022 new US Presidential Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities

1. Introduction

After the successive debacles over previous EU – US personal data flow arrangements, i.e., the "**Safe Harbor**" and "**Privacy Shield**" arrangements that were both struck down by the Court of Justice in, respectively, the Court's *Schrems I* (2015)[1] and *Schrems II* (2020)[2] judgments, in March this year the EU and the US authorities announced they had reached a new "political agreement" on data transfers that is apparently to be called the (new) **European Union-U.S. Data Privacy Framework (EU-US DPF)** (hereafter also referred to as "***the Framework***").[3] But little concrete results were shown until, on 7 October, the White House issued an Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities (hereafter: "***the Executive Order***" or "***the EO***") that is meant to address the deficiencies in US law – in particular, the excessively broad US surveillance laws and the lack of effective judicial redress under them for EU persons – identified by the EU Court, that led the Court to declare the previous arrangements invalid.[4]

In this note, I analyse the Executive Order and in particular seek to provide an early indication of whether it meets the requirements relating to third country surveillance activities indicated in the above-mentioned *Schrems I* and *Schrems II* judgments (and subsequent judgments), as reflected in the European Data Protection Board's European Essential Guarantees for surveillance (**EEGs**).[5] To this end, I first provide a brief overview of the Executive Order (section 2), followed by a brief overview of EU general legal standards for surveillance and the EEGs in particular (section 3, with reference to a more detailed write-up of the *Schrems* judgments and the EEGs by Ian Brown and myself in a report prepared for the European Parliament last year).[6] In section 4, I assess the arrangements set out in the Executive Order in more detail against the various stipulations in the EEGs. Section 5 provides a summary of my assessments and conclusions.

---

1 CJEU, Grand Chamber judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems I*"), ECLI:EU:C:2015:650

2 CJEU Grand Chamber judgment of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), ECLI:EU:C:2020:559.

3 See the Fact Sheet issued by the White House on the US Presidential executive order referenced in the next footnote, that uses this name for the new arrangement. The fact sheet is 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/

4 US Presidential Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, 7 October 2022, available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

5 EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

6 Ian Brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment, study carried out at the request of the European Parliament's Civil Liberties (LIBE) Committee, June 2021, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

2. The Executive Order (overview)

This section provides a brief overview of the EO. The elements and provisions of the EO relevant to the question of "adequacy" are discussed in section 4, with reference to the relevant EU standards, summarised in section 3.

The EO first of all sets out the **purpose** of US signals intelligence, which is, in the broadest terms:

> to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm (EO, section 1, discussed in sub-section 4.2)

Section 2(a) sets out **three principles** that must be followed in carrying out signals intelligence; in paraphrase:

- it must be appropriately authorised (by statute, executive order, Presidential Order, etc.) and undertaken in accordance with the US Constitution and applicable authorisations;
- it must be subject to appropriate safeguards to "*ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities*" and more specifically that "*the activities are **necessary** to advance a validated intelligence priority*" and "*conducted only to the extent and in a manner that is **proportionate** to the validated intelligence priority for which they have been authorized*";
- it must be "*subjected to* rigorous oversight *in order to ensure that they comport with the [above] principles*".

Section 2(b) contains a long list of what are stipulated to be "**legitimate objectives**", and by contrast "**prohibited objectives**", of signals intelligence, and a process for **validation** of specific activities in the light of those objectives.

Section 2(c)(i) seeks to clarify in some detail **how data collection is to be targeted and tailored**.

However, section 2(c)(ii) clarifies that while "*[t]argeted collection shall be prioritized*", **bulk collection (*that is by definition indiscriminate*: see section 4.3) can still be authorised** if "*the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection*", but only for **somewhat more limited objectives** (as also discussed there).

Section 2(c)(iii) requires the adoption and implementation of "*policies and procedures designed to **minimize the dissemination and retention of personal information collected through signals intelligence***", and rules on **data security and access**, **data quality**, the use of **queries of bulk collection** and **documentation**.

Section 2(c)(iv) addresses the need to **update and publish relevant policies and procedures**, subject to review by the Privacy and Civil Liberties Oversight Board (PCLOB)

Section 3 deals with the complex, multi-layer **individual redress mechanism** (as summarised in section 4.5, below).

Section 4 sets out a series of definitions, and section 5 contains a series of general, final provisions.

3. The European Essential Guarantees for surveillance

3.1 The broader European human rights-legal framework

In Europe, data protection is regarded as a fundamental, universal human right. This means that, in the broadest terms, any processing of personal data (broadly defined to include collection of personal data and anything done after collection with the data up to and including their destruction) must meet the standard human rights requirements of the European Convention on Human Rights and of the EU Charter of Fundamental Rights. In summary:

- The collection and further processing must be based on clear and precise, accessible (i.e., *publicly available*), and in their application foreseeable, legal rules ("**based on law**").
- It must serve a clear, specified and narrowly defined **legitimate purpose** ("purpose specification and limitation"); this means also that:
  - vague and broadly phrased purposes such as "business purposes", "law enforcement purposes" or "national security purposes" are not sufficient; they must be narrowed down in relation to any specific processing operation; and
  - a purpose is not "legitimate" simply because it is set out in law: "legitimate" [F: *licite*, D: *rechtmässig*] is wider than "lawful" [F: *légal*; D: *gesetzmässig*]); processing of personal data may, for instance, not lead to discrimination.
- The processing and the data must be "**necessary**" and "**proportionate**" *in relation to the specified and narrowly-defined legitimate aim* – and *strictly* necessary and *clearly* proportionate to that aim if the data are in any way sensitive or intrusive, or the results of the processing can significantly affect fundamental rights.

  (Cf. Article 8 – 11 ECHR; Article 52 EU CFR)

And, crucially:

- Whether a law authorising processing of personal data, and any actual specific personal data processing operation carried out under such a law, meets the above standards (any and all of the above standards) must be **justiciable**; and more in particular:
- **Individuals who are affected by the processing (or who can reasonably argue they may be affected by it) must have an effective judicial remedy** against any processing that does not meet any of the above tests, i.e., that is (*in the view of the competent court*) not based on a sufficiently clear legal rule, does not serve a sufficiently clearly defined legitimate aim, has wrong consequences (such as discrimination or excessive false positives), or that is not necessary or proportionate to the relevant legitimate aim.
- (Cf. Article 13 ECHR; Article 47 of the EU CFR)

The European Essential Guarantees for surveillance must be read within this fundamental, constitutional European legal framework (as is often expressly stated in them, as noted next).

3.2 The European Essential Guarantees for surveillance (a re-cap)

Ian Brown and I have summarised the reasons why the EU Court of Justice invalidated the "Safe Harbor" and "Privacy Shield" arrangements in our 2021 study for the European Parliament in some detail, with reference to the relevant passages in the *Schrems I* and *II*, *Privacy International* and *La Quadrature du Net* judgments.[7] As also pointed out there, the European Data Protection Board's European Essential Guarantees for surveillance measures (EEGs) are clearly and expressly based on those judgments and on the broader legal framework set out in the previous sub-section:[8]

> Following the analysis of the jurisprudence, the EDPB considers that the applicable legal requirements to make the limitations to the data protection and privacy rights recognised by the Charter [for the purposes of national security] justifiable can be summarised in four European Essential Guarantees:
>
> A. Processing should be based on clear, precise and accessible rules [that are foreseeable in their application];
>
> B. [Strict] necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated [which must relate to a serious threat to national security that is shown to be genuine and present or foreseeable];
>
> C. An independent oversight mechanism should exist; and
>
> D. Effective remedies need to be available to the individual.
>
> The Guarantees are based on the fundamental rights to privacy and data protection that apply to everyone, irrespective of their nationality.

The EEGs expand on each of these guarantees; the words added by me to the above list in square brackets paraphrase the relevant sections. More specifically, the requirement that all processing of personal data – including any collecting, filtering, analysing or using such data for national security purposes – must be based on clear, precise and accessible rules that are foreseeable in their application ("**based on law**") – Guarantee A – reflects a general, fundamental European human rights and rule of law principle, as noted at 3.1.

The requirements relating to Guarantee B ("**legitimate purpose**" and "**strict necessity and proportionality**") are derived from the CJEU judgment in *La Quadrature du Net*:[9]

> In *La Quadrature du net and others*, it can be noted that the CJEU ruled, in relation to the law of a Member State and not to a third country law, that the objective of safeguarding national security is, due to its importance, capable of justifying measures entailing more

---

[7] Ian Brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment (footnote 4, above), section 2.3.1.3, *Requirements relating to access to personal data by state authorities*, under the heading "*CJEU requirements relating to indirect or direct access to personal data by third country intelligence agencies*", pp. 42 – 45. For references to *Schrems I* and *II*, see footnotes 1 and 2, above. The other judgments are:
CJEU, GC judgment in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020, ECLI:EU:C:2020:790.
CJEU, GC judgment in Joined Cases C-511/18, C-512/18, *La Quadrature du Net v. France*, and C-520-18, *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL and others v. Belgium*, 6 October 2020, ECLI:EU:C:2020:791.

[8] EDPB, European Essential Guarantees for surveillance measures (footnote 5, above), para. 24.

[9] EDPB, European Essential Guarantees for surveillance measures (footnote 5, above), para. 34.

> serious interferences with fundamental rights, than those which might be justified by other objectives such as of combating crime. It found however that this is the case as long as there are sufficiently solid grounds for considering that the State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable and subject to meeting the other requirements laid down in Article 52(1) of the Charter.[10]

In line with this, in that same judgment, just before the above, the Court of Justice gave the following **definition of national security** that must also be seen as **the only "legitimate" "specified purpose" of national security in terms of European law**:[11]

> That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.

This is similar to the derogation clause in the European Convention on Human Rights that refers to "*time[s] of war or other public emergency threatening the life of the nation*" (Article 15).

This has **implications for the tests of necessity and proportionality**. As the Board explained in a footnote to the earlier quote:[12]

> [In *Privacy International* the Court specified that threats to national security] can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. § 75. For instance, in *La Quadrature du Net and others*, the Court noted that **the automated analysis of traffic and location data covering generally and indiscriminately the data of persons using electronic communications systems constitutes an interference particularly serious so that, such measure can meet the requirement of proportionality only in situations in which the Member State concerned is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and, among other conditions, provided that the duration of the retention is limited to what is strictly necessary** (§§174-177).

On the issue of **procedural/enforcement guarantees** (Guarantees C and D), the Board has pointed out elsewhere, with reference to *Schrems I*, that, in relation to the issue of access to data by a third country intelligence agencies:[13]

> [a]lthough the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union, a system consistent with the European one must be [in place].

---

10 *La Quadrature du Net and others*, §§ 136 and 137. [*original footnote, remainder quoted in the text*]

11 *Idem*, para. 135.

12 EDPB, European Essential Guarantees for surveillance measures (footnote 5, above), para. 34, footnote 36, emphasis added.

13 Article 29 Working Party, Adequacy Referential, adopted on 28 November 2017, as last revised and adopted on 6 February 2018 (WP254rev01), section C, available at:
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108/
The referential was endorsed by the EDPB:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

Such a system, it said, is "*characterized by the existence of the following elements*":[14]

- there must be one or more "completely independent" and impartial supervisory authorities with effective supervisory and enforcement powers;
- the system should ensure "a good level of compliance" in practice, which can be ensured through sanctions, verifications and audits;
- the system should ensure accountability, by "oblig[ing] data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority", e.g., through data protection impact assessments, the keeping of records or log files of data processing activities, the designation of data protection officers, or data protection by design and by default; and
- the system must provide "support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms".

In the next section, I assess (with reference also to the analyses by Elizabeth Goitein and Ashley Gorski) whether the Presidential Executive Order that is supposed to create the basis for the proposed new EU-US Data Privacy Framework meets the standards set out in the EEGs.

4. The EO assessed against the requirements of the EEGs

4.1 Does the EO have the "quality of law"?

i. EU legal standards

In European legal terms, any processing of personal data – including the mere collection or "hoovering up" of such data – *ipso facto* constitutes an interference with the data subjects' rights to data protection and private life, and must therefore be based on law. Moreover, as noted in section 3.1, above, under European human rights instruments, the question of whether a set of rules can be said to constitute "law" is not a merely formal one. Rather, an interference with a fundamental rights can only be said to be based on "law" if the relevant set of rules have what the European Court of Human Rights calls "the quality of law": they must be clear and precise, accessible (i.e., *publicly available*), and in their application foreseeable.

ii. The EO

The sweeping nature and vagueness of the purposes for which the US agencies can exercise their surveillance powers under the EO, noted in the next sub-section, in themselves raise serious doubts as to whether the rules are "foreseeable in their application" and prevent arbitrary uses of the sweeping surveillance powers granted. But the crucial issue is that the order gives the Presidenct the right to change the lists of purposes for which "signals intelligence", respectively "bulk collection", may be used **in secret:**

> The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that signals intelligence collection activities may be used. The Director of National Intelligence (Director) shall publicly release any updates to the list of

[14] *Idem* (paraphrased).

> objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.
>
> (section 2(b)(i)(B), repeated *verbatim* in section 2(c)(ii)(C), with the words "bulk collection" substituted for the words "signals intelligence collection")

As Goitein puts it:[15]

> [T]he order gives the president authority to expand the list of objectives – and to do so secretly, if publishing the updated list "would pose a risk to the national security of the United States." The order thus expressly endorses the possibility of secret law,[16] including its most pernicnous variant: a set of secret rules that differs from the publicly available version, thus actively misleading the public.

She rightly concludes that:

> It is hard to imagine that the CJEU will be satisfied with a set of paper constraints that might or might not match those actually in force.

In fact, this ties in with a wider problem of "secret law" in the USA. As Brown and I pointed out in our 2021 report in relation to the rules we covered (that are still in place) and with reference to Goitein:

> **"Secret law"**
>
> While the publication of E.O. 12333 and PPD-28 provides a greater level of transparency than in many other countries,[17] it is still the case 'the president may "modify" or "waive" them simply by departing from their terms, without providing any notice to the public.'[18]
>
> Even with statutory provisions, the US Department of Justice's Office of Legal Counsel (OLC) regularly issues classified legal interpretations on national security matters which are binding on the executive branch. If a court later disagrees, the Justice Department will still not "investigate or prosecute somebody for acting in reliance" on such an opinion.[19] Such opinions were used during the George W. Bush administration to justify US torture and warrantless surveillance, with a later Bush-appointed attorney-general (Jack Goldsmith) observing OLC lawyers dealt with the Foreign Intelligence Surveillance Act "the way they dealt with other laws they didn't like: they blew through them in secret based on flimsy legal

---

15 Elizabeth Goitein, The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance, 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/

16 Elizabeth Goitein, *The Government's Addiction to 'Secret Law'*, New York Times, 18 October 2016, available at: https://www.nytimes.com/2016/10/18/opinion/the-governments-addiction-to-secret-law.html [*original link*]

17 Ian Brown, Morton H. Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, Towards Multilateral Standards for Surveillance Reform, In Russell A. Miller (ed., 2017) Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, Cambridge University Press, pp.461–491.

18 Elizabeth Goitein, The New Era of Secret Law, Brennan Center for Justice at New York University School of Law, 2016, p.5, at: https://www.brennancenter.org/sites/default/files/2019-08/Report_The_New_Era_of_Secret_Law_0.pdf

19 *Ibid*. p.37.

> opinions that they guarded closely so no one could question the legal basis for the operations."[20]
>
> Congressional committees, particularly the permanent intelligence committees, frequently issue reports with classified annexes. Some of these are important for the interpretation of statutes, and in some cases their provisions are incorporated by reference into legislation.[21] And the Foreign Intelligence Surveillance Court's decisions, such as authorising surveillance programmes under FISA s.702, can contain significant legal interpretations. One example was the Court's interpretation of s.215 of the Patriot Act, on whether business records sought by the government were "relevant" to a terrorism investigation, to cover almost every American's phone records.[22]
>
> While important FISC opinions have been declassified and published by the Director of National Intelligence, which is now required by the USA Freedom Act of 2015, one 2016 assessment "ascertained that most of the significant pre-Snowden FISA case law remains undisclosed, including 25-30 still-classified opinions or orders issued between mid-2003 and mid-2013 that were deemed significant by the Attorney General."[23]

iii. Assessment

In my opinion:

The Presidential Executive Order is not clear or precise or foreseeable in its application, and can be secretly amended by the president. It does not have the "quality of law" required under European human rights standards.

4.2 Does the EO ensure that US signal intelligence will serve only "legitimate" national security purposes?

i. EU legal standards

As noted at 3.2, above, according to the EU Court of Justice, in terms of EU law, a state's activities can only said to serve that state's "national security" if the activities are aimed at protecting "***the essential functions of the State*** *and* ***the fundamental interests of society***"; and this can be said to be the case in relation to "***the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country*** *[or] of* ***directly threatening society, the population or the State itself****, such as terrorist activities*".

ii. US law and the EO

As Brown and I noted in our 2021 report,[24] section 702 of the US Foreign Intelligence Surveillance Act (FISA), that is still in place, allows the use of "signal intelligence capabilities" to collect and use

---

20 *Ibid*. p.38.
21 *Ibid*. pp.29—31.
22 *Ibid*. p.58.
23 *Ibid*. p.6.
24 Ian Brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment (footnote 4, above), section 3.2, *US surveillance laws*.

"foreign intelligence information"; and in relation to non-US persons, that term includes not only information that relates to threats against the USA (§ 1801, para. (e)(1)), but also:

> **information** with respect to a foreign power or foreign territory that **relates to**, … —
>
> (A) the national defense or the security of the United States; or
>
> (B) **the conduct of the foreign affairs of the United States**.
>
> (§ 1801, para. (e)(2), emphases added. In relation to US persons the information must be "necessary" for these purposes.)

Executive Order (EO) 12333 furthermore allows the collection and use of this kind of information also "*for foreign intelligence and counterintelligence purposes to support national and departmental missions*".

Although Presidential Policy Directive (PPD) 28 placed limits on the use of signals intelligence collected in "bulk" by the intelligence community for certain purposes, we still noted that:

> the CJEU invalidated the EU Commission Privacy Shield decision because it determined that FISA Section 702 and E.O. 12333, even as limited by PPD-28, are too permissive to meet the GDPR's standards of necessity and proportionality ...

We concluded, in relation to the present issue, that:

> The laws (in particular FISA) do not require surveillance measures to serve a "legitimate purpose" in a democratic society: they allow, e.g., espionage for political or economic purposes.

The 7 October Executive Order is much more detailed than FISA S. 702 and EO 12333 in listing the purposes ("**objectives**") for which signal intelligence and bulk data collection capabilities may be used, and in stressing the need to consider the rights of the individuals affected.

In the broadest terms, it stipulates that the relevant capabilities may only be used for "**validated intelligence priority objectives**"; that they may not be used for **prohibited objectives**; and that in determining whether a specific capability should be used, the "*the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside*" must be considered (section 2(a)(ii)).[25]

The objectives in relation to which the use of signal intelligence capabilities generally can be legitimate are listed in section 2(b)(i); and a further list of more restrictive objectives in relation to which bulk collection of data (such as extraction of data from the global Internet communication cables) can be authorised is set out in section 2(c)(ii)(B).

Many of the listed objectives clearly fall within the ambit of "national security" as understood by the EU Court of Justice, e.g.:

- "*understanding or assessing the capabilities, intentions, or activities of … international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners*" (section 2(b)(i)(2), cf. also section 2(c)(ii)(B)(1): "*protecting against terrorism*"); or

[25] The EO also provides for a process for validation that I will discuss in sub-section 4.3, below.

- "*protecting against threats from the development, possession, or proliferation of weapons of mass destruction …* " – first sub-sentence of sections 2(b)(i)(7) and 2(c)(ii)(B)(3)).*

  * On the stipulations in the second parts of these sections, see the further list, below.

However, some of the other purposes (objectives) for which signals intelligence capabilities (including collection of data in bulk), can be used are at odds with the European concept of national security. For example, signals intelligence capabilities and bulk collection of data can still be authorised for these broadly phrased purposes:

- "*protecting against … threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person*" (section 2(b)(i)(7), section 2(c)(ii)(B)(3));*

  * The words after the "…" constitute the second parts of these sections; the two parts are connected by the word "and", i.e., the threats listed here need not relate to the threats covered by the first parts of these sections (quoted above), that concern threats relating to weapons of mass destruction.

- "*protecting against … the holding of individuals captive … conducted by … a … foreign person*" (sections 2(b)(i)(5) and 2(c)(ii)(B)(1));

- "*protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person*" (sections 2(b)(i)(6) and 2(c)(ii)(B)(2)) – i.e., in effect, any counter-espionage purpose;

- "*protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a … foreign person*" (sections 2(b)(i)(6) and 2(c)(ii)(B)(2));

- "*protecting against threats to the personnel of the United States or of its allies or partners*" (sections 2(b)(i)(9) and 2(c)(ii)(B)(5));

- "*protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in [subsections (b)(i) and/or 2(c)(ii)(B)]*" (sections 2(b)(i)(10) and 2(c)(ii)(B)(6)).

Authorisation of signals intelligence and/or bulk data collection for the above (as for any) of the listed objectives is subject to a prohibition of the use of such capabilities for the following **prohibited objectives**:

- suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;
- suppressing or restricting legitimate privacy interests;
- suppressing or restricting a right to legal counsel; or
- disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.

And it is also "not a legitimate objective" to:

- collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business

> sectors commercially. The collection of such information is authorized only to protect the national security of the United States or of its allies or partners.

But those prohibitions do not otherwise affect the sweeping nature of the objectives listed above. The crucial point is that the broadly-phrased threats mentioned there (in the first and penultimate indents indeed *any* threats) are not qualified so as to relate to what the Court of Justice considers legitimate national security aims. Not all kidnappings or even assassinations or (unqualified) "*threats to the personnel of the United States or of its allies or partners*", let alone all "*cybersecurity threats*", or all "*transnational criminal threats*" related to such other threats, are "*capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country [or] of directly threatening society, the population or the State itself*". Many of the above-listed tasks should in all but the most exceptional circumstances be the responsibility of ordinary law enforcement agencies operating under normal rule of law conditions and requirements (including where appropriate mutual assistance procedures) – and not of much less constrained intelligence agencies.

iii. Assessment

On the basis of the above, I can only conclude that:

The purposes for which the Presidential Executive Order allows the use of signal intelligence and bulk data collection capabilities are clearly <u>not</u> limited to what the EU Court of Justice regards as legitimate national security purposes. From the EU legal perspective, this is a lethal defect in the new regime that is fundamentally incompatible with the EU Charter of Fundamental Rights.

4.3 Does the EO ensure that US signal intelligence will always be limited to what is "necessary" and "proportionate in relation to legitimate national security purposes?

i. EU legal standards

The European tests of "necessity" and "proportionality" are not absolute but relative: the necessity and proportionality of any measure that interferes with fundamental rights (such as collecting, analysing and using personal data) can only be determined in relation to the relevant (narrowly specified) purpose. Actions that can be considered necessary and proportionate to serve one purpose (e.g., to protect against terrorism, or to counter serious crime) may be not necessary or proportionate to serve another purpose (e.g., to advance a country's economic interests, or to counter minor crimes, or to send targeted marketing messages to individuals).

In addition, as the Court of Justice put it in its *Schrems II* judgment:[26]

> a legal basis [i.e., a legal instrument such as the EO] which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, **itself define** the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.

[26] CJEU, *Schrems II* judgment (footnote 2, above), para. 180, emphasis added.

Moreover, measures that affect the "**essence**" of a fundamental right can never be necessary or proportionate to any purpose – not even to the purpose of protecting national security as defined by the Court. In its *Schrems I* judgment, the EU Court of Justice held that:[27]

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

The Court qualified this somewhat in its judgment in *La Quadrature du Net* (*LQDN*) in relation to the kinds of threats to "*the essential functions of the State and the fundamental interests of society*", already noted at 4.2, above:[28]

> [EU law including the Charter of Fundamental Rights] does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services **to retain traffic and location data of all users of electronic communications systems *for a limited period of time***, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a ***serious threat***, as referred to [above], to national security which is shown to be ***genuine and present or foreseeable***. Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection … with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.

As the European Data Protection Board explained in its EEGs:[29]

> **[T]he automated analysis of traffic and location data** covering ***generally and indiscriminately*** the data of persons using electronic communications systems constitutes an interference particularly serious so that, such measure can meet the requirement of proportionality only in situations in which the Member State concerned is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and, among other conditions, provided that the duration of the retention is limited to what is strictly necessary.

In other words, under EU law:

- instruments authorising surveillance should never allow for the indiscriminate capturing, analysis and use of **communications content data**: that can never be necessary or proportionate, even in relation to the most serious threats to "the essential functions of the State and the fundamental interests of society";
- such instruments may only impose the mandatory retention and making available (to the intelligence agencies) of **communications traffic and location (meta-)data** in extreme situations, for a strictly limited period (and, one might add, in defined geographical areas) when there is a specific, real threat to those essential functions and interests. For instance,

---

27 CJEU, *Schrems I* judgment (footnote 1, above), para. 94, with reference to its earlier judgment in *Digital Rights Ireland*. Emphases added.

28 CJEU, *LQDN* judgment (footnote 7, above), para. 137, emphases added.

29 EDPB, European Essential Guarantees for surveillance measures (footnote 5, above), para. 34, footnote 36, with reference to *LQDN*, paras. 174 – 177, emphasis added.

if the intelligence agencies receive specific, credible intelligence that a particular terrorist group will carry out an attack in a particular area, in a certain period and

- outside of such extreme situations, the *indiscriminate* mandatory retention, analysis and use of communications data (content and metadata) will never be "necessary" or "proportionate" in terms of EU (fundamental rights) law: only ***targeted*** measures can meet those criteria. Thus, outside of such extreme situations, meta- and content data should only ever be obtained (or made subject to a "data freezing" [preservation] order) if there is a link, if perhaps only indirectly, between the individuals whose communication data are to be obtained and a relevant serious crime or serious threat to public order or safety.[30]

ii. The EO

In terms of limiting the use of signal intelligence and bulk data collection , the EO first of stipulates that the relevant capabilities may only be used for "**validated intelligence priority**" purposes (section 2(a)(ii)), and provides for a **process for validation** that is to ensure that an intelligence priority is only "validated" (approved) if:

- the priority "advances" one or more of the legitimate objectives discussed in the previous sub-section;
- the priority is "*neither … designed [to] nor … anticipated to result in*" signals intelligence collection in contravention of the prohibited objectives also noted there; and
- the priority is established only "*after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside*".

  (section 2(b)(iii)(A))

Given the still excessively broadly defined (legitimate) "objectives" of signal intelligence and bulk data collection, noted in the previous sub-section, the first two conditions do not limit the use of such capabilities to what under EU law can be considered "necessary" and "proportionate" to legitimate national security purposes. And the requirement that "appropriate consideration" must be given to the privacy and civil liberties of those affected in itself also does not ensure compliance with EU standards of necessity and proportionality in these contexts (although recognition that the rights and liberties of all persons, "*regardless of their nationality or wherever they might reside*" is a significant advance in terms of US law).[31]

In addition to the stipulations about validated intelligence priorities, the Executive Order mentions necessity, proportionality, the achievement of "a proper balance" and "targeting"in several places, including in these sections (emphases added):

---

30 Cf. also CJEU, *Privacy International* judgment (footnote 7, above), paras. 77 – 78 (referenced by the EDPB).

31 Cf. Ian Brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment (footnote 4, above), section 2.2, *Fundamental matters*, sub-section 2.2.1, *In Europe, data protection is a fundamental right*, under the heading "The principle of universality of human rights (and therefore of data protection)", where we noted that "the USA does not accept this principle of universal/extraterritorial application of international human rights law or of the international human rights treaties to which it is a party"

> [S]ignals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are **necessary** to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority.
>
> (section 2(a)(ii)(A), repeated almost *verbatim* in relation to "specific signals intelligence collection activit[ies]" in section 2(c)(i)(A))
>
> [S]ignals intelligence activities shall be conducted only to the extent and in a manner that is **proportionate** to the validated intelligence priority for which they have been authorized, with the aim of achieving a **proper balance** between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.
>
> (section 2(a)(ii)(B))
>
> Signals intelligence collection activities shall be **as tailored as feasible to advance a validated intelligence priority** and, taking due account of relevant factors, **not disproportionately impact privacy and civil liberties**. Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.
>
> (section 2(c)(i)(B))
>
> **Targeted collection shall be prioritized.** The bulk collection of signals intelligence shall be authorized only based on a determination — by an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees — that **the information necessary to advance a validated intelligence priority** cannot reasonably be obtained by targeted collection. **When it is determined to be necessary to engage in bulk collection in order to advance a validated intelligence priority, the element of the Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.**
>
> (section 2(c)(ii)(A))

iii. Assessment

The main issue of concern from an EU perspective is the issue of "**bulk collection**". This is defined as:

> [T]he authorized collection of large quantities of signals intelligence data 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).

In other words, *"bulk collection" as practiced by the USA (in close cooperation with the UK and the other "Five Eyes" countries, Australia, Canada and New Zealand), is by definition indiscriminate*; it is not limited to data that has some link, even indirectly, to any serious threat or known person. It refers to what the Court of Justice of the EU calls the collection of data "on a generalised basis". Only after (bulk) collection is there an attempt to filter out data that are not relevant, necessary or proportionate to the relevant objective.[32]

The above means that it is an inherent feature of bulk collection that most of the data that are "hoovered up" (in particular, from the Internet backbone cables) are manifestly not necessary or proportionate – indeed, not even in any way relevant – in relation to any legitimate purpose including the protection of national security (as narrowly defined by the EU Court): the Order explicitly clarifies that, in the view of the US intelligence agencies, in some (many?) situations, "*information [that is] necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection*", and that therefore the "net" is cast widely, to collect bulk data that will mostly not be relevant, so as to extract some silver needles from the resulting haystack (to mix my metaphores). As Goitein observes:[33]

> Bulk collection – the collection of communications or other data not tied to any particular surveillance target – is inherently problematic, because it inevitably results in the collection of private information that the government has no legitimate need to collect. The EO attempts to mitigate the privacy incursion through back-end "minimization" requirements, which include limiting the retention of non-pertinent data. But these requirements roughly mirror those currently in place for U.S. persons, under which agencies may retain data for five years or even longer in many cases. As further detailed [later in her paper], these post-collection constraints do not and cannot cure the massive intrusion on privacy that bulk collection entails.
>
> To engage in bulk collection, an element of the Intelligence Community must determine that it is necessary to do so. The order's "necessity" standard, however, applies to all forms of surveillance, bulk and otherwise. Requiring such a finding for bulk collection does not impose an further limitation on this particularly dangerous form of surveillance. All it does is endorse the notion that bulk surveillance may sometimes be necessary. The order also requires intelligence agencies to apply "reasonable methods and technical measures" to limit the acquisition of non-pertinent data. But without additional information about what these measures are, how well they work, and what will lead intelligence agencies to deem

---

[32] For a description of the joint UK-US bulk collection of communications data from the global Internet cables, see Ian Brown and Douwe Korff, The inadequacy of UK data protection law in general and in view of UK surveillance laws, *Part Two on UK surveillance law*, November 2020, section 2.2.2, *Indiscriminate collection in bulk*, available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf
This first describes "*What is collected and how*" and then discusses whether this collection "*Is targeted or indiscriminate*", concluding it is the latter. The paper draws on a more detailed descriptions of the relevant practices by Greg Nojeim for the Center for Democracy & Technology (CDT), *Not a Secret: bulk interception practices of intelligence agencies*, 2019, available at:
https://cdt.org/insights/not-a-secret-bulk-interception-practices-of-intelligence-agencies/

[33] Elizabeth Goitein, The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance (footnote 15, above), pp. 4 – 5.

> them "reasonable", it is impossible to assess whether this requirement will have any measurable impact.
>
> The order contains some limits on how the government may use information collected in bulk. These limits are actually somewhat *less* restrictive then those set forth in Presidential Policy Directive 28 (PPD-28) issued by President Obama, which the new order replaces. They are actualized through a weak requirement that queries of bulk-collected data be "consistent" with such uses, which could in theory permit a query based on the smallest possible chance that it might return relevant information (as opposed to a requirement that a query be reasonably likely to return relevant information). And once again, the order authorizes the president to loosen these restrictions in secret.

She adds, specifically as concerns the issue of "necessity" and "proportionality", that:[34]

> The U.S. government's use of bulk collection – and the scope of any targeted collection – ostensibly would be limited by the order's requirement that surveillance be necessary to advance, and [be] proportionate to, a validated intelligence priority. **"Necessity" and "proportionality" are key terms in international law; they are the primary legal yardstick by which European courts will measure U.S. surveillance authorities. On their own, however, they are too vague and subjective to provide much guidance. Unless the United States intends to rely on the body of international case law interpreting and applying these terms, their inclusion in the order is little more than legal window dressing.**
>
> **The Department of Justice has disclaimed any such intent.** In regulations accompanying the issuance of the executive order,[35] the Department stated 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*" (emphasis added). It is one thing to acknowledge the truism that the United States is not bound by non-U.S. courts in this context. It is another altogether to assert that the United States will rely only on U.S. law, without considering international courts' rulings, in construing terms borrowed from international law. **This pronouncement gives little confidence that the "necessary and proportionate" test will be applied in a way that provides any meaningful check on U.S. surveillance activities.**
>
> Indeed, the proportionality test set forth in the order is already flawed. The order requires that surveillance activities be conducted in a manner proportionate "to the validated intelligence priority for which they have been authorized." Although the National Intelligence Priorities Framework is classified, much of it is reflected in the unclassified Worldwide Threat Assessment,[36] which often describes threats in highly general terms.[37] Such threats have included, for example, "organized crime" and "migration."

---

34 *Idem*, p. 5, emphasis added.

35 https://www.justice.gov/opcl/page/file/1541321/download [*original link that however does not open*]
The correct link is provided in Part 2 and is to this page:
https://www.ecfr.gov/current/title-28/chapter-I/part-201
The words quoted are in § 201.10, *Guiding principles of law*, at (a).

36 https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2015/item/1171-odni-general-counsel-robert-litt-s-as-prepared-remarks-on-signals-intelligence-reform-at-the-brookings-institute [*original link*]

37 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf [*original link*]

> **Proportionality will thus be considered at an extremely high level of generality, with more important priorities ostensibly justifying broader and more intrusive surveillance.**
>
> This odd formulation makes it far too easy to justify bulk or mass surveillance simply by pointing to the importance of the ultimate goal. Instead, the proportionality test should take place at the level of specific surveillance decisions, and it should be based on the likely outcome of that surveillance rather than the general priority it serves. In other words, in any given instance, the level of privacy intrusion—as measured by the type of data obtained, the duration of surveillance, the scope of incidental collection, and other such factors—should be proportionate to the particular information the analyst expects to obtain.

The view that indiscriminate bulk collection of data can be necessary for vaguely defined intelligence purposes may be shared by the intelligence agencies of other countries including those of the UK (and several EU Member States). But it is at odds with the case-law of the EU Court of Justice.

Specifically:

- the EO does not envisage any absolute prohibition of indiscriminate bulk collection of communications content data (such as the EU Court has imposed in *Schrems I*);
- the EO does not limit the indiscriminate collection of communications metadata (traffic and location data) to immediate, temporary, serious threats to "*the essential functions of the State and the fundamental interests of society*" (such as the Court required in *LQDN*); and
- the EO allows the use of bulk collection of data for any of the excessively broadly phrased purposes I noted in the previous sub-section (i.e., to counter any kind of general threat; kidnapping; any kind of cybersecurity threat; any kind of threat against US personnel; any kind of foreign espionage; etc.).

In my opinion, it follows from the above that:

The Presidential Executive Order does not limit signal intelligence generally, and indiscriminate bulk collection of personal data inclusing e-communications content and metadata in particular, to what is considered "necessary", "proportionate" and "legitimate" in relation to national security under EU law. In particular:

- **the EO 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.**

4.4 Does the EO provide for an independent oversight mechanism?

i. EU legal standards

As noted at 3.2, above, the EEGs, as always reflecting the EU Charter of Fundamental Rights and CJEU case-law, requires a system of oversight over processing of personal data for national security purposes that entails one or more "*completely independent*" and "*impartial*" supervisory authorities with *effective* supervisory and *binding* enforcement powers and that provide *real and effective* "support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms." I will look at the individual redress mechanisms below, at 4.5. Here, I should note that the words "with complete independence" in the EU data protection instruments and in the EEGs:[38]

> must be interpreted as meaning that the supervisory authorities for the protection of personal data must enjoy an independence which allows them to perform their duties free from … any external influence, direct or indirect, which is liable to have an effect on their decisions

Moreover, it is not sufficient that the relevant law stipulates that the members of the oversight body are "*independent and [not] bound by instructions of any kind in the performance of their duties*". Such a stipulation is an essential, but not a sufficient condition. Rather:[39]

> The independence required … is intended to preclude not only direct influence, in the form of instructions, but also … any indirect influence which is liable to have an effect on the supervisory authority's decisions.

As Gorski rightly sums it up, with reference to the case-law:[40]

> [The] EU's law "independence" standard … requires a judicial [oversight] body to operate "wholly autonomously" and free from any "hierarchical constraint."

ii. The EO and its predecessor

As Gorski notes:[41]

> In *Schrems II*, the CJEU … consider[ed] whether a novel mechanism for alleging unlawful surveillance, the "Privacy Shield ombudsperson," satisfied Article 47. In concluding that the ombudsperson was inadequate, the court emphasized several problems. The ombudsperson was housed within the State Department, reporting to the Secretary of State; the Secretary of State could dismiss the ombudsperson without consequence, underscoring the position's lack of independence; and there was no indication that the ombudsperson had the power to adopt binding decisions, other than the U.S. government's

---

[38] CJEU, *EDPS v. Austria* judgment of 16 October 202, ECLI:EU:C:2012:631, para. 41, with reference to its earlier judgment of 9 March 2010 in *Commission v. Germany*, ECLI:EU:C:2010:125, paras. 19, 25, 30 and 50.

[39] *Idem*, paras. 42 – 43.

[40] Ashley Gorski, The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance, 4 November 2022, available at:
https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/
The quoted words are taken from the CJEU judgment of 17 February 2018 in *Associação Sindical dos Juízes Portugueses* (ECLI:EU:C:2018:117), para. 44.

[41] *Idem*, under the heading "*From 'Privacy Shield Ombudsperson' to the New Administrative Redress Procedure*."

representation that the intelligence agencies would correct violations found by the ombudsperson. For these reasons, the court concluded that U.S. legal remedies did not satisfy the standards of EU law.

A little later, he observes that:[42]

> While the new procedure [introduced by the 7 October EO] is an improvement over the Privacy Shield ombudsperson, there appear to be several significant problems under EU law.
>
> The first problem is independence … [43]
>
> Although the Biden administration has taken several steps to try to ensure the independence of the second tier of the redress mechanism, both tiers are fundamentally administrative ones, housed within the executive branch. The fact-finding will be conducted by an ODNI office, not a court; the Data Protection Review Court judges will be selected by the Attorney General, not a third-party agency outside of the intelligence community; there's no limitation on the President's ability to remove the judges; and 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. Thus, the Data Protection Review Court does not function "wholly autonomously," nor is it free from "hierarchical constraint."
>
> Relatedly, the CJEU has emphasized[44] the importance of "protect[ing] against external interventions or pressure liable to impair the independent judgment of [judges] and to influence their decisions." Rules concerning length of service and dismissal of judges must "dispel any reasonable doubt in the minds of individuals as to the imperviousness of that body to external factors and its neutrality with respect to the interests before it." The executive order and related regulations set forth several rules that restrict the removal of the Data Protection Review Court judges. However, the judges' terms are renewable every four years, which may indirectly result in pressure to rule in the government's favor to ensure renewal.

iii. Assessment

I can only concur with Gorski:

The oversight system created by the Presidential Executive Order is neither "wholly autonomous" nor "free from hierarchical constraint"; its judges are appointed for only four years and can be removed by the US President at will; and the President can overrule its decisions (even in secret). The system does not meet the European Article 47 CFR standards of independence and impartiality.

---

42 *Idem*, under the heading "*The New Redress Procedure Likely Fails to Satisfy Article 47*".

43 I note the second, third, fourth and fifth problems identified by Gorski in the next sub-section, 4.5.

44 Link to the CJEU judgment of 24 June 2019 in *European Commission v. Poland* (ECLI:EU:C:2019:531) that in fact, in para. 72, cross-refers to para. 44 of the judgment in *Associação Sindical dos Juízes Portugueses*, referenced in footnote 40, above.

4.5 Does the EO provide for effective remedies for individuals affected by US surveillance?

i. EU legal standards

Under Article 47 of the EU Charter of Fundamental Rights (CFR), anyone whose fundamental rights are affected by a state measure must have access to an "*effective remedy*" provided by an "*independent and impartial tribunal previously established by law*" in "*a fair and public hearing*".

Although, under Article 6 of the European Convention on Human Rights with which all EU Member States must also comply in relation to EU law),[45] "*the press and public may be excluded from all or part of the trial in the interests of … national security in a democratic society*", the judgment of any court "*shall [always] be pronounced publicly.*" Under the "essential equivalence" test for third country adequacy, the same should apply in a third country if it is to be held to provide adequate protection to personal data and adequate, effective redress.

ii. US law and the EO

As Gorski notes:

> In *Schrems II*, the CJEU held that U.S. law failed to provide an avenue of redress "essentially equivalent" to that required by Article 47. The court observed that neither Executive Order 12333 nor Presidential Policy Directive-28 grants rights that are enforceable in U.S. courts, and it quoted the European Commission's assessment[46] of obstacles to U.S. judicial redress.

With regard to general remedies against undue surveillance under US law – that are essentially only available to US persons (i.e., US citizens and permanent US residents) – Gorski explains the following serious practical limitations:[47]

> In theory, an ordinary U.S. federal court under Article III of the U.S. Constitution would satisfy the standard of an "independent" and "impartial" tribunal to protect privacy rights. But once again, theory is belied by reality, because vanishingly few plaintiffs in U.S. surveillance cases ever have the merits of their claims heard by a judge or jury.
>
> Indeed, the U.S. government relies on multiple layers of secrecy to thwart virtually all civil litigation challenging foreign intelligence surveillance in U.S. courts. As a matter of U.S. government policy, people generally do not receive notice of this surveillance, even after the surveillance has ended and even where notice would not jeopardize an active investigation. When people have reason to believe that they are subject to surveillance—for example, due to press accounts—the government's assertions of secrecy make it exceedingly difficult to establish standing[48] to challenge that surveillance. Although surveillance plaintiffs may meet the plausibility threshold at the outset of a case, plaintiffs are eventually required to prove their standing with admissible evidence. Yet the executive branch routinely invokes secrecy[49] to block litigants from accessing the relevant evidence, even under a protective order or via security-cleared counsel.

---

45 See Article 52(3) of the Charter.

46 Link to the *Schrems II* judgment, referenced in footnote 2, above.

47 *em*, under the heading "*Article 47 of the Charter of Fundamental Rights and the Redress Conundrum*".

48 https://www.law.cornell.edu/wex/standing [*original link*]

49 https://www.aclu.org/legal-document/wikimedia-v-nsa-defendants-memorandum-points-and-authorities-opposition-plaintiffs [*original link*]

> The government also routinely[50] argues[51] that *courts* should not be permitted to review secret surveillance materials in civil cases, even ex parte and in camera. Moreover, in the few cases where plaintiffs manage to obtain public, admissible evidence establishing their standing, the executive branch often seeks (and courts often grant) wholesale dismissals of lawsuits based on the "state secrets" privilege. As the Wikimedia Foundation has argued in a recent cert petition[52] in a challenge to Section 702 "Upstream" surveillance, these dismissals are improper where a plaintiff may be able to make its case based on public evidence.[1] But unless and until the Supreme Court weighs in, lower courts will continue to dismiss meritorious suits on state secrets grounds.
>
> Due to this combination of policy and doctrinal hurdles, no civil lawsuit challenging the lawfulness of surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) or Executive Order 12333 has resulted in a U.S. court opinion addressing the legality of that surveillance. Nor has any litigant obtained a remedy of any kind for Section 702 or EO 12333 surveillance.

EU persons are in fact not even granted the above-mentioned (in practice, ineffective) judicial redress possibilities before a US constitutionally established court (an "Article III court"): most of the US constitutional rights do not apply to non-US persons.[53]

So what does the new Executive Order put in place? A complex system, as also neatly summarised by Gorski:[54]

> The Biden administration's new redress procedure is designed to address at least some of these shortcomings. It involves a two-layer review process.
>
> First, an individual from a "qualifying state"—the list of which is to be determined by the Attorney General [but that will presumably include the EU Member States if the European Commission is prepared to issue another positive adequacy decision – DK] —may file a complaint with an appropriate public authority in that state, who will in turn submit the complaint to a Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence (ODNI). The CLPO will then determine whether there was a "covered violation"—i.e., a violation arising from signals intelligence activities regarding data transferred to the United States from a qualifying state—that contravenes one or more of the U.S. Constitution, FISA, EO 12333, the new EO, or applicable implementing procedures.
>
> Notably, the CLPO must "giv[e] appropriate deference to any relevant determinations made by national security officials." It is unclear exactly what level of deference the CLPO will apply. Nor is it clear whether individual CLPOs will be free to take legal positions that differ from other CLPOs, or whether they will conduct an independent analysis of a critical

---

50 https://www.theguardian.com/commentisfree/2022/sep/26/us-courts-government-accountability-state-secrets [*original link*]

51 https://www.supremecourt.gov/DocketPDF/22/22-190/242125/20220929160726768_22-190%20Wikimedia%20Foundation%20v%20NSA%20Amicus%20Curiae%20Brief%20in%20Support%20of%20Petitioner.pdf [*original link*]

52 https://www.aclu.org/legal-document/wikimedia-v-nsa-petition-writ-certiorari [*original link*]

53 See Douwe Korff, The rule of law on the Internet and in the wider digital world, "*Issue Paper*" written for the Commissioner for Human Rights of the Council of Europe, 2014, section 3.2.2, *US law*, available at: https://rm.coe.int/ref/CommDH/IssuePaper(2014)1

54 Ashley Gorski, o.c. (footnote 40, above)*, under the heading "From 'Privacy Shield Ombudsperson' to the New Administrative Redress Procedure."*

question: whether some foreign targets of U.S. surveillance may, by virtue of their substantial connections to the United States, have Fourth Amendment rights. (In U.S. litigation, the executive branch has taken the position that foreign targets of Section 702 collection categorically lack Fourth Amendment rights.)

If the CLPO concludes that there was a covered violation, he or she determines the appropriate remedy and informs the Assistant Attorney General for National Security. After the review, the CLPO provides the complainant with a scripted response: "the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation."

Second, the complainant or an element of the intelligence community may seek review of the CLPO's determinations by a new administrative tribunal, the Data Protection Review Court. The judges on the court are appointed by the Attorney General and serve four-year terms. They may not be removed by the Attorney General except for malfeasance, incapacity, or similar misconduct, but notably, there is no limitation on the President's removal power. Upon an application for review, DOJ convenes a three-judge panel, and then the panel selects a security-cleared "Special Advocate." The Special Advocate is not an agent of or counsel for the complainant; its job is to assist the court's work, "including by advocating regarding the complainant's interest in the matter." If the complainant filed the application for review, the Special Advocate may transmit written questions to the complainant, but only after DOJ review of these questions.

The court's mandate is to review the determinations made by the CLPO with respect to whether a covered violation occurred and the appropriate remediation, based on the record created by the CLPO's review and any information provided by the complainant, Special Advocate, or the intelligence community. The court may also ask the CLPO to supplement the record or make additional factual findings.

If the court finds a covered violation, the executive order provides that the intelligence community "shall comply" with the court-determined remediation. After a review in response to a complainant's application (but not in response to a government application, because that could disclose that the complainant was in fact subject to surveillance), the court informs the complainant that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."

iii. Assessment

As Gorski rightly points out:[55]

> The second problem[56] is that the one-sided nature of the proceedings violates Article 47's "fair trial" principles, which require that litigants have the right to take cognizance of evidence submitted to the court; to exchange views on that evidence, so that they may seek to persuade the court; and to have procedural equality with other side.[57] Under EU law, a

---

55 Ashley Gorski, The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance (footnote 40, above), under the heading "*The New Redress Procedure Likely Fails to Satisfy Article 47*".

56 The first problem identified by Gorski concerned the oversight system, as noted in the previous sub-section.

57 Under the European Convention on Human Rights, these elements are subsumed under the rubric "equality of arms" – DK.

> government may limit these rights only insofar as is necessary and proportionate. Here, however, it is doubtful that the constraints, secrecy, and procedural unfairness of the redress process satisfy that standard—particularly because there is no case-by-case assessment of whether the limitations are necessary; the fact-finding will be conducted by an ODNI office; and vast majority of the fact-finding will take place at the first stage of the process, without even the opportunity for a Special Advocate's input.
>
> The third problem is the boilerplate nature of the ODNI and Data Protection Review Court's responses to a complainant. In an analogous context, the CJEU has held[58] that Article 47 requires that:
>
> > the person concerned must be able to ascertain the reasons upon which the [governmental] decision taken in relationship to him is based . . . so as to make it possible for him to defend his rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in his applying to the court having jurisdiction.
>
> Yet the response from the ODNI office fails to provide a complainant with any more information than the complainant had at the outset of the process, making it impossible for the complainant to bring a meaningfully informed appeal. And even if a complainant appeals, the Data Protection Review Court's response has likewise been scripted by the executive branch, which raises questions about whether it qualifies as an independent "judgment" under EU law, and whether this categorical rule can satisfy the proportionality test under EU law. At a minimum, one would expect that where a surveillance violation has been found and redressed, that fact would be disclosed to the complainant. Similarly, where the challenged surveillance is no longer taking place, and where disclosure would not jeopardize an ongoing investigation, these scripted responses are at odds with the fact-specific proportionality analysis that EU law requires.

In my opinion, 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 in the (in any case, as Gorksi notes, seriously deficient and unfair) process. That "judgment" is kept secret, in direct violation of Article 6 ECHR and therefore also of the EU Charter of Fundamental Rights.

Gorski continues:

> Fourth, U.S. government data purchases are excluded from the definition of "covered violation." When a U.S. government agency collects Europeans' private data in bulk, but does so by paying for it, rather than using electronic surveillance, that collection is simply beyond the scope of the new executive order. Given intelligence and defense agencies' extensive practice of buying data in bulk,[59] this is cause for concern.
>
> Finally [fifth], the lack of notice to people subject to U.S. foreign intelligence surveillance remains an issue. In the *Schrems II* litigation, the Advocate General's opinion critiqued the U.S.'s failure to provide notice to individuals even after the surveillance had concluded, and

---

[58] Link to the CJEU judgment of 18 July 2013 in *European Commission and United Kingdom v. Bulgaria, Italy, Luxembourg and Hungary* (ECLI:EU:C:2013:518). The quote is from para. 100.

[59] As noted also in Ian Brown and Douwe Korff, The inadequacy of UK data protection law in general and in view of UK surveillance laws, *Part Two on UK surveillance law* (footnote 32, above).

after the point at which notice would no longer jeopardize an investigation. He observed that notification concerning access to data is a "prerequisite to the exercise of the right to a remedy under Article 47 of the Charter." As the CJEU had previously explained:[60]

> "That notification is, indeed, necessary to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves . . . of an effective remedy before a tribunal[.]"

Without notice of U.S. government surveillance, Europeans would rarely have a reason to file a complaint or an appeal in pursuit of a remedy.

Once again, I can only concur with Gorski:

The redress system for individuals who may be affected by US surveillance is not "effective" or "fair" in terms of the EU Charter of Fundamental Rights. It is essentially secret, grants the individuals nothing that approaches "equality of arms", and the "judgment" (the outcome of the process) is not made public or available to the complainant (the "boilerplate" prescribed responses cannot be regarded as the judgment). Individuals who have been under surveillance but not found to be implicated in any of the threats covered by the EU are never informed of this, not even if this informing would not jeopardise an ongoing investigation. And the redress system does not cover at all US surveillance by means of data bought by the USA from private companies (or accessed by the US agencies under arrangements with such companies).

In sum: the redress system, too, does not meet the European Article 47 CFR standards on fair and effective redress.

5. Summary and Conclusions

As the above analyses show, the new Executive Order does not really fundamentally change the fact that the US authorities insist on carrying out indiscriminate, untargeted mass surveillance, also of EU persons and EU governmental and non-governmental entities, by means of bulk collection of data, without independent substantive judicial oversight or effective redress.

Specifically, the analyses show:*

* NB: The numbering below corresponds to the numbering of the sub-sections in section 4.

1. The Presidential Executive Order is not clear or precise or foreseeable in its application, and can be secretly amended by the president. It does not have the "quality of law" required under European human rights standards.

2. 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. From the EU legal perspective, this is a lethal defect in the new regime that is fundamentally incompatible with the EU Charter of Fundamental Rights.

60 Link to the CJEU judgment in *LQDN* (footnote 7, above). The quote is from para. 190.

3. "Bulk collection" as practiced by the USA (in close cooperation with the UK and the other "Five Eyes" countries, Australia, Canada and New Zealand), is by definition indiscriminate; it is not limited to data that has some link, even indirectly, to any serious threat or known person. It refers to what the Court of Justice of the EU calls the collection of data "on a generalised basis". Only after (bulk) collection is there an attempt to filter out data that are not relevant, necessary or proportionate to the relevant objective.

   Moreover, the Presidential Executive Order does not limit signal intelligence generally, and indiscriminate bulk collection of personal data inclusing e-communications content and metadata in particular, to what is considered "necessary", "proportionate" and "legitimate" in relation to national security under EU law.

   In particular:

   - the EO 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.

4. The oversight system created by the Presidential Executive Order is neither "wholly autonomous" nor "free from hierarchical constraint"; its judges are appointed for only four years and can be removed by the US President at will; and the President can overrule its decisions (even in secret). The system does not meet the European Article 47 CFR standards of independence and impartiality.

5. The redress system for individuals who may be affected by US surveillance is not "effective" or "fair" in terms of the EU Charter of Fundamental Rights. It is essentially secret, grants the individuals nothing that approaches "equality of arms", and the "judgment" (the outcome of the process) is not made public or available to the complainant (the "boilerplate" prescribed responses cannot be regarded as the judgment). Individuals who have been under surveillance but not found to be implicated in any of the threats covered by the EO are never informed of this, not even if this informing would not jeopardise an ongoing investigation. And the redress system does not cover at all US surveillance by means of data bought by the USA from private companies (or accessed by the US agencies under arrangements with such companies). In sum: the redress system, too, does not meet the European Article 47 CFR standards on fair and effective redress.

Overall conclusion:

In my opinion, given the above many clear and serious defects, it should be inconceivable that the European Commission would issue yet another positive adequacy decision on the USA, based on yet another inadequate system of regulation of and oversight over US signal intelligence and bulk data collection. However, history shows that the Commission tends to try and issue such decisions in spite of such defects, presumably for trading and political reasons. Yet yet another judicial debacle – "*Schrems III*" – should surely be avoided.

Hopefully, the European Parliament and civil society will forcefully speak out against any attempt to endorse with yet another fundamentally flawed and inadequate arrangement.

One final thought ("ceterum censeo …"):

As Goitein and Gorski also rightly argue, what is needed in the USA is fundamental reform of surveillance laws and practices, to provide full and proper protection against undue surveillance to US and non-US persons alike.

But I should also recall what Ian Brown and I already argued in our 2021 study for the European Parliament, i.e., that:[61]

> [t]he EU institutions and in particular the European Parliament should stand up for the rule of law and demand that both the Member States and third countries bring their intelligence practices and domestic law frameworks fully in line with international human rights law.

Until the surveillance laws and practices of the EU member States – and the UK! – are also brought in line with fundamental European human rights principles – which they curfrently manifestly are not in many member states and the UK – it will always be politically difficult for Europeans to argue against the inadequacies of US law in this respect. The fact that all Western European countries are party to the European Convention on Human Rights is not sufficient in this regard: it takes years to challenge wrongful practices and the Convention enforcement system remains weak. Even in countries in which the Convention can be directly invoked and applied by the domestic courts, it remains extremely difficult to change the engrained human rights-unfriendly attitudes and approaches of the intelligence agencies.

- o – O – o -

Douwe Korff (Prof.)
Cambridge (UK), November 2022

[61] Ian Brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment (footnote 6, above), section 4.4.2, *Recommendations*, recommendation no. 3. See also the text at the end of section 2.3.1.3, *Requirements relating to access to personal data by state authorities*, under the heading "*Hypocrisy and "Double standards"? US criticism of the EU and the EU Member States*".