5-2023

Necessity, Proportionality, and Executive Order 14086

Alex Joel

AMERICAN UNIVERSITY
WASHINGTON
COLLEGE of LAW

TECH, LAW & SECURITY
PROGRAM

Necessity, Proportionality, and Executive Order 14086

May 2023

Alex Joel

Privacy Across Borders

Tech, Law & Security Program (TLS)

TLS is a rapidly expanding initiative at the American University Washington College of Law that tackles the challenges and opportunities posed by emerging technologies — offering innovative solutions, engaging our students, and training the leaders of tomorrow.

Privacy Across Borders (PAB)

Privacy Across Borders is a TLS project that brings together global experts and practitioners from the government, private sector, and civil society to develop practical, actionable recommendations for challenges to cross-border data flows.

Necessity, Proportionality, and Executive Order 14086
By Alex Joel

Contents

Executive Summary

In this paper, I examine how EO 14086 addresses the requirements articulated in *Schrems II* regarding necessity and proportionality; I also respond to specific questions about the EO in the EDPB's recent opinion. The terms "necessary" and "proportionate" have specialized meanings under the jurisprudence of the Court of Justice of the European Union and the European Court of Human Rights. The paper examines in depth how the EO articulates and explains those terms, interpreting them in light of U.S. law and legal traditions.

This paper reviews the EO's articulation of "legitimate objectives" for signals intelligence and compares it with the more general definitions of "national security" that are the norm in Europe. The President's ability to add to the list of legitimate objectives—to account for the emergence of unanticipated threats—echoes case law in Europe that the term "national security" is not "capable of exhaustive definition."

The paper then focuses on questions raised in the EDPB opinion about targeted collection under Section 702 of the Foreign Intelligence Surveillance Act, and bulk collection under the EO. The information that the U.S. government has released, including surveillance statistics, oversight reports, and rulings from the Foreign Intelligence Surveillance Court, show that Section 702 surveillance is not "massive and indiscriminate," and that the Court is closely involved in overseeing targeting decisions. In particular, the Court examines compliance with the requirement that "the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information" of the type authorized by the Court.

Turning to bulk collection, the paper explains that such collection is permissible under European jurisprudence if conducted in accordance with specific safeguards. It points out that bulk collection is prohibited by U.S. law for data after it has been transferred to the U.S. With respect to concerns about interception of data in the course of transmission to the U.S., the paper examines the EO's bulk collection safeguards and responds to specific concerns raised in the EDPB opinion. It highlights the oversight role played not only by the Privacy and Civil Liberties Oversight Board, but also by Congress, which given its status as a separate, co-equal, and independent branch of government, plays a different role than parliamentary oversight plays in other legal systems.

The paper concludes that there is ample ground for finding that the EO's necessity and proportionality safeguards are essentially equivalent to EU legal standards.

Introduction

In the *Schrems II* case,[1] the Court of Justice of the European Union (CJEU) invalidated the European Commission's adequacy finding for Privacy Shield[2] relating to three national security legal instruments: Section 702 of the Foreign Intelligence Surveillance Act,[3] Executive Order (EO) 12333,[4] and Presidential Policy Directive-28 (PPD-28).[5] The CJEU found that the U.S. national security legal framework did not provide safeguards that were "essentially equivalent" to those under European Union (EU) law in the areas of redress and proportionality.[6] To address those concerns, the European Commission and the U.S. government announced the EU-U.S. Data Privacy Framework.[7] As part of that framework, President Biden issued EO 14086,[8] and the Attorney General published regulations establishing a new Data Protection Review Court.[9]

In its draft adequacy decision published in December 2022,[10] the European Commission (EC) found that with these changes, the U.S. national security legal framework now meets EU standards. The European Data Protection Board (EDPB) issued its advisory opinion in February 2023 (EDPB opinion). The EDPB opinion points out that "[i]t is important to recognise that the EDPB does not expect the US data protection framework to replicate European data protection law. However, the EDPB recalls that, to be considered as providing an adequate level of protection, [EU law] require[s] the third country's legislation to provide data subjects with a level of protection essentially equivalent to that guaranteed in the EU".[11] It then notes that the

[1] Case C-311/18, *Data Prot. Comm'r, v. Facebook Ireland Ltd* (*Schrems II*), ECLI:EU:C: 2020:559, (July 16, 2020).
[2] Commission Implementing Decision 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 48 (EU) (Privacy Shield adequacy decision).
[3] 50 U.S.C. Section 1881a
[4] Exec. Order No. 12,333, 46 Fed. Reg. 59441 (1981), posted as amended by Executive Orders 12384 (2003), 13355 (2004) and 13470 (2008).
[5] Presidential Policy Directive-28, Signals Intelligence Activities (2014). Note that PPD-28 has been largely superseded by Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities (2022).
[6] *Schrems II*, *supra* note 1, at para. 185, 197. It is common to refer to this area as relating to "necessity and proportionality." As further discussed below, these are closely interrelated terms. In the *Schrems II* decision, the Court specifically refers to the "principle of proportionality." *See* paras. 174, 178, 180, and 184.
[7] Press Release, United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework, March 25, 2022.
[8] Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities (2022).
[9] 28 C.F.R. Part 201 (2022).
[10] European Commission, Commission implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, December 13, 2022 (draft).
[11] EDPB opinion, at 2.

changes wrought by EO 14086 are a "significant improvement."[12] However, it also "identified in its assessment a number of points for additional clarifications, for attention or for concern."[13]

This paper examines the necessity and proportionality aspects of EO 14086.[14] It also answers certain questions the EDPB posed in its opinion. It concludes that the U.S. national security legal framework, as amended by EO 14086, provides ample grounds for a finding of essential equivalence with the necessity and proportionality standard under EU law.

Legal Interpretations

Before diving into the EO's use of the terms "necessary" and "proportionate," it is helpful to consider the question of interpretation. These terms have special significance under European Union (EU) law as well as under the European Convention of Human Rights (ECHR). Under EU law, these terms appear in Article 52(1) of the Charter of Fundamental Rights of the European Union (EU Charter):[15]

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. *Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest* recognised by the Union or the need to protect the rights and freedoms of others.[16]

These terms also appear in the legal regime established by the European Convention on Human Rights (ECHR),[17] as interpreted by the European Court of Human Rights (ECtHR). The ECtHR's rulings on this topic are directly relevant to the CJEU's legal analysis because of Article 52(3) of the Charter:

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms [ECHR], the meaning and scope of those rights shall be the same as those laid down by the said

[12] European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, Opinion of the Board (Art. 70.1.s), February 28, 2023, at 4 (EDPB Opinion).
[13] EDPB Opinion, at 5.
[14] The Privacy Across Borders team examines redress in depth in other papers and articles, which are posted on the Privacy Across Borders website. *See, generally* Privacy Across Borders (last visited May 6, 2023) (featuring articles, papers and resources on topics such as the EU-U.S. Data Privacy Framework, global data flows, privacy, and government access to data for national security and law enforcement purposes).
[15] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391 (2000).
[16] Id. (emphasis added).
[17] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950.

> Convention. This provision shall not prevent Union law providing more extensive protection.

In its opinion, the EDPB cites Article 52(3) and states: "Therefore, in the following assessment, the EDPB has taken into account the jurisprudence of the ECtHR, to the extent that the EU Charter, as interpreted by the CJEU, does not provide for a higher level of protection which prescribes other requirements than the ECtHR case-law."[18]

Article 8 of the ECHR establishes the "right to respect for privacy and family life," and provides that "[t]here shall be no interference by a public authority with the exercises of this right except such as is in accordance with law and is necessary in a democratic society in the interests of national security."[19] The ECtHR has ruled that the term "necessary" encompasses the concept of proportionality: "[a] restriction on a Convention Right cannot be regarded as 'necessary in a democratic society' … unless … it is proportionate to the legitimate aim pursued."[20] For decades, the ECtHR has been fleshing out the meaning of necessity and proportionality in cases challenging the surveillance laws and practices of ECHR parties.[21]

The challenge for those seeking to apply these specialized legal terms to U.S. surveillance activities is that the U.S. is not a member state of the EU; nor is it a party to the ECHR. The U.S. national security legal framework has its roots in the U.S. Constitution, and its statutory and case law developed over centuries,[22] independently of EU law and ECtHR jurisprudence. Because the terms "necessary" and "proportionate" have their own range of legal meanings under U.S. law, the drafters of the EO took care to incorporate the principles underlying those terms in a manner that translates these European principles into the U.S. legal framework. It is in that context that the Department of Justice regulation setting up the new Data Protection Review Court (DPRC) reminds the DPRC's judges to nonetheless "interpret [the

---

[18] EDPB Opinion, para. 102.

[19] Article 8 reads in full as follows:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[20] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, August 31, 2020, para. 26.

[21] For an official summary of ECtHR's national security cases, *see* European Court of Human Rights, Press Unit, Mass Surveillance, September 2022.

[22] U.S. national security law is a rich and complex topic that is itself the subject of semester-long courses in U.S. law schools, with many treatises and case books written either as "surveys" covering a range of issues, or as in-depth analyses of particular issues. *See, e.g.,* Stephen Dycus, et al, National Security Law (7th ed.) (2020); David S. Kris, J. Douglas Wilson, National Security Investigations and Prosecutions (3d ed.) (2019-2023). My course is but one example of many in U.S. law schools on national security law topics: American University Washington College of Law, National Security Surveillance and Secrecy, last delivered Fall 2022.

EO] exclusively according to United States law and legal traditions."[23] Consistent with this direction, this paper interprets relevant provisions of EO 14086 "according to United States law and legal traditions." Notwithstanding the independent development of the U.S. legal framework from EU and ECtHR law, the following analysis finds substantial overlap on the principles of necessity and proportionality.

EU Charter: "Objectives of General Interest Recognised by the Union"

As noted earlier, Article 52(1) of the Charter provides that *"*[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." How does the EO's approach compare to the Charter's concept of "objectives of general interest"?

Legitimate Objectives under EO 14086

Among the notable changes reflected in EO 14086 is the articulation of 12 "legitimate objectives."[24] The wording of each objective is important—each entails understanding, assessing, or protecting against *threats*. Indeed, the word "threat" directly appears in six of the objectives:

- terrorist threats;[25]
- transnational threats that impact global security;[26]
- threats posed by weapons of mass destruction; [27]
- cybersecurity threats;[28]
- threats to personnel of the U.S. or its allies or partners;[29]
- and transnational criminal threats.[30]

In addition, the concept of "threat" is necessarily implicit in the remaining objectives:

[23] 28 CFR Part 210, at Section 201.10.
[24] EO 14086, section 2(b)(i).
[25] Section 2(b)(ii)(2).
[26] Section 2(b)(ii)(3).
[27] Section 2(b)(ii)(7).
[28] Section 2(b)(ii)(8).
[29] Section 2(b)(ii)(9).
[30] Section 2(b)(ii)(10).

- assessing the capabilities and intentions of a foreign government or military "in order to protect the national security of the United States and of its allies and partners";[31]
- protecting against foreign military activities;[32]
- protecting against terrorism and hostage taking;[33]
- protecting against espionage, sabotage, or assassination;[34]
- protecting the integrity of elections and infrastructure;[35] and
- advancing capabilities in order to do the above.[36]

Significantly, the EO bookends these legitimate objectives with prohibited ones. It provides:

> Signals intelligence collection activities shall not be conducted for the purpose of: 1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press; 2) suppressing or restricting legitimate privacy interests; 3) suppressing or restricting a right to legal counsel; or 4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.[37]

In addition, the EO clarifies that "[i]t is 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."[38]

For bulk collection, intelligence agencies may only use signals intelligence information collected in bulk for six objectives rather than 12. To paraphrase, these are protecting against terrorism and hostage taking; protecting against espionage, sabotage, and assassination; protecting against threats involving weapons of mass destruction; protecting against cybersecurity threats; protecting against threats to personnel of the U.S. or of its allies and partners; and protecting against transnational criminal threats including sanctions evasion.[39]

[31] Section 2(b)(ii)(1).
[32] Section 2(b)(ii)(4).
[33] Section 2(b)(ii)(5).
[34] Section 2(b)(ii)(6).
[35] Section 2(b)(ii)(11).
[36] Section 2(b)(ii)(12).
[37] Section 2(b)(ii)(A).
[38] Section 2(b)(ii)(B).
[39] Section 2(c)(ii)(B).

EO 14086: "The President may authorize updates to the list of objectives."

After listing the objectives, the EO provides that "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."[40] The EDPB notes the President's ability to add to the list without analyzing what it means for its necessity and proportionality analysis. For example, in discussing safeguards for signals intelligence, the EDPB states:

> In the context of collection of signals intelligence, the EO provides for a list of 12 objectives for which data can be collected, which have to be further substantiated into intelligence priorities (see paragraph 117), as well as a list of 5 objectives for which signals intelligence collection activities shall not be conducted. In principle these provisions constitute a guarantee to ensure the necessity of the collection of data. *Yet, the EDPB recalls that EO 14086, also provides for the possibility for the President of the United States to add other objectives to the list.*[41]

Although EO 14086 indeed provides for the possibility that the President could add objectives, this ability is not unbounded. First, any new objective must respond to "new national security imperatives." The word "imperative" as used here connotes something that is mandatory or urgent in terms of protecting national security. In addition, any new objective must focus on "national security." In keeping with U.S. legal traditions, one could turn to canons of statutory construction to determine the meaning of "national security," including referring to the list of 12 objectives as a guidepost.[42] Moreover, any additional objective must be made public unless disclosure would harm national security. Importantly, the prohibitions on objectives continue to apply; any new objective cannot run afoul of those prohibitions.

But why is such a provision even necessary? In this rapidly changing world, with new technology and new threats developing at an increasingly rapid pace, this provision is a recognition that a new threat might arise that is not covered by one of the specified objectives. Locking in a list of detailed objectives raises the dangerous possibility that some unanticipated threat may manifest due to changed conditions.

"National Security" in Europe

The EO's specification of "legitimate objectives" for national security surveillance, coupled with a formal process for adding to the list, goes beyond what is required in Europe,

---

[40] EO 14086, at Sections 2(b)(i)(B) and 2(c)(ii)(C).
[41] EDPB Opinion, at paras. 130-131 (emphasis added).
[42] *See, e.g.,* Congressional Research Service, Statutory Interpretation: General Principles and Recent Trends, September 24, 2014.

either by the ECtHR or the CJEU. The ECtHR has opined that the term "national security," standing alone, without further definition or delineation, is sufficient under the ECHR. In *Kennedy v. The United Kingdom*, the ECtHR noted that "the condition of foreseeability does not require States to set out exhaustively by name the specific offenses which may give rise to interception."[43] The Court pointed out:

> The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance.[44]

Similarly, in *Esbester v. United Kingdom*, the European Commission of Human Rights, found that the human rights principles governing surveillance "do not necessarily require a comprehensive definition of the notion of 'the interests of national security'" and "*the term 'national security' is not amenable to exhaustive definition*."[45] More recently, in the *Case of Centrum för Rättvisa v. Sweden* (the "Sweden case"), the ECtHR pointed out that under Swedish law, "[f]oreign intelligence is, according to the Foreign Intelligence Act . . . conducted in support of Swedish foreign, defence and security policy, and in order to identify external threats to the country."[46] In ruling on Sweden's bulk collection legal regime, the ECtHR noted:

> [A]ccording to the Signals Intelligence Act signals intelligence may be conducted only to monitor:
> 1. external military threats to the country;

---

[43] *Kennedy v. The United Kingdom,* App. No. 26839/05 (2010), at para. 159.

[44] *Id*. Note that Article 8(2) of the Convention states:

> There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Convention does not itself further define "national security."

[45] Esbester v. United Kingdom, App. No. 18601/91, Eur. Ct. H.R. (1993), at p. 10 of PDF version (emphasis added). Note that the European Commission of Human Rights was the body hearing individual applications under the European Convention of Human Rights until 1998,

[46] *Case of Centrum för Rättvisa v. Sweden,* App. No. 35252/08, (2021), at para. 15.

2. conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations;
3. strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national interests;
4. the development and proliferation of weapons of mass destruction, military equipment and other similar specified products;
5. serious external threats to society's infrastructure;
6. foreign conflicts with consequences for international security;
7. foreign intelligence operations against Swedish interests; and
8. the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy.[47]

Although the Court took issue with the extent to which Swedish law established the necessary "end-to-end" safeguards, it did not object to the way in which Sweden delineated the national security purposes. Also in the Sweden case the ECtHR observed:

> While technological capabilities have greatly increased the volume of communications traversing the global Internet, the threats being faced by Contracting States and their citizens have also proliferated. These include, but are not limited to, *global terrorism, drug trafficking, human trafficking and the sexual exploitation of children*. Many of these threats come *from international networks of hostile actors* with access to increasingly sophisticated technology enabling them to communicate undetected. Access to such technology also permits *hostile State and non-State actors to disrupt digital infrastructure and even the proper functioning of democratic processes* through the use of cyberattacks, a serious threat to national security which by definition exists only in the digital domain and as such can only be detected and investigated there.[48]

Note that in the above passage, the ECtHR begins its list of threats with the phrase "[t]hese include, but are not limited to," thus leaving the list open-ended.

When seeking to understand what is encompassed by the term "national security" under EU law, it is helpful to look first at the EU's founding treaties. Article 4(2) of the Treaty on European Union (TEU)[49] carves out "national security" from the EU's remit. It provides:

---

[47] The Sweden case, at para. 284.
[48] The Sweden case at para. 237 (emphasis added). Various European governments intervened to submit supporting arguments for the Swedish government's position. The Netherlands was one such government and submitted that "bulk interception was necessary to identify *hitherto unknown threats to national security*. In order to protect national security, intelligence services needed the tools to investigate *emerging threats* in a timely and effective manner."
[49] Consolidated Version of Treaty on European Union (C 326) (2012).

> The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

In *La Quadrature du Net and Others* (LQDN) the CJEU examined the scope of the national security exception.[50] In pointing out certain limits to the exception, it observed that "it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security."[51] It went on to state:

> [I]t should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. 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*.[52]

The CJEU then noted that "[t]he importance of the objective of safeguarding national security … goes beyond that of … combating crime in general," and observed that "[t]hreats such as those referred to [in the quoted text above] can be distinguished, by their nature and particular seriousness…."[53]

These passages convey the CJEU's understanding that the term "national security" involves protecting against activities "directly threatening society, the population or the State itself" and includes "terrorist activities"; and that national security is different by its "nature" and "particular seriousness" from "combating crime in general." Although these general characterizations do not provide detailed guidance, they seemingly encompass the EO's specific delineation of legitimate objectives.

Given the recognition that national security is necessarily a broad term that is "not capable of exhaustive definition," the process set forth in EO 14086 appears to be a reasonable

[50] Joined Cases C-511, 512 and 520/18, *La Quadrature du Net and Others*, ECLI:EU:C:2020:791 (Oct. 6, 2020).
[51] LQDN, para. 99.
[52] LQDN, para. 135 (emphasis added).
[53] LQDN, para. 136.

attempt to set specific legal boundaries in a manner that does not create undue risks in light of unanticipated new threats.

Necessary and Proportionate under EO 14086

The principles of "necessity" and "proportionality" are closely related under EU law as well as under the ECHR. Article 51 of the EU Charter provides: "*Subject to the principle of proportionality,* limitations may be made only *if they are necessary* and genuinely meet objectives of general interest recognised by the Union…."[54] The ECtHR has ruled that the term "necessary" encompasses the concept of proportionality: "[a] restriction on a Convention Right cannot be regarded as 'necessary in a democratic society' … unless … it is proportionate to the legitimate aim pursued."[55] The EO seeks to tease apart these concepts and articulate them in a way that fits within U.S. legal traditions.

EO 14086: "Necessary to Advance a Validated Intelligence Priority"

The EO provides that, before conducting a signals intelligence activity, there must be a "determination that [the activity] is *necessary* to advance a validated intelligence priority."[56] To facilitate oversight and redress, this determination must be documented (to the extent reasonable), including its factual basis.[57] The EO defines a "validated intelligence priority" as "a priority validated under the process described in section 2(b)(iii) of this order."

Section 2(b)(iii) in turn leverages existing legal requirements for how intelligence priorities are determined and transmitted to the agencies to direct their collection activities. Section 2(b)(iii) refers to the DNI's authority under Section 102A of the National Security Act of 1947.[58] Specifically, the National Security Act provides that the "Director of National Intelligence shall establish … priorities … for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination . . . of national intelligence."[59] In addition, the DNI is to "determine requirements and priorities for, and manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community."[60] The DNI exercises this responsibility through the

[54] EU Charter at Article 51 (emphasis added).
[55] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, August 31, 2020, para. 26.
[56] EO 14086, at Section 2(c)(i) (emphasis added).
[57] EO 14086, at Section 2(c)(iii)(E).
[58] Codified at 50 U.S.C. Section 3001 et seq.
[59] National Security Act, at Section 102A(f)(1)(A) (codified at 50 U.S.C. Section 3024(f)(1)(A)).
[60] National Security Act, at Section 102A(f)(1)(B) (codified at 50 U.S.C. Section 3024(f)(1)(B)).

National Intelligence Priorities Framework (NIPF), which is laid out in Intelligence Community Directive 204.[61]

EO 14086 makes a crucial—and groundbreaking—change to this key national security process: it interposes the Civil Liberties Protection Officer. The EO provides:

> In order to ensure that signals intelligence collection activities are undertaken to advance legitimate objectives, before presenting the NIPF or any successor framework that identifies intelligence priorities to the President, the Director shall obtain from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) an assessment as to whether, with regard to anticipated signals intelligence collection activities, each of the intelligence priorities identified in the NIPF or successor framework: 1) advances one or more of the legitimate objectives set forth in subsection (b)(i) of this section; 2) neither was designed nor is anticipated to result in signals intelligence collection in contravention of the prohibited objectives set forth in subsection (b)(ii) of this section; and 3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.[62]

Only after the intelligence priority has been validated in this way, with the unprecedented involvement of the CLPO, can it be deemed a "validated intelligence priority."

What does "necessary" mean when used in these provisions? According to Black's Law Dictionary, something is "necessary" if it is "needed for some purpose or reason; essential." The EO clarifies, however, that the signals intelligence activity "does not have to be the sole means available." Rather, a determination to use signals intelligence must be arrived at after considering "the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence."[63] In other words, the activity can be conducted if there are no "available, feasible, and appropriate" alternatives.

EO 14086: "Proportionate to the Validated Intelligence Priority"

The EO captures the principle of "proportionality" by providing that "signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the

[61] Office of the Director of National Intelligence, Intelligence Community Directive 204, Roles and Responsibilities for the National Intelligence Priorities Framework (September 13, 2007).
[62] EO 14086, at Section 2(b)(iii).
[63] EO 14086, Section 2(c)(i).

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."[64]

The term "proportionality" does not itself appear in U.S. surveillance law but has legal significance in other areas of U.S. law. According to a U.S. constitutional law scholar, "some areas of U.S. constitutional law embrace proportionality as a principle . . . or contain other elements of 'structured proportionality review' widely used in foreign constitutional jurisprudence, including the inquiry into 'narrow tailoring' or 'less restrictive alternatives' found in U.S. strict scrutiny."[65] The term "strict scrutiny" is a familiar one to U.S. lawyers, and refers to the test certain types of government action must pass; in general, if an action involves "fundamental rights," the government must show that the action (or legislation) is "necessary" or "narrowly tailored" to promote a compelling government interest.[66] According to another U.S. constitutional law scholar, "in its insistence that any infringement of fundamental rights must be necessary or narrowly tailored to compelling governmental interests, the strict scrutiny formula possesses important commonalities with (though possibly also some important differences from) the similarly generic 'proportionality' tests applied in Germany, Canada, and Israel and by the European Court of Justice."[67]

In addition, the concept of proportionality is frequently used in discussions of how much force police officers can use in response to a threat. As one law review article put it using a formulation that should be familiar to EU lawyers, "the proportionality requirement is logically linked to the concept of necessity. Whereas necessity requires that the least coercive means to achieve a given legitimate end be used, proportionality tests whether those means are worth it--whether the end is important enough to justify the cost of achieving it."[68]

---

[64] EO 14086, Section 2(a)(ii)(B).

[65] Vicki C. Jackson, Constitutional Law in an Age of Proportionality, 124 Yale L.J. 3094, 3096 (2015). The article lists examples, including: Eighth Amendment cases determining whether punishments are "grossly disproportionate" to the severity of the offense; Due Process Clause cases on whether punitive damages in civil cases are "reasonable and proportionate" to the harm caused to the plaintiff and the general damages recovered; and Takings Clause cases on whether conditions for zoning permits have "rough proportionality" to the effects of the proposed use of the property. *Id.* at 3014-3015.

[66] *See* Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. Rev. 1267, 1268 (2007). This article discusses a range of examples, including challenges under the Equal Protection Clause, the First Amendment, and the Due Process Clause. *Id*.

[67] *Id.* At 1295 (pointing out that U.S. strict scrutiny may be in certain cases "more rigorous" than from how foreign legal frameworks define proportionality). That said, it is important to note that while concepts such as "strict scrutiny" can be helpful in understanding how the U.S. legal framework and traditions might view the principle of "proportionality" as articulated in EO 14086, the test itself only applies to judicial review of certain types of government actions under specific circumstances. I do not mean to suggest that a court would literally apply the strict scrutiny legal standard when reviewing an EO 14086 issue.

[68] Harmon, Rachel, *When is Police Violence Justified?* (July 9, 2008). Northwestern University Law Review, Vol. 102, No. 3, 2008, at 60.

This notion of determining "whether the end is important enough to justify the cost of achieving it" is apparent in EO 14086's above-quoted proportionality formulation, which requires that signals intelligence activities must seek to "achiev[e] *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."[69] "Achieving a proper balance" is a familiar concept in the U.S. legal framework. As pointed out by former ODNI General Counsel Robert Litt in correspondence to the European Commission that formed part of the Privacy Shield adequacy decision, "[a]s for the concept of 'reasonableness,' it is a bedrock principle of U.S. law. It signifies that Intelligence Community elements will not be required to adopt any measure theoretically possible, but rather will have *to balance their efforts* to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities."[70]

The EO provides additional guidance on proportionality, stating that "[s]ignals 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."[71] Given the extensive U.S. constitutional law jurisprudence on "tailoring" alluded to earlier in this section, this term is a familiar one to U.S. lawyers but may be less familiar to Europeans.

Merriam-Webster's online dictionary defines the verb "tailor" as "to make or fashion as the work of a tailor" and "to make or adapt to suit a special need or purpose." The Department of Justice uses the term when referring to case law regarding the scope of government searches of its own workplaces: "A search will be 'permissible in its scope' when 'the measures adopted are reasonably related to the objectives of the search and [are] *not excessively intrusive* in light of the nature of the misconduct.' This standard requires employers and their agents *to tailor work-related searches to the alleged misfeasance*."[72]

Black's Law Dictionary, referring to First Amendment jurisprudence, defines the term "narrowly tailored" as "being only as broad as is reasonably necessary to promote a substantial governmental interest that would be achieved less effectively without the restriction." The

---

[69] EO 14086, Section 2(a)(ii)(B) (emphasis added).

[70] Privacy Shield adequacy decision, at Annex VI (emphasis added). As the Supreme Court held in a landmark Fourth Amendment case, "[i]n order to assess the reasonableness of [the police officer's] conduct as a general proposition, it is necessary 'first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen,' for there is 'no ready test for determining reasonableness other than by *balancing* the need to search (or seize) against the invasion which the search (or seizure) entails." *Terry v. Ohio*, 392 U.S. 1, 21 (1968) (citations omitted) (emphasis added).

[71] EO 14086, at Section 2(c)(i)(B) (emphasis added).

[72] Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, at 55 (emphasis added) (citation omitted).

Supreme Court's use of the term "narrowly tailored" is summarized by a constitutional law scholar:

> The Supreme Court … frequently presents the strict scrutiny inquiry as if it possessed two discrete parts. First, has the government defended a challenged regulation by referring to the need to protect a genuinely compelling interest? Second, if so, is the challenged regulation *narrowly tailored* to that interest in the sense of being neither under- nor overinclusive?
> ….
> The Court must determine whether infringements of constitutional rights, which can be more or less grievous, can be justified in view of the benefits likely to be achieved, the scope of infringement of protected freedoms, and the available alternatives.

Returning to EO 14086, after calling on signals intelligence activities to be "as tailored as feasible," it goes on to list some of the factors to be taken into account:

> 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.[73]

This specific articulation of factors fits within the U.S. legal tradition on reasonableness, balancing, and tailoring, which aim to constrain government intrusions on individual rights and freedoms.

Comparison with Europe

How does the above compare with proportionality under EU law? In an earlier issuance the EDPB stated:

> Regarding the principle of proportionality, the Court [in *Schrems II*] held, in relation to Member State laws, that the question as to whether a limitation on the rights to privacy and to data protection may be justified must be assessed, on the one hand, by measuring the seriousness of the interference entailed by such a limitation and by

[73] EO 14086, at Section 2(c)(i)(B).

> verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness, on the other hand.[74]

Another EU legal instrument is also instructive here. Directive 2016/680—commonly referred to as the Law Enforcement Directive—discusses the concepts of necessity and proportionality in the law enforcement arena:

> Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done [for law enforcement purposes] as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. . . . The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected *are not excessive* and not kept longer than is necessary for the purpose for which they are processed.[75]

In the main operative clause on this point, Article 4 of the Law Enforcement Directive states: "Member States shall provide for personal data to be . . . adequate, relevant and not excessive in relation to the purposes for which they are processed."

> The ECtHR, in its landmark surveillance case *Klass and Others v. Germany*, stated:
>
> As the Preamble to the Convention states, 'Fundamental Freedoms ... are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which (the Contracting States) depend. In the context of Article 8 (art. 8), this means that a *balance must be sought between the exercise by the individual of the right guaranteed to him under paragraph 1 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) to impose secret surveillance for the protection of the democratic society as a whole*.[76]

---

[74] European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, November 10, 2020, para. 33.

[75] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Recital 26 (emphasis added).

[76] *Klass and Others v. Germany*, App. No. 5029/71, para. 58 (Sept. 6, 1978). In examining Germany's surveillance laws and practices, the ECtHR proclaimed that "[t]he Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse." *Id.* at para. 50.

Not surprisingly given how much care the U.S. and European Commission teams took in developing relevant text, the proportionality formulation in EO 14086, when understood in context of "U.S. law and legal traditions," tracks closely with the manner in which the CJEU refers to proportionality.

Targeted Collection under FISA Section 702

The provisions discussed above apply to all types of signals intelligence activity, whether it is "targeted" or "bulk collection." This section of the paper analyzes targeted collection under Section 702 of FISA; later, it will review bulk collection. This paper will not repeat here the many detailed descriptions that exist about FISA Section 702,[77] including those set forth in the draft adequacy decision and the EDPB's opinion. Instead, this section will focus on the EDPB's questions and concerns about Section 702.

EDPB opinion: "To exclude that massive and indiscriminate access to personal data of non-U.S. persons takes place"

In its opinion, the EDPB refers favorably to the PCLOB's descriptions of FISA 702, including its finding that the program "does not operate by collecting communications in bulk."[78] The EDPB notes, however, that in the Third Annual Joint Review of the Privacy Shield[79] "it was clarified … that a 'person' to be identified as a target could refer to several individuals using the same identifier, provided that all these individuals … fulfill the applicable criteria for being targeted." The EDPB then recalls its 2019 request for "further clarification in the context of the UPSTREAM program … to exclude that massive and indiscriminate access to personal data of non-U.S. persons take place."[80]

The PCLOB report on Section 702 described "upstream" collection in detail.[81] As made clear in that report, the aspect of upstream collection that raised the most concern was so-

[77] The U.S. government has published a large volume of information about Section 702. Much of it is indexed in the Guide to Posted Documents, which provides links to officially released documents relating to the Intelligence Community's use of national security authorities. This guide can be found on the Intelligence Community's transparency platform for national security authorities, IC on the Record.

[78] EDPB opinion at para. 170.

[79] European Data Protection Board, EU-U.S. Privacy Shield – Third Annual Joint Review, November 12, 2019.

[80] EDPB opinion at para. 171.

[81] Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014. Upstream collection is described on pages 7, 35-41. For example, on page 7 the report describes upstream collection as follows: "the acquisition occurs with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies." On pages 36-37, the report makes clear that upstream collection is still centered on "selectors" such as email addresses and phone numbers:

called “abouts” collection, which NSA terminated in 2017.[82] The FISC confirmed this termination and approved new procedures that implemented the change, such that all 702 collection must be directed at communications that are “to” or “from” the target, rather than also “about” that target.[83] In recent congressional testimony, PCLOB Chair Sharon Bradford Franklin summarized the current status of this aspect of Section 702, and pointed out that “[s]ince the NSA suspended ‘abouts’ collection in 2017, it has changed the ways in which it conducts upstream surveillance under Section 702, and the changes have significantly reduced the privacy risks from upstream collection.”[84]

On April 28, 2023, the ODNI released the tenth Annual Statistical Transparency Report.[85] This report, covering calendar year 2022, documents key statistics regarding the Intelligence Community’s use of national security authorities. The report includes the estimated number of targets under Section 702. As the report states, that number “reflects an estimate of the number of non-U.S. persons who are the users of tasked selectors.” According to the report, during calendar year 2022, the Intelligence Community targeted 246,073 “users of tasked selectors.” This number represents all Section 702 targets; there is no separate category for “upstream.” Note that this number applies to all targeted users outside the United States on a worldwide basis, of which EU residents would be a subset.

> Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet communications …. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases.

[82] National Security Agency, Press Release, NSA Stops Certain Section 702 “Upstream” Activities, April 28, 2017. In that press release, NSA announced:

> Under upstream collection, NSA acquires communications "to, from, or about" a Section 702 selector. An example of an "about" email communication is one that includes the targeted email address in the text or body of the email, even though the email is between two persons who are not themselves targets…. After considerable evaluation of the program and available technology, NSA has decided that its Section 702 foreign intelligence surveillance activities will no longer include any upstream internet communications that are solely "about" a foreign intelligence target. Instead, this surveillance will now be limited to only those communications that are directly "to" or "from" a foreign intelligence target.

[83] Department of Commerce, Department of Justice, Office of the Director of National Intelligence, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, White Paper, September 2020, at page 14.

[84] Statement of Sharon Bradford Franklin, Chair, Privacy and Civil Liberties Oversight Board, before the Subcommittee on Crime and Federal Government Surveillance of the House Judiciary Committee Hearing titled “Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them,” April 27, 2023. Her discussion of “abouts” collection appears on pages 5-6. Note that Chair Franklin highlights the fact that current legislation prohibits the resumption of “abouts” without FISC approval and congressional notification, and urges Congress to “remove the provision authorizing the government to restart this type of collection.”

[85] Office of the Director of National Intelligence, Annual Statistical Transparency Report Regarding the Intelligence Community’s Use of National Security Surveillance Authorities, April 2023.

An explanatory infographic about Section 702 that the Intelligence Community published in 2017 compared the number of targeted users at the time with the estimated total number of Internet users and arrived at 0.004%.[86] Updating this methodology with estimates from 2022 (5 billion users outside the U.S. and 246,000 targets), the percentage is now about 0.005%.[87]

In short, Section 702 collection does not enable "massive and indiscriminate" surveillance.

EDPB Opinion: "The FISC does not appear to be bound by the additional safeguards of the EO 14086"

EO 14086 unquestionably binds the Executive Branch, and agencies are required by law to abide by the restrictions of EO 14086. This legally binding nature does not depend on whether compliance is subject to FISC oversight. That said, in paragraph 212 of its opinion, the EDPB states that it "regrets that … the FISC does not appear to be bound by the additional safeguards of the EO 14086, when certifying the programs authorising the targeting of non-U.S. persons."[88]

Because the Intelligence Community is obligated by law to apply EO 14086 protections to surveillance activities conducted under Section 702, the government could update the targeting, querying, and minimization procedures it must submit to the FISC each year for its review and approval as part of the annual certification process. Those procedures are legally binding on the government. For example, Section 702 expressly provides that "an acquisition authorized under [Section 702] shall be conducted only in accordance with the targeting and minimization procedures adopted in accordance with [the relevant provisions of this Section]."[89] The FISC must review and approve these procedures and if it finds the procedures meet legal requirements, it issues an order that is binding on the government.[90]

---

[86] Office of the Director of National Intelligence, Section 702 Overview, originally posted in 2017.

[87] Statistics for internet users worldwide drawn from Statista (5.3 billion) as well as number of U.S. internet users (299 million) (site last visited May 7, 2023). In addition, note that NSA's website states the following about the scope and scale of NSA collection (site last visited May 7, 2023):

> According to figures published by a major tech provider, the Internet carries 1,826 Petabytes of information per day. In its foreign intelligence mission, NSA touches about 1.6% of that. However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission - that's less than one part in a million. Put another way, if a standard basketball court represented the global communications environment, NSA's total collection would be represented by an area smaller than a dime on that basketball court.

[88] It is important to note that certain safeguards are already present in FISA Section 702 and subject to FISC supervision; we will discuss this further in the next section.

[89] 50 U.S.C. Section 1881a(c).

[90] 50 U.S.C. Section 1881a(c).

As part of the annual certification process, the FISC also examines the government's compliance with the procedures. In its November 2020 order, the FISC stated: "FISC review of the sufficiency of Section 702 procedures is not limited to the procedures as written, but also encompasses how they are implemented."[91] In that opinion, the FISC examined in detail the government's compliance record (the discussion covers 25 pages). The FISC concluded this analysis as follows: "[a]fter considering the matters discussed above and other incidents reported by the government and assessing the overall state of implementation of the current targeting, querying, and minimization procedures, the Court finds that the proposed procedures, as reasonably expected to be implemented, comply with applicable statutory and Fourth Amendment requirements."[92]

Therefore, one way to bring any additional EO 14086 commitments (as relevant to Section 702) within the FISC's ambit, is to modify applicable procedures accordingly as part of the Section 702 annual certification process. That said, as explained below, even without such modification, Section 702 and its implementing procedures already include important protections for non-U.S. persons, and those protections are subject to FISC oversight.

EDPB Opinion: "The EDPB maintains its concern that the FISC does not provide effective judicial oversight on the targeting of non-U.S. persons"

In paragraph 211 of its opinion, the EDPB raises a concern about FISC oversight on the targeting of non-U.S. persons. The opinion states:

> As the CJEU noted in its Schrems II decision, the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs. Therefore, the EDPB maintains its concern that the FISC does not provide effective judicial oversight on the targeting of non-U.S. persons which appears not to be resolved by the new EO 14086.

It is true that, as part of the annual certification process, the FISC approves the mandatory procedures and requirements that NSA must follow to identify targets but does not approve each target *ex ante*. However, it would be inaccurate to conclude that "the FISC does not provide effective judicial oversight on the targeting of non-U.S. persons." To the contrary, as discussed below, the FISC oversees in granular detail all aspects of Section 702, including the actual targeting of non-U.S. persons.

A fundamental protection regarding the targeting of non-U.S. persons under Section 702 is the following core requirement in NSA's targeting procedures:

---

[91] Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Nov. 18, 2020, at 35.
[92] Id. at 60.

> NSA must also reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting under a certification or authorization executed by the Director of National Intelligence and the Attorney General in the manner prescribed by Section 702. This assessment must be particularized and fact-based, informed by analytic judgment, the specialized training and experience of the analyst, as well as the nature of the foreign intelligence information expected to be obtained.[93]

The extensive compliance and oversight measures described in the draft adequacy decision are designed to enforce FISC orders, which include the requirement to follow the targeting procedures. Teams of expert personnel review every aspect of Section 702's implementation, identify and document compliance incidents, and report each incident in detail to the FISC. This includes the individual targeting decisions that NSA makes. They report their findings directly to the FISC as well as to Congress. This process is described in detail in the joint semiannual compliance assessments carried out by the Department of Justice's National Security Division (NSD) and the ODNI. Although public release is not required by legislation, the ODNI has carefully redacted and posted unclassified versions of this report, which can be found on IC on the Record.[94]

As described in the 24th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, NSA targets a particular non-United States person reasonably believed to be located outside the United States by "tasking" a "specific communications identifier" (also known as a "facility" or "selector") such as an email address.[95] Among the detailed requirements NSA analysts must follow is to "provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning that foreign power or foreign territory" and to document the "targeting rationale" in the tasking record.[96] As part of their compliance reviews, NSD and ODNI conduct periodic onsite visits at NSA. Prior to each such visit:

---

[93] Exhibit A, Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, October 18, 2021, at 4.

[94] www.icontherecord.tumblr.com.

[95] Department of Justice and Office of the Director of National Intelligence, Semiannual Assessment of Compliance with Procedures and Guidelines Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence (December 2021), at A-3 (Joint Semiannual Compliance Assessment).

[96] Joint Semiannual Compliance Assessment, at A-6.

> NSA electronically sends the tasking record (known as a tasking sheet) for *each* facility tasked during the reporting period to NSD and ODNI. . . . [During this initial review, the joint oversight team] reviews whether the tasking was in conformance with the targeting procedures and statutory requirements (i.e., that the target is a non-United States person reasonably believed to be located outside the United States, and that the target is reasonably expected to possess, receive, and/or likely communicate foreign intelligence information related to the categories of foreign intelligence information specified in the certifications).[97]
>
> During the onsite review, the joint oversight team examines the cited documentation underlying these identified tasking sheets . . . . The joint oversight team works with NSA to answer questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement. Interaction continues following the onsite reviews in the form of electronic and telephonic exchanges to answer questions and clarify issues. (p. 9)
>
> . . . .
>
> Additionally, the joint oversight team investigates and reports incidents of noncompliance with NSA's targeting, minimization, and querying procedures, as well as with the Attorney General Acquisition Guidelines. . . . All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC. (p. 10)

Evidence of the FISC's access to information about individual targeting determinations appears throughout the report's description of targeting compliance issues the oversight team identified and addressed. For example, the 24th joint assessment states that among the compliance incidents documented and reported to the FISC in the reporting period were

> [c]ertain . . . errors result[ing] from NSA's failure to establish a valid 'foreign intelligence information purpose' for the tasking (i.e., that the targeted user is not reasonably expected to possess or receive, and/or is not likely communicate foreign intelligence information . . . in relation to the categories of foreign intelligence information specified in the Section 702 certifications. . . . Any erroneously collected information was purged, and no [intelligence reporting based on the erroneously collected information] was identified. (p. 50).

Thus, the U.S. government has established a comprehensive compliance and oversight system that reviews Section 702 targeting decisions to ensure they comply with safeguards, with compliance issues directly reported to the FISC, together with remediation action (e.g., purging

[97] Joint Semiannual Compliance Assessment, at pp. 8-9.

of improperly acquired data). The FISC has the authority to "enter any order it deems necessary and appropriate to compel compliance."[98]

Bulk Collection: Permissibility and Limitations

Permissibility of Bulk Collection under EU Law.

In its draft resolution on the EU-U.S. Data Privacy Framework, the "LIBE Committee" of the European Parliament "[r]egrets the fact that the EO does not prohibit the bulk collection of data by signals intelligence."[99] The EDPB opinion, on the other hand, recognizes the legality of bulk collection if properly conducted and constrained. In paragraph 134, it states: "The EDPB thus notes that the CJEU did not exclude, by principle, bulk collection, but considered in its *Schrems II* decision that for such bulk collection to take place lawfully, sufficiently clear and precise limits must be in place to delimit the scope of such bulk collection."[100] Thus, the question is not whether the EO should have prohibited bulk collection, but rather, whether the safeguards and limitations for "bulk interception" are essentially equivalent to those required by EU law.

It is important to note that bulk collection is also permitted under the European Convention of Human Rights. In the Sweden case discussed previously, the ECtHR considered the legality of Sweden's bulk interception activities. In doing so, it observed that "[a]t least seven Contracting States (being Finland, France, Germany, the Netherlands, Sweden, Switzerland and the United Kingdom) officially operate bulk interception regimes over cables and/or the airways" and that "[i]n one additional State (Norway) a draft law is being debated: if enacted, it will also authorise bulk interception."[101] After examining existing case law and

---

[98] Foreign Intelligence Surveillance Court, Rules of Procedure, Rule 19(b).

[99] European Parliament, Committee on Civil Liberties, Justice and Home Affairs [LIBE Committee], Draft Motion for a Resolution, 2023/2501 (RSP), February 14, 2023. The resolution that the European Parliament passed on May 11, 2023, does not repeat this statement, and instead notes that it is "convinced that PPD-28 will not stop electronic mass surveillance of EU citizens by U.S. authorities." *European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework*, para. 3, 2023/2501 (RSP). Because EO 14086 largely supersedes PPD-28, presumably the resolution intended to refer to the EO rather than to the PPD.

[100] EDPB Opinion at para. 134. As summarized by an EU legal expert, "In the national security setting, …. the CJEU expressly conceded that intelligence services could order general and indiscriminate retention of communications data, albeit under conditions including that it be time limited, justified by the existence of a serious threat, 'strictly necessary' and 'not systematic in nature.'" Theodore Christakis, Kenneth Propp, *How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States*, Lawfare, March 8, 2023.

[101] Case of Centrum för Rättvisa v. Sweden, at paras. 222, 223. In addition, the ECtHR noted that the French Government "[emphasized] the importance of bulk interception activities for the identification of unknown threats" and argued "that States enjoy a wide margin of appreciation in operating bulk interception regimes." Id., at paras 224, 225. It also observed that Dutch government "submitted that bulk interception was necessary to

analyzing the issues raised by bulk collection, the ECtHR stated: "in order to minimise the risk of the bulk interception being abused, the Court considers that the process must be subject to 'end-to-end safeguards."[102] Although the court found shortcomings in the Swedish system, it stated: "The Court is in no doubt that bulk interception is of vital importance to Contracting States in identifying threats to their national security…. It appears that, in present-day conditions, no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power."[103]

Bulk Collection under U.S. National Security Law

When seeking to understand bulk collection under the U.S. national security legal framework, one must subdivide the topic into two distinct questions. First, can the government use bulk collection methods to access data held by U.S. companies *after* the data has been transferred to the U.S.? The short answer is "no." As stated in the European Commission's draft adequacy decision, "collection of data within the United States . . . is the most relevant for the present adequacy finding as it concerns data that has been transferred to organisations in the U.S" and such collection "must always be targeted."[104] This is well established in U.S. law and is comprehensively discussed in the draft adequacy decision.[105] Second, what does the national security legal framework have to say about the potential bulk collection of data as it is being transferred to the U.S.? Because bulk collection is forbidden by law with respect to data *after* transfer, EO 14086's bulk collection safeguards are relevant only in response to this latter question.

The earlier discussion on necessity and proportionality applies to bulk collection. In that regard, it is important to note that the EO establishes a hierarchy for collection. It directs

---

identify hitherto unknown threats to national security. In order to protect national security, intelligence services needed the tools to investigate emerging threats in a timely and effective manner.... A complicating factor in all of this was the development of new means of digital communication and the exponential increase of data that was transmitted and stored globally. In many instances the nature and origin of a particular threat was unknown and the use of targeted interception was not feasible." Id. at paras. 228, 229. The Norwegian government submitted that it was "without doubt that modern capacities like bulk interception were needed in order to find unknown threats operating in the digital domain and to enable the services to discover and follow relevant intelligence threats." Id., at para. 233 (emphasis added).

[102] The Sweden case, at para. 264.

[103] The Sweden case, at para. 365.

[104] Draft Adequacy Decision, at para. 134.

[105] Detailed descriptions of U.S. law to this effect are included paras 135-146, as well as in Annex VII (letter from ODNI General Counsel Christopher Fonzone). In short, only targeted collection is permitted under the Foreign Intelligence Surveillance Act (FISA) and under authorities for "national security letters" (a form of administrative subpoena); these legal authorities do not permit bulk collection. Note in this regard that the European Parliament's 11 May 2023 resolution (at para. H) states that "while U.S. agencies are prohibited from collecting the bulk data of US citizens living in the United States, this prohibition does not apply to EU citizens." This is inaccurate. The bulk collection prohibitions and limitations described in the draft adequacy decision apply regardless of nationality.

intelligence agencies to prioritize targeted collection over bulk collection and specifies that bulk collection "shall be authorized *only* based on a determination . . . that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection."[106] In addition, the EO requires agencies to "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."[107] Moreover, as discussed previously, the EO cuts in half the legitimate objectives for bulk collection.[108] The EO lays out a range of additional controls which are summarized in the draft adequacy decision.[109]

In short, in the limited circumstances where bulk collection is permitted by U.S. law, it may only take place if the information that is responsive to a validated intelligence priority cannot reasonably be obtained through targeted collection, and must be directed at six legitimate objectives. Once collected, the data is subject to strict use, storage, query, security, and dissemination restrictions.

EDPB Opinion: "Independent authorisation at the outset"

In its opinion, the EDPB highlights the issue of independent authorization for bulk collection. Its discussion of this point focuses on the ECtHR's opinion in the *Big Brother Watch* case.[110] The opinion quotes from that case as follows:

> The EDPB stresses that the ECtHR dedicates a significant importance to prior independent authorization in the context of bulk collection of data for national security purposes. Indeed the Court ruled in particular that '*in order to minimise the risk of the*

[106] EO 14086, Section 2(c)(ii). This principle that targeted collection should be prioritized over bulk collection—and indeed, bulk collection should be available only when targeted collection is not feasible—is reflected in the approaches of other countries. For example, in the Sweden case (para. 229), the ECtHR presented the views of the Netherlands about the need for bulk interception given that "[i]n many instances the nature and origin of a particular threat was unknown and the use of targeted interception was not feasible."

[107] EO 14086, Section 2(c)(ii)(A).

[108] EO 14086, Section 2(c)(ii)(B).

[109] Draft Adequacy Decision, at para. 134. Note that like other signals intelligence, bulk collection data must meet the minimization, security, data quality, and query requirements set forth in Section 2(c)(iii)(A), (B), and (C), and (E)). In addition, the EO imposes controls on how bulk collection may be queried (Section 2(c)(iii)(E)). The details of these controls will be laid out in agency implementation policies, which must ensure that queries are consistent with the six permitted legitimate objectives for bulk collection. Finally, documentation, compliance, oversight, and reporting measures are set forth in Sections 2(c)(iii)(D) and 2(d). In addition, as explained at length in the draft adequacy decision, oversight is provided by other entities, including the Privacy and Civil Liberties Oversight Board and the Congress. (I discuss this system of many layers with many players in Protecting Privacy and Promoting Transparency in a Time of Change: My Perspective after 14 Years as Civil Liberties Protection Officer).

[110] *Case of Big Brother Watch and Others v. United Kingdom*, App. No. 58170/13, 62322/14, and 24960/15 (May 25, 2021) (Big Brother Watch case).

> *bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime*.'
>
> . . . .
>
> In this context, the EDPB notes that the EO does not provide for such independent prior authorization for bulk collection.[111]

It is important to note that in the Big Brother Watch case, the ECtHR the ECtHR envisoned a broad form of authorization, one that focuses on "both the purpose of the interception and the bearers or communication routes likely to be intercepted" so that the authorizing body can "assess the necessity and proportionality" of bulk collection."[112] It emphasized that the prior authorization requirement does *not* require pre-approval of all selectors that might be used to later query the data. In discussing this issue, the ECtHR referred to government submissions as well as to the findings of the United Kingdom's Investigatory Powers Tribunal (IPT):

> The use of selectors – and strong selectors in particular – is one of the most important steps in the bulk interception process, as this is the point at which the communications of a particular individual may be targeted by the intelligence services….[T]he Court notes that the Governments of both the United Kingdom and the Netherlands have submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception. This was accepted by the IPT, which found that the inclusion of the selectors in the authorisation would "unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic."
>
> Taking into account the characteristics of bulk interception, the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines

[111] EDPB Opinion, at paras. 142, 144 (emphasis in original).
[112] Big Brother Watch case, at para. 352.

which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used. [113]

Both the EDPB opinion and the ECtHR's precedent make clear that purpose of prior authorization is to form part of "end-to-end safeguards" to "minimise the risk of the bulk interception power being abused."[114] In the U.S. national security legal framework, minimizing the risk of abuse is a critical task of intelligence oversight. A key player in the oversight framework is the PCLOB.[115] The EDPB discusses at some length the role of the oversight role of PCLOB and concludes: "The EDPB welcomes the PCLOB's independence and oversight of the national intelligence community."[116] In this regard, it is important to note that the PCLOB's oversight extends beyond that which the President has invited the PCLOB to carry out in EO 14086. Under the PCLOB's enabling statute, it has the authority to "continually review" not only the development of regulations, policies, and procedures within its ambit, but also their *implementation.*[117]

In addition, EO 14086 directs agencies to enable their Privacy and Civil Liberties Officers to conduct periodic oversight on how the agencies are complying with applicable law, and to provide them with "access to all information pertinent to carrying out their oversight responsibilities."[118] Agencies are required by law to have such officers in place.[119] These officers submit periodic reports on their activities to the PCLOB, which in turn has the statutory authority and responsibility to coordinate their activities.[120] Therefore, both directly and through these officers, the PCLOB can oversee the implementation of EO 14086's bulk collection safeguards on an end-to-end basis.[121]

The EDPB opinion also "notes that … various other bodies within the U.S. government oversee the activities of the U.S. intelligence agencies such as … the Congressional committees" and that those committees "can carry out their own investigations and reports."[122] Unfortunately, the opinion does not discuss Congress's functions further; in not covering Congress's role in greater depth, the EPDP opinion misses an opportunity to examine the key

---

[113] Big Brother Watch case, at para. 353, 354 (citations and cross-references omitted).
[114] EDPB Opinion at para. 142; Big Brother Watch case at para. 150.
[115] *See, generally,* Alex Joel, A System of Many Layers with Many Players, Privacy Across Borders, Feb. 13, 2023.
[116] EDPB Opinion at para. 205.
[117] 42 U.S.C. Section 2000ee(d)(1)(B) and (d)(2)(A).
[118] EO 14086, Section 2(d)(i).
[119] 42 U.S.C. Section 2000eee. The ODNI's Civil Liberties Protection Officer is one of these officers and has statutory duties under this statute as well as under the National Security Act of 1947. For a detailed description of this position, *see* Alex Joel, *Protecting Privacy and Promoting Transparency in a Time of Change: My Perspective after 14 Years as Civil Liberties Protection Officer*, Privacy Across Borders, February 13, 2023.
[120] 42 U.S.C. Section 2000ee(d)(3).
[121] Note that the PCLOB has conducted oversight over EO 12333 and PPD-28. Relevant reports can be found on the PCLOB's oversight page.
[122] EDPB opinion, at para. 194.

role Congress plays in the U.S. national security legal framework. Congress is unquestionably a separate, independent body under the U.S. Constitution, and serves as an essential check and balance on the Executive, including in the national security arena.

Congress's inherent separation and independence from the Executive distinguishes the United States from many other democracies, including parliamentary systems. Congress itself described this difference in a Senate Report:

> The U.S. Constitution provides for a system of government by three independent branches—the executive, legislative, and judicial branches—each with its own powers and prerogatives, and each with powers to 'check and balance' the powers of the other branches. Intelligence oversight by the U.S. Congress is carried out within this framework utilizing the powers and prerogatives provided by the U.S. Constitution as the basic source of its authority. Thus, the U.S. Congress is, among other things, vested by the Constitution with the responsibility to appropriate funds for the activities of the Executive branch, including intelligence activities and the Senate is required by the Constitution to provide its advice and consent to the appointment of certain Executive officials by the President, including certain intelligence officials.
>
> *In other political systems, such powers may not be lodged in the legislature*. In a unitary parliamentary form of government, for example, the legislature often does not wield power independent of the executive function. Appropriation of funds is virtually a foregone conclusion since a failure to approve the government's bill would trigger the fall of the government as a whole. Similarly, the confirmation of government officials may not be meaningful in a parliamentary system where such officials are usually senior members of the majority legislative party and may be elected members of the parliament itself.[123]

In assessing the U.S. legal system, therefore, it is important to recognize the vital role that Congress plays as an independent and co-equal branch, one in which the majority party may well be different from that of the President. Crucially for assessing the "prior authorization" issue, Congress has broad powers to fund—or refuse to fund—and to authorize—or refuse to authorize—Executive actions, including in the national security arena. As described in a report by the Belfer Center:

> The ability to authorize and appropriate funds provides Congress with a powerful tool for oversight and control of intelligence activities. This "power of the purse," a two-step process of appropriation and authorization over federal spending, provides

[123] Senate Select Committee on Intelligence, 103rd Cong., Report on Legislative Oversight of Intelligence Activities: The U.S. Experience, 1 (emphasis added) (Comm. Print 1994).

> opportunities for accountability from the Intelligence Community (IC) to Congress. As budgets are drafted and appropriations are made, Congress has the right and responsibility to ensure that the IC spends monies to best meet national security goals.[124]

Congress regularly enacts authorization statutes for the Intelligence Community.[125] These authorization statutes can contain important protections and constraints on surveillance activities. For example, Section 309 of the Intelligence Authorization Act for Fiscal Year 2015 provides for a five-year retention period for certain "nonpublic telephone or electronic communications acquired without the consent of a person who is a party to the communication."[126] As noted in the EC's draft adequacy decision, the EO now applies this retention period to U.S. person and non-U.S. person communications alike.[127] More recently, in Section 6310 of the Intelligence Authorization Act for Fiscal Year 2023, Congress specifically directed the DNI to "conduct a review to ascertain the feasibility and advisability of compiling and making public information relating to activities of the intelligence community under Executive Order 12333."[128]

Congress' "power of the purse" is perhaps the authority that provides it with the most direct impact on executive branch activities. The executive branch cannot engage in activities that cost money—and just about everything one can imagine an agency doing will cost money in some way (including the salaries of the people performing the activities). Funding comes in the form of "appropriations" from Congress. As stated by the General Accounting Office:[129]

> To the extent it is possible to summarize appropriations law in a single paragraph, this is it. Viewed in the aggregate, the Antideficiency Act and related funding statutes '[restrict] in every possible way the expenditures and expenses and liabilities of the government, so far as executive offices are concerned, to the specific appropriations for each fiscal year.'

Thus, under the U.S. national security legal framework and its system of many-layered oversight, both the PCLOB and Congress are able to provide end-to-end oversight over intelligence activities.

---

[124] Eric Rosenbach & Aki J. Peritz, Belfer Center, The Congressional Authorization and Appropriation Processes (2009).

[125] The Legislation page of the Senate Select Committee on Intelligence includes a list of Intelligence Authorization Acts.

[126] Intelligence Authorization Act for Fiscal Year 2015, Pub. L. 113-293, Dec. 19, 2014, codified at 50 U.S.C. Section 1813.

[127] Draft Adequacy Decision, at para. 150.

[128] Intelligence Authorization Act for Fiscal Year 2023 Pub. L. 117-347, Dec. 23, 2022.

[129] General Accounting Office, Principles of Federal Appropriations Law, Vol. II, at 6-38.

EDPB Opinion: "Retention periods are not clearly defined with regards to data collected in bulk"

The EDPB opinion expresses concern that retention periods "are not clearly defined in this EO with regards to data collected in bulk."[130] The EO requires that the Intelligence Community apply to non-U.S. person information "the same retention periods that would apply to comparable information concerning United States persons."[131] Section 309 of the Intelligence Authorization Act of 2015 lays out a detailed retention framework for retaining "covered communications," which are defined as "nonpublic telephone or electronic communication acquired without the consent of a person who is a party to the communication, including communications in electronic storage."[132] This framework in essence provides for a five-year retention period for such communications unless they have earlier been "affirmatively determined … to constitute foreign intelligence or counterintelligence or is necessary to understand foreign intelligence or counterintelligence."[133] The EO now ensures that this statutory retention framework applies to all such communications, regardless of whether they pertain to U.S. or non-U.S. persons.

In addition, the EO provides that agencies "shall continue to use the policies and procedures issued pursuant to" PPD-28 until they are updated pursuant to the EO.[134] NSA's existing PPD-28 policy specifies how it will retain signals intelligence data and sets forth the 5-year retention period.[135]

Conclusion

The EO's use of the terms "necessary" and "proportionate," read in the context of U.S. law and legal traditions, constrains signal intelligence activities in a closely comparable manner to how those terms are used under EU and ECHR law. Both the U.S. and EU legal frameworks establish controls in law with enforceable rights, approach the identification of national security objectives in similar fashion, and accept the need for bulk collection when accompanied by appropriate safeguards.

---

[130] EDPB Opinion, at para. 146.
[131] EO 14086, Section 2(c)(iii)(A)(2).
[132] 50 U.S.C. Section 1813.
[133] 50 U.S.C. Section 1813(b)(3)(B).
[134] EO 14086, at Section 2(c)(iv)(A).
[135] National Security Agency, PPD-28 Section 4 Procedures, Section 6 (January 12, 2015).