**U.S. Department of Justice**

National Security Division

*Office of the Assistant Attorney General* *Washington, D.C. 20530*

**Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086**

Executive Order 14086, signed on October 7, 2022, establishes a two-level redress mechanism for the review of qualifying complaints filed by individuals through an appropriate public authority in a "qualifying state" and alleging certain violations of U.S. law concerning signals intelligence activities. The Attorney General may designate a country or a "regional economic integration organization" as a qualifying state if he determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that it meets three requirements set forth in section 3(f) of the Executive Order.

This memorandum, prepared by the National Security Division of the Department of Justice, provides information in support of designating as qualifying states the European Union ("EU"), which is a regional economic integration organization comprising twenty-seven Member States, and the three non-EU countries Iceland, Liechtenstein, and Norway. The information set forth below shows how those entities meet the three requirements in section 3(f) of Executive Order 14086. Those entities are grouped for consideration here because together they make up the European Economic Area ("EEA"). The agreement establishing the EEA makes applicable to Iceland, Liechtenstein, and Norway the EU's General Data Protection Regulation ("GDPR"), which includes provisions restricting the cross-border transfer of personal data.[1] Designating the EU and those three additional EEA countries (together the "EU/EEA") as qualifying states, so that individuals in any of the thirty EU/EEA countries may file complaints through the redress mechanism established by Executive Order 14086, is an essential step for the European Commission to issue an adequacy decision for the United States under the GDPR as part of the EU-U.S. Data Privacy Framework. The adequacy decision will in turn permit the transfer of personal information for commercial purposes in reliance on the EU-U.S. Data Privacy Framework from the territory of EU/EEA countries to the territory of the United States.

## I. Determinations to be made to designate a "qualifying state" under Executive Order 14086

Section 3(f) of Executive Order 14086 lists three determinations to be made to designate a country or regional economic integration organization a "qualifying state," followed by three corresponding determinations any one of which may be a basis to revoke or amend a designation:

[1] *See* Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation" or "GDPR"); Joint Committee Decision incorporating Regulation (EU) 2016/679 into Annex XI of the EEA Agreement (6 July 2018).

*(i) To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:*

*(A) the laws of the country, the regional economic integration organization, or the regional economic integration organization's member countries require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization;*

*(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries of the regional economic integration organization permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; and*

*(C) such designation would advance the national interests of the United States.*

*(ii) The Attorney General may revoke or amend such a designation, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:*

*(A) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not provide appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or to a member country of the regional economic integration organization;*

*(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not permit the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; or*

*(C) such designation is not in the national interests of the United States.*

## II. Determination that the laws of the EU/EEA require appropriate safeguards for signals intelligence activities affecting U.S. persons

The first determination to be made to designate the EU/EEA, pursuant to section 3(f)(i)(A) of Executive Order 14086, is that the laws of the EU/EEA "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory" of an EU/EEA country. The following discussion describes how the laws of the EU/EEA meet this standard.

As a threshold matter, it is important to note that Executive Order 14086 does not require a "qualifying state" to provide identical or reciprocal safeguards to those provided under U.S. law. Rather, the Executive Order simply calls for a determination that the laws of the qualifying state "require appropriate safeguards." The flexibility inherent in this standard accounts for the fact that different countries, even those sharing democratic values and a commitment to the rule of law, will have legal and national security systems with differing histories and institutions, such that they may legitimately take differing approaches towards enacting privacy safeguards for signals intelligence activities. In other words, the Executive Order's "appropriate safeguards" standard does not impose a rigid "one-size-fits-all" model, but rather asks, in light of the importance of maintaining trust and confidence in the free flow of data in today's networked global economy, whether the laws of a potential qualifying state, when viewed holistically, require appropriate privacy safeguards with respect to its national security activities.

This deferential approach, allowing for differing yet legitimate approaches to protecting privacy in the conduct of signals intelligence activities, is an important factor when considering this first determination under section 3(f) of Executive Order 14086 for the EU/EEA. The United States and the thirty EU/EEA countries have adopted a variety of different approaches to authorizing signals intelligence activities and enacting associated privacy safeguards into law. As discussed below, in some areas it appears that U.S. safeguards, as adopted in Executive Order 14086 and other U.S. law, surpass those required by the laws of the EU/EEA, while in other areas the laws of the EU/EEA require safeguards not provided in the United States.

All thirty EU/EEA countries are contracting parties to the European Convention on Human Rights ("ECHR"), under which the domestic laws of EU/EEA countries governing signals intelligence activities and establishing related privacy safeguards have been subject to review for decades by the European Court for Human Rights ("ECtHR"). That court has identified categories of "minimum safeguards" that EU/EEA countries must adopt for signals intelligence activities, which are similar on the whole to the safeguards in Executive Order 14086—requiring that intelligence surveillance be undertaken in pursuit of a legitimate objective and based on reasonable justifications, restricting the post-acquisition handling of the data acquired, establishing oversight bodies to ensure adherence to legal requirements, and ensuring a path to individualized redress. In this regard, the European Commission has provided a letter, attached to this memorandum, signed by EU Commissioner for Justice Didier Reynders and addressed to the Attorney General and the Secretary of Commerce, which sets forth information about the safeguards for signals intelligence activities required by the ECHR, as well as applicable EU law, along with his view that "this information provides a strong basis to inform

your determination under section 3(f)(i)(A) of Executive Order 14086 that appropriate safeguards apply in this area in the EU/EEA."

Additionally, twenty-four EU/EEA countries, the European Union, and the United States are signatories to the 2022 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, which sets forth seven principles for protecting privacy during government access to data for law enforcement and national security purposes, reflecting their shared democratic values and commitment to the rule of law. Those seven principles are on the whole similar both to the "minimum safeguards" that the European Court for Human Rights has identified for signals intelligence activities in EU/EEA countries and to the safeguards in Executive Order 14086. In that OECD Declaration, the United States affirms that it takes into account a destination country's effective implementation of the Declaration's principles as a positive contribution towards facilitating transborder data flows.

Taking into account these commitments in the OECD Declaration, together with the deferential "appropriate safeguards" standard in Executive Order 14086, and the importance of commercial transfers of data between Europe and the United States, as well as EU/EEA countries' clear commitment to privacy with respect to their national security activities, it is within the Attorney General's discretion to conclude, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that notwithstanding certain areas of divergence between the laws of the United States and the laws of the EU/EEA, the laws of the EU/EEA require appropriate safeguards for purposes of a section 3(f)(i)(A) determination.

The following discussion supporting this determination proceeds as follows. Subsection (a) analyzes the safeguards required by the ECHR and applicable EU law, and subsection (b) discusses safeguards required by the domestic laws of representative EU/EEA countries. Subsection (c) provides an overall assessment of these signals intelligence safeguards, concluding that the EU/EEA's safeguards, when viewed on the whole, demonstrate a sufficient commitment to privacy with respect to their national security activities to determine that the safeguards required by the laws of the EU/EEA are "appropriate." The discussion in subsection (b) of the laws of individual EU/EEA countries is a limited analysis of publicly available statutes, regulations, and court decisions in representative EU/EEA countries, drawing also on other sources including the reports of independent expert bodies such as the EU Fundamental Rights Agency. In light of our limited access to information about the intelligence laws of EU/EEA countries in this area, and the complexity of such laws, further exchanges of information between the European Commission, EU/EEA countries, and the United States would be welcome to ensure that the United States has an accurate understanding of the safeguards in the laws and practice of each EU/EEA country for signals intelligence activities that may affect the personal data of U.S. persons.

a. Safeguards required by the European Convention on Human Rights and EU law

i. The European Convention on Human Rights

All thirty EU/EEA countries are contracting parties to the ECHR. The ECHR establishes the ECtHR, the jurisdiction of which extends, according to article 32 of the ECHR, to all matters concerning its interpretation and application. Regarding interferences with privacy, article 8 mandates that "[e]veryone has the right to respect for his private and family life, his home and his correspondence," with a proviso for government interference stating that "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 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 ECtHR has for decades decided cases applying article 8 to EU/EEA countries' laws authorizing government surveillance of individuals' electronic communications for law enforcement and national security purposes. In its seminal decision in *Klass and Others v. Germany*, the ECtHR stated that it "must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse." *Klass and Others v. Germany,* Application no. 5029/71, § 50 (1978). Recognizing the need for each country to authorize and conduct surveillance for national security purposes under its own domestic legal system, the ECtHR in *Klass* stated that "as concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion." *Id.* §§ 48-49. The ECtHR then decided that the challenged intelligence surveillance statute in Germany had sufficient limitations and conditions to satisfy article 8 of the ECHR, even though the German statute excluded judicial oversight and effectively restricted judicial redress, given that sufficient other independent oversight and redress mechanisms were in place. *Id.* §§ 22-24, 49-56.

The ECtHR has over decades emphasized the legitimacy of differences among national approaches to protecting privacy in the exercise of national security authorities. In two 2021 decisions the ECtHR reiterated that "national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security," consistent with the Convention requirement for safeguards that establish "adequate and effective guarantees against abuse." *Centrum För Rättvisa v. the Kingdom of Sweden*, Application no. 35252/08, §§ 252-53 (2021); *Big Brother Watch and Others v. the United Kingdom*, Application nos. 58170/13, 62322/14 and 24960/15, §§ 338-39 (2021). This principle rests on longstanding ECtHR jurisprudence affording national authorities the discretion to choose how to protect national security while at the same time protecting individual rights, and not substituting the ECtHR's own assessments for those of national authorities. *See, e.g.*, *Kennedy v. United Kingdom*, Application no. 26839/05, § 150 (2010); *Weber and Saravia v. Germany*, Application no. 54934/00, § 106 (2006); *Klass and Others v. Germany*, § 49 ("It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field."). Furthermore, the ECtHR generally does not prescribe exact standards or constraints that a country must adopt, but instead reviews a country's laws in the aggregate. In its recent review of Sweden's intelligence surveillance program, the "Court further

reiterate[d] that it is not its role to prescribe an ideal model for signals intelligence but rather to review for Convention compliance the existing legal and practical arrangements, which vary conceptually and functionally from one Contracting Party to another. In this exercise, the Swedish signals intelligence model and its safeguards against abuse must be seen as one whole." *Centrum För Rättvisa v. Sweden*, § 366.

The ECtHR has identified several categories of "minimum safeguards" that EU/EEA countries must adopt to ensure effective safeguards against abuse of government powers to access electronic communications for national security purposes. The Commission's letter, attached to this memorandum, explains that these categories of minimum safeguards identified by the ECtHR are similar on the whole to the safeguards adopted in section 2(c) of Executive Order 14086. They include the grounds for authorizing surveillance; the categories of people liable to have their communications accessed; procedures for examining, using, storing, retaining, and erasing the data obtained; procedures for preserving the integrity and confidentiality of data; precautions to be taken when communicating the data to other parties; arrangements for supervising the implementation of surveillance measures and compliance with safeguards; and the remedies provided for by national law. *See Roman Zakharov v. Russia*, Application no. 47143/06, §§ 233-34 (2015); *Weber and Saravia v. Germany*, § 95; *Kennedy v. United Kingdom*, §§ 152-53; see discussion at *Centrum För Rättvisa v. the Kingdom of Sweden*, §§ 249-55; *Big Brother Watch and Others v. the United Kingdom* § 335-41. The ECtHR has also found it important for domestic law to require intercepting agencies to keep records of interceptions, in order to ensure that supervisory bodies have effective access to details of surveillance activities undertaken. *Roman Zakharov v. Russia*, § 272; *Big Brother Watch and Others v. the United Kingdom*, § 356.

Comparable to the requirement in section 2(a)(i) of Executive Order 14086 that U.S. signals intelligence activities be authorized by law, article 8 of the ECHR requires that any interference by a public authority of an EU/EEA country with an individual's right to privacy for national security purposes be "in accordance with the law." The Commission's letter refers to ECtHR decisions interpreting this provision to require not only that a surveillance measure have a basis in domestic law, but also to refer to the quality of the law, which should be accessible to the public and foreseeable as to its consequences. *See, e.g.*, *Kennedy v. United Kingdom*, § 151; *Amann v. Switzerland*, Application no. 27798/95, § 50 (2000); *Malone v. United Kingdom*, Application no. 8691/79, §§ 66-68 (1984). The law must be sufficiently clear to give individuals an adequate indication as to the circumstances in which, and the conditions under which, public authorities are empowered to resort to surveillance. *See Malone v. United Kingdom*, § 67. Moreover, the law must indicate with sufficient clarity the scope of any discretion conferred on competent authorities and how it may be exercised. *See Roman Zakharov v. Russia*, § 230; *Weber and Saravia v. Germany*, § 94.

Comparable to the requirement in section 2(b) of Executive Order 14086 that U.S. signals intelligence activities be conducted in pursuit of a legitimate objective, the Commission's letter refers to ECtHR decisions requiring that intelligence surveillance pursue a legitimate aim, such as protecting national security. *See, e.g.*, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332/00, § 87 (2006). This requirement for a legitimate objective is rooted in the requirement in article 8 of the ECHR that interference in privacy rights must be foreseeable "in

accordance with the law"; article 8 also specifies that such interference must be "in the interests of national security, public safety or" other listed purposes. The ECtHR has recognized that the term "national security" in a country's intelligence legislation sets out a sufficiently clear objective, in particular where implementing authorities provide further clarification on how the term is applied in practice; the court has recognized in this context specific examples of activity constituting threats to national security, including espionage, terrorism, activities threatening the free democratic constitutional order, threats to the security of allies' armed forces stationed in a country's territory, and activities which are intended to undermine or overthrow Parliamentary democracy. *See, e.g.*, *Kennedy v. United Kingdom*, § 159; *Roman Zakharov v. Russia*, § 247; *Klass and Others v. Germany*, §§ 46, 48.

Comparable to the necessity and proportionality requirements in section 2 of Executive Order 14086, the Commission's letter refers to the ECtHR's application of principles of necessity and proportionality in cases involving article 8 of the ECHR. Article 8 sets out an explicit "necessity" requirement, stating that interference with privacy rights is permissible only where "necessary in a democratic society in the interests of national security" or other specified purposes. Regarding proportionality, while the ECtHR has "recognize[d] that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens . . . must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued." *Segerstedt-Wiberg and Others v. Sweden*, § 88; *see also Roman Zakharov v. Russia*, § 260 (surveillance measures must "meet[] the requirement of 'necessity in a democratic society', as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued"); *Kennedy v. United Kingdom*, § 155. Furthermore, according to the principle of proportionality, the interest of the state in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his or her private life. *See Leander v. Sweden*, Application nos. 62332/00, 9428/81, § 59 (1987).

EU/EEA countries (unlike the United States) may legally authorize the collection of information in bulk for national security purposes within their territories. If they do so, the ECtHR has required additional safeguards. The Commission's letter refers to ECtHR decisions requiring that bulk surveillance be carried out subject to "end-to-end safeguards." *Centrum för Rättvisa v. Sweden*, § 264; *Big Brother Watch and Others v. the United Kingdom*, § 350. In particular, an assessment has to be made at each stage of the process of the necessity and proportionality of the measures being taken, the collection should be subject to independent authorization at the outset, and the operation should be subject to supervision and independent *ex post facto* review. *See, e.g.*, *Centrum för Rättvisa v. Sweden* § 270; *Big Brother Watch and Others v. the United Kingdom*, § 356.

The Commission's letter refers to specific safeguards applicable to the sharing of data collected in bulk with foreign intelligence services. When disseminating data gathered through bulk surveillance to a foreign government, an EU/EEA country must ensure that the receiving country has safeguards in place to prevent abuse and disproportionate interference, and must guarantee the secure storage of the material and restrict its onward disclosure. *Big Brother Watch v. the United Kingdom*, § 362. In addition, the transfer of data to foreign intelligence services should be subject to independent control. *Id.* The receiving country need not

necessarily provide protections for the data that are comparable to those of the sending EU/EEA country, nor must an assurance necessarily be given prior to every transfer. *Id.; see also Centrum För Rättvisa v. the Kingdom of Sweden*, §§ 326-30 (identifying the absence of a requirement to consider privacy interests of affected individuals when transmitting intelligence material to foreign partners a shortcoming in the Swedish bulk interception program).[2]

Independent and effective oversight of intelligence activities is among the safeguards required by the ECtHR. Although the ECtHR has not required that intelligence surveillance measures always be subject to *ex ante* review and approval by an independent body, it has required at least effective *post factum* oversight and review. *See Szabó and Vissy v. Hungary*, Application no. 37138/14, § 77 ("The *ex ante* authorisation of such a measure is not an absolute requirement *per se*, because where there is extensive *post factum* judicial oversight, this may counterbalance the shortcomings of the authorization"); *Big Brother Watch and Others v. the United Kingdom*, § 350. The ECtHR has required that intelligence surveillance be subject to independent oversight, normally by the judiciary and, in any event, by an authority that is independent of the executive. *See Szabó and Vissy v. Hungary*, § 74; *Klass and Others v. Germany*, § 55. The ECtHR has highlighted that criteria for independence of an intelligence oversight body include, among others, "the manner of appointment and the legal status of the members of the supervisory body" and the absence of conflicts of interest. *Roman Zakharov v. Russia*, §§ 278-80. Further, with respect to investigatory powers, the ECtHR has emphasized "that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required." *See id.* § 281 (citing *Kennedy v. United Kingdom*, § 166). The ECtHR has also highlighted that oversight bodies must be vested with sufficient powers to remediate unlawful conduct. *See id.* § 282 (highlighting the power to "stop or remedy the detected breaches of law," to hold those responsible accountable, and to destroy unlawfully obtained intercept material); *Klass and Others v. Germany*, § 56.

Regarding redress for individuals submitting complaints alleging violations of intelligence laws, the laws of the EU/EEA may be compared to the redress mechanism established by Executive Order 14086, which would become available to EU/EEA individuals upon Attorney General designation of the EU/EEA. The redress mechanism established by the Executive Order ensures that individuals may obtain effective redress in response to complaints alleging unlawful signals intelligence activities while protecting the government interest in the confidentiality of those activities. Whether an individual was or was not subject to surveillance is typically sensitive national security information held in secret, so that an individual filing such a complaint typically will not be able to demonstrate that the government accessed his or her data. The redress mechanism established by the Executive Order ensures effective redress while accounting for these factors, by referring individuals' complaints to an independent entity which has full access to the classified national security information necessary to review this type of

[2] We are not aware of information indicating that the ECtHR has specified precise further requirements restricting how EU/EEA countries handle data acquired through signals intelligence—including exactly how long such data may be retained before being destroyed, under what specific conditions the data may be shared with other agencies such as the EU/EEA country's own law enforcement agencies or the security agencies of another country, and what restrictions apply to querying of the data. Thus these issues may be left to be regulated by the domestic laws of EU/EEA countries.

complaint, has binding authority to order remedial measures, and can inform the individual that the review was completed and remedial orders were issued to address any identified violation of law. E.O. 14086 §§ 3(d)(i)(H), 3(d)(ii)-(iv); 28 C.F.R. §§ 201.7(d), 201.9(b), (g), (h).

Two paths to individualized redress must be considered under the laws of the EU/EEA—the ECtHR itself, and redress mechanisms under the laws of EU/EEA countries. Under article 34 of the ECHR any individual, regardless of nationality or place of residence, may, after exhausting remedies under the domestic law of an EU/EEA country, bring a complaint against that EU/EEA country before the ECtHR. A U.S. person may thus allege that specific signals intelligence activities undertaken by an EU/EEA country violated the ECHR (or, alternatively, that the EU/EEA country's national legal framework governing signals intelligence activities violates the ECHR). In principle the ECtHR could provide effective redress for such a complaint. However, where the U.S. person complainant is not able to demonstrate that the intelligence agencies of an EU/EEA country accessed his or her data, affording redress could be difficult in practice unless the ECtHR can require the government of the EU/EEA country to disclose information about surveillance activities undertaken by its intelligence agencies. While the ECtHR's rules authorize it to take measures such as conducting an inquiry, carrying out an on-site investigation, or inviting parties to produce documentary evidence, and EU/EEA countries are obliged to assist the ECtHR as necessary in implementing such investigative measures, Rules of Court, ECtHR, Annex to the Rules (concerning investigations), Rules A1-A2 (20 March 2023), we are not aware of ECtHR jurisprudence expressly addressing whether the ECtHR is empowered to compel the government of an EU/EEA country to disclose sensitive national security information. Only if such compulsory powers exist would the ECtHR be able to assess whether a U.S. person complainant was subject to surveillance by an EU/EEA country's intelligence agencies, which is a prerequisite to assessing the legality of any such surveillance and fashioning a remedy if needed.

As for redress under the domestic laws of EU/EEA countries, the Commission's letter refers to ECtHR decisions requiring that, among the "minimum safeguards" for intelligence surveillance, an EU/EEA country must provide individuals a path to redress for complaints alleging that signals intelligence activities conducted by the EU/EEA country violated its domestic law, even where the individual is not aware of and is not able to demonstrate that he or she was actually subject to surveillance by the EU/EEA country's intelligence agencies. *See Centrum För Rättvisa v. Sweden*, § 271; *Roman Zakharov v. Russia*, § 234. Further, the redress provided by EU/EEA countries for complaints alleging violations of intelligence surveillance laws, whether through a court or non-judicial redress mechanism, must be independent and have binding authority. *See Big Brother Watch*, § 359; *Centrum För Rättvisa v. Sweden*, § 273.[3] The Commission's letter also refers to broader ECtHR case law (outside the context of challenges to intelligence surveillance) indicating other requirements relating to redress, such as the criteria for

[3] We did not identify further information regarding precisely what other safeguards the ECHR requires in EU/EEA countries for judicial or non-judicial redress for complaints alleging violations of intelligence surveillance laws. For example, it is not clear whether the ECtHR requires judicial or non-judicial redress mechanisms in EU/EEA countries to hear all types of complaints including allegations by foreigners located abroad concerning all types of signals intelligence activities including access to communications sent from or received abroad or to data in transit, or to ensure that the entity administering the redress mechanism has full access to classified information.

a tribunal's independence[4] and due process requirements when sensitive national security information is in evidence.[5] As additional challenges are brought against EU/EEA countries' signals intelligence activities, the ECtHR may have occasion to apply similar requirements in the context of redress as a safeguard for intelligence surveillance under article 8 of the ECHR.

In summary, ECtHR jurisprudence identifies categories of "minimum safeguards" that EU/EEA countries must adopt for signals intelligence activities, which are similar on the whole to the safeguards in Executive Order 14086. The Commission has advised that in a number of areas, the ECtHR indicates with some clarity what safeguard is required—for example, EU/EEA countries must ensure that signals intelligence activities are authorized by law; establish in law the objectives for which signals intelligence activities may be authorized and conducted; ensure that signals intelligence activities are necessary and proportional in light of the authorized objective; require additional safeguards for bulk collection; establish independent oversight mechanisms with sufficient powers to remediate unlawful conduct; and provide individuals a

[4] For purposes of the right to a fair trial under article 6(1) of the ECHR, the ECtHR has referred to criteria for the independence of a tribunal including the manner of appointment of a tribunal's members, the duration of their term of office, the existence of guarantees against outside pressures and whether the body presents an appearance of independence. *See Kleyn and Others v. the Netherlands*, Application nos. 39343/98, 39651/98, 43147/98 and 46664/99, § 190 (2003) (challenges to independence of Council of State deciding appeals against government's transport infrastructure planning decisions); *Langborger v. Sweden*, Application no. 11179/84, § 32 (1989) (challenge to independence of Rent Review Board and House and Tenancy Court hearing dispute over rent and other lease terms for apartment). With respect to the manner of appointment of tribunal members, the ECtHR has further recognized that the appointment by the Executive is permissible, provided that appointees are free from influence or pressure when carrying out their adjudicative role. *See Henryk Urban and Ryszard Urban v. Poland*, Application no. 23614/08, § 49 (2010) (challenge to independence of district court deciding criminal case), *citing Campbell and Fell v. the United Kingdom*, Application nos. 7819/77, 7878/77, § 79 (1984) (challenge to independence of Prison Board of Visitors hearing disciplinary proceedings for prisoners). In addition, the ECtHR has stressed that a tribunal must be composed of members selected on the basis of merit, fulfilling requirements of technical competence and moral integrity. *See Guðmundur Andri Ástráðsson v. Iceland*, Application no. 26374/18, §§ 219-220 (2020) (challenge to independence of Court of Appeal upholding criminal conviction).

[5] Regarding due process requirements for purposes of article 6(1) of the ECHR, the ECtHR has held that in order to carry out a detailed examination, a tribunal must be able to take complete cognizance of all relevant documents and evidence. *See Ternovskis v. Latvia*, Application no. 33637/02, § 68 (2014) (challenge to refusal of security clearance)*; Regner v. Czech Republic*, no. 35289/11, § 152 (2017) (challenge to revocation of security clearance). Further, the ECtHR has held that, while there may be restrictions on the right to an adversarial procedure, those must be strictly necessary in the light of a strong countervailing public interest such as national security and must be counterbalanced by procedures followed by judicial authorities. *Regner v. Czech Republic*, § 148*; Ternovskis v. Latvia*, § 67. Such restrictions may include withholding confidential evidence from the parties, *Regner v. Czech Republic*, § 148, or not holding oral hearings, *Kennedy v. the United Kingdom*, § 188 (challenging whether proceedings before Investigatory Powers Tribunal satisfied right to fair hearing under article 6 of ECHR). In a variety of contexts not involving challenges to the lawfulness of intelligence surveillance, the ECtHR has recognized various mechanisms to balance national security and due process, such as special advocates with access to classified information (i.e. appointed to represent individuals in closed hearings, with the right to submit arguments on their behalf, for instance on whether or not information was lawfully withheld); or, in cases involving classified evidence, independent and impartial tribunals with unlimited access to the classified evidence and the power to examine the reasons given for non-disclosure of classified documents. *See Regner v. Czech Republic*, §§ 152-53*; A and Others v. the United Kingdom*, Application no. 3455/05, § 220 (2009) (challenge under article 5(4) of ECHR to security-based detention); *I.R. and G.T. v. the United Kingdom,* Application nos. 24876/12 and 63339/12, §§ 61, 63 (2014) (challenge to security-based denial of entry into country); *Jasper v. the United Kingdom*, Application no. 27052/95, § 56 (2000) (challenge to prosecution's non-disclosure of material in criminal proceeding).

path to independent and binding redress for complaints alleging that signals intelligence activities conducted by an EU/EEA country violated its domestic law, even where the individual is not able to demonstrate that he or she was actually subject to surveillance. In a number of other areas, however, it appears that the ECtHR has not, or has not yet, specified the precise safeguards that are required for an EU/EEA country's signals intelligence activities, either because the ECtHR has not had occasion to do so or because the ECtHR leaves those issues to EU/EEA countries' discretion.

ii. The law of the European Union

In addition to the ECHR which applies in all thirty EU/EEA countries, twenty-seven of the thirty EU/EEA countries are Member States of the EU. Those twenty-seven countries are parties to the EU Treaties and are subject to the law of the EU on matters with respect to which they have conferred competence upon the EU under the treaties. Certain EU legal acts, including the GDPR as noted above, are also incorporated into the EEA Agreement and are thus applicable to the three additional EU/EEA states.

The EU Charter of Fundamental Rights—which has the same legal status as the EU Treaties—protects against interferences with privacy (article 7) and data protection (article 8). The Commission's letter explains that the rights enshrined in the ECHR, including the right to the respect for privacy discussed above, constitute general principles of EU law. Treaty on the European Union art. 6(3). According to article 52(3) of the Charter, the rights of the Charter that correspond to those of the ECHR must have the same meaning and scope as the ECHR, unless EU law provides more extensive protections. In other words, as the the Court of Justice of the EU ("CJEU") has held, the corresponding rights of the ECHR are considered the "minimum threshold of protection." *La Quadrature du Net and Others v Premier Ministre and Others*, Joined Cases C-511/18, C-512/18 and C-520/18, § 124 (2020) ("*La Quadrature du Net*").

At the same time, the EU Treaties specify that "national security remains the sole responsibility of each Member State." Treaty on European Union art. 4(2). Accordingly, unlike the ECtHR, the CJEU has not undertaken a comprehensive review of any EU Member State's laws authorizing signals intelligence activities. Instead, regarding safeguards that are required for signals intelligence activities in EU Member States, the CJEU has clarified that the requirements of EU law apply only to data processing obligations imposed by Member States on private operators, whereas national constitutional requirements and the ECHR apply when EU Member States directly implement measures for national security purposes without imposing data processing obligations on private operators. *See Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, Case C-623/17 (2020) ("*Privacy International*"), §§ 47-48. Consistent with the EU's established competence to regulate how personal data is processed by private companies, CJEU decisions on government access to electronic communications have historically focused on the validity of EU or Member State laws requiring private companies to retain their customers' personal data for possible later access by Member States' law enforcement agencies. *See, e.g.*, *Tele2 Sverige and Others v. Watson and Others*, Joined Cases C-203/15 and C-698/15 (2016) (precluding Member State laws requiring providers to retain electronic communications data on a general and discriminate basis; setting conditions for access by Member States' law enforcement agencies to retained data); *Digital*

*Rights Ireland and Seitlinger and Others v. Minister for Justice, Equality and Law Reform and Others*, Joined Cases C-293/12 and C-594/12 (2014) (invalidating EU regulation that required providers to retain electronic communications data of all subscribers and registered users and did not set conditions relating to access to the data by Member States' law enforcement agencies).

In two decisions issued on October 6, 2020, the CJEU for the first time reviewed aspects of EU Member States' laws requiring private companies to retain or disclose data for national security purposes. *La Quadrature du Net*; *Privacy International*. In both decisions the CJEU affirmed that EU Member State legislation imposing a legal obligation on a private company to retain data or disclose data to government agencies for national security purposes falls within the scope of EU law. *La Quadrature du Net* §§ 87-104; *Privacy International* §§ 30-49. In contrast, as discussed more fully below, both decisions held that Member States' access to data not based on the imposition of a legal obligation on a private company to process data falls outside of EU law. In one decision, in addition to its rulings on data retention requirements, the CJEU held that a French law requiring a company to employ an algorithm to screen targeted government requests against its general customer traffic and location data and disclose matching data in real time to the government to identify terrorism threats was permitted under EU law only if an independent body verifies that a serious national security threat is genuine and present or foreseeable and that disclosure of the data is based on a valid suspicion that the targeted person is involved in terrorist activities. *La Quadrature du Net* §§ 169-92. In the other decision, the CJEU recognized that the objective of protecting national security is capable of justifying more serious interferences with data privacy than might be justified by other state objectives, but found that the United Kingdom's laws authorizing the general and indiscriminate transmission of personal data by a private company to the government for national security purposes (which have since been reformed under the law of the United Kingdom) failed to meet the requirement of "proportionality" in EU law. *Privacy International* §§ 50-81.

The Commission's letter explains that these two CJEU decisions from 2020 reflect general principles on necessity and proportionality restricting government interferences with the right to data protection. Regarding the principle that limitations on the right to data protection may only be imposed for a legitimate objective, for example, the CJEU indicated that the protection of national security, while remaining the sole responsibility of each Member State, encompasses the prevention and punishment of activities capable of seriously destabilizing the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself (e.g. terrorist activities). *La Quadrature du Net*, § 135. The CJEU also indicated that it follows from EU law that any limitation on the right to privacy must be necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others, and that the importance of the public interest objective pursued must be proportionate to the seriousness of the limitation to the rights of the individual. *Id.* §§ 130-31.

Beyond these two 2020 decisions, the CJEU does not appear to have identified what privacy safeguards are specifically required by EU law, beyond those required by the ECHR, for signals intelligence activities authorized by an EU Member State, particularly as they may affect the personal data of U.S. persons or other non-EU persons located outside the EU. For example, the CJEU has not, to our knowledge, directly addressed what requirements specific to EU law

apply to an EU Member State's judicial or non-judicial redress mechanisms for complaints by any person, including a U.S. person, alleging that the activities of an intelligence agency of a Member State violated the Member State's domestic law.

iii. Applicability of safeguards required by the ECHR and EU law to extra-territorial signals intelligence activities

It appears that none of the safeguards for signals intelligence activities discussed above have thus far been applied to an EU/EEA country's extraterritorial signals intelligence activities—that is, signals intelligence activities conducted outside an EU/EEA country's jurisdiction—either by the ECtHR under the ECHR[6] or by the CJEU under EU law.[7] Rather, the requirements of the ECHR and EU law for signals intelligence activities appear to have been applied to require privacy safeguards for EU/EEA countries' government access to electronic communications or other data only within each country's territorial jurisdiction.

However, the United States and other countries have consistently taken the position that access by the intelligence agencies of a destination country to data in transit between countries should not be a relevant consideration for the regulation of commercial flows of data.[8] The primary basis for this position is that a destination country's laws and practices regarding signals intelligence activities do not uniquely govern the privacy protection that is afforded to data located outside of that country or outside of any country. Rather, assessing possible privacy interferences with data while in transit would require reviewing the widely divergent laws and

[6] ECtHR decisions on intelligence surveillance appear to have reviewed only the domestic surveillance programs of EU/EEA countries. In three ECtHR decisions we have identified that were not brought by a resident of the respondent state, the ECtHR's review concerned only surveillance *within* the respondent state's territorial jurisdiction. *Big Brother Watch and Others v. the United Kingdom*, § 272 ("the Government raised no objection under Article 1 of the Convention, nor did they suggest that the interception of communications was taking place outside the State's territorial jurisdiction. . . . . Therefore, for the purposes of the present case, the Court will proceed on the assumption that . . . the matters complained of fell within the jurisdictional competence of the United Kingdom"); *Liberty and Others v. the United Kingdom*, Application no. 58243/00, §§ 42, 47 (2008) (applicants, which included Irish civil liberties organizations, and the government of the United Kingdom both proceeded on the basis that the claimed interception of communications occurred at a facility in England); *Weber and Saravia v. Germany*, §§ 86-88 (rejecting claim by the Uruguayan applicants that the surveillance involved extraterritorial measures, and noting that "[s]ignals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In light of this, the Court finds that the applicants failed to provide proof . . . that the German authorities . . . have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.").

[7] CJEU decisions likewise indicate that EU law does not apply to EU Member States' extraterritorial signals intelligence activities, which generally involve direct, non-compulsory access to data, not imposing obligations on companies within its jurisdiction to disclose data. *La Quadrature du Net*, § 103 ("where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only . . . ."); *Privacy International* § 48; *accord* EU Fundamental Rights Agency, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Update* at 11-14 (2023) (EU law applies to surveillance by Member States' intelligence services of electronic communications only where private companies assist with the surveillance).

[8] *See, e.g.*, U.S. Government White Paper, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after* Schrems II at 17-18 (2020), *available at* https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF .

practices of many other countries than the destination country, and also the possibility of illicit access by a wide range of private actors. Accordingly, in determining whether the laws of the EU/EEA "require appropriate safeguards" for data "that is transferred from the United States to the territory of" an EU/EEA country for purposes of section 3(f)(i)(A), it is reasonable to exclude from consideration whether the laws of the EU/EEA require appropriate safeguards for signals intelligence activities not conducted in the territory of the EU/EEA country conducting the activities.

b. Safeguards required in the domestic laws of EU/EEA countries

Individual EU/EEA countries authorize, conduct, and regulate signals intelligence activities under their domestic laws. Such domestic laws are required to be consistent with the ECHR and applicable EU law, which prevail over national law in case of conflict, and are subject to review by the ECtHR and EU courts. The structure and scope of the signals intelligence activities authorized, and the associated privacy safeguards enacted, vary substantially among the thirty EU/EEA countries. As noted above, the ECtHR in 2021 emphasized that it does not "prescribe an ideal model for signals intelligence" but rather reviews each country's intelligence safeguards as a whole, recognizing that "the existing legal and practical arrangements . . . vary conceptually and functionally from one Contracting Party to another." *Centrum För Rättvisa v. Sweden*, § 366.

The following discussion represents limited research conducted by the U.S. government of publicly available statutes, court decisions, and other laws and regulations on signals intelligence activities in representative EU/EEA countries. It does not address restrictions or other protections that may exist in non-public regulations or procedures in EU/EEA countries. The discussion also draws from independent external sources, including in particular three reports published by the EU Fundamental Rights Agency ("EU FRA")[9] on EU Member States' intelligence laws and privacy safeguards. EU FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Update* (2023) ("EU FRA Intel. Rep't Update"); EU FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Volume II: Field Perspectives and Legal Update* (2017) ("EU FRA Intel. Rep't Vol. II"); EU FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Mapping Member States Legal Frameworks* (2015) ("EU FRA Intel. Rep't Vol. I"). The EU FRA assessed in 2017 that "the legal frameworks regulating intelligence work in the EU's [then-]28 Member States remain both extremely diverse and complex." EU FRA Intel. Rep't Vol. II at 9.

i. Legitimate objectives

The ECHR requirement that signals intelligence access to personal data be conducted only for legitimate objectives is implemented by EU/EEA countries in a variety of ways. *See* EU FRA Intel Rep't Vol. I at 24-26. Many EU/EEA countries enumerate in domestic legislation a list of objectives that may justify signals intelligence activity. The EU FRA found that while

[9] The EU Fundamental Rights Agency was established in 2007 to provide EU institutions and agencies "with assistance and expertise relating to fundamental rights," acting with "complete independence." EU Council Regulation 168/2007, O.J. (L 53) 1, arts. 2, 16.

protection of national security was the primary objective identified in EU Member States' intelligence laws, "the concept is not harmonised across EU Member States." EU FRA Intel. Rep't Vol. I at 27.

It appears that some EU/EEA countries' public laws permit signals intelligence activities in pursuit of security objectives stated in general terms such as "internal security," "external security," or the "security of the state." *See id.* The objectives listed in the laws of EU/EEA countries vary in specificity, with some listing such broad objectives, or other broad objectives such as "foreign affairs," or "national defense," along with more specific objectives such as protection against espionage, terrorism, and the proliferation of weapons of mass destruction. *See, e.g.*, *Bekendtgørelse af lov om Forsvarets Efterretningstjeneste* [Defense Intelligence Service Act], *Lovbekendtgørelse nr 1287*, 28 November 2017, §§ 1.1, 3.1 (Denmark) (Defense Intelligence Service authorized to collect information concerning matters abroad to support Denmark's foreign, security and defense policy); *Code de la sécurité intérieure* [French Code on Internal Security] ("FCIS") art. L. 811-3 (France) (authorizing intelligence surveillance for purposes including the national defense, major foreign policy interests, and major economic, industrial and scientific interests, as well as prevention of, among other threats, terrorism, proliferation of weapons of mass destruction, and attacks on the republican form and institutions); *Legge n. 124/2007,* 3 August 2007*, Gazzetta Ufficiale della Repubblica Italiana*, 13 August 2007, n. 187 § 6 (Italy) (authorizing intelligence collection for purposes including the defense of the independence, integrity and security of the Republic as well as counter-proliferation and counter-espionage activities); *Lag om signalspaning i försvarsunderrättelseverksamhet* [Signals Intelligence Act], *Svensk författningssamling* [SFS] 2008:717 § 1 (Sweden) (signals intelligence collection authorized to map out (i) external military threats, (ii) conditions and threats related to peace keeping and humanitarian operations, (iii) international terrorism and other serious cross-border criminal activity, (iv) the development and spread of weapons of mass destruction, war material and dual-use products, (v) severe external threats against community infrastructure, (vi) conflicts in foreign countries that may have consequences for international security, (vii) foreign intelligence operations aimed at Swedish interests, or (viii) foreign powers' acts or intentions of vital importance to Swedish foreign, security or defence politics).

The laws of some EU/EEA countries also include prohibited objectives that may never justify collection—for example, collection that aims at reducing or impeding fundamental rights, collection on the basis of an individual's religion, race, sexual life, or impose additional conditions or procedural requirements for the collection of certain types of data—for example, data on religion, race or health, information subject to professional secrecy, journalistic sources. *See, e.g.*, *Loi organique des services de renseignement et de sécurité (French) / Wet houdende regeling van de inlichtingen- en veiligheidsdienst (Dutch)* [Intelligence Services Act] of November 30, 1998, Moniteur Belge / Belgische Staatsblad, 18 December 1998, p. 40312 arts. 2(1)-(2) (Belgium); *Wet op de inlichtingen- en veiligheidsdiensten 2017* [Intelligence and Security Services Act 2017, or "Wiv 2017"], Stb. 2017 p. 11 § 19(3) and 30(2)-(3) (Netherlands); *Gesetz über den Bundesnachrichtendienst* [Federal Intelligence Service Act], law of 12 December 1990, BGBl. I S. 2954, 2979, last changed 5 July 2021, § 8(5) (Germany).

ii. Requirements for necessity and proportionality and other limitations

It appears that the laws of EU/EEA countries generally require that acquisition of data through signals intelligence activities be undertaken based on principles of necessity and proportionality or other reasonable justifications, in addition to other limiting principles such as prioritizing less intrusive surveillance methods. *See, e.g.*, Intelligence Services Act arts. 2, 18/10, 43/1 (Belgium) (intrusive surveillance techniques subject to principles of subsidiarity and proportionality; collection of the content of electronic communications permitted only when less intrusive measures are insufficient to collect necessary information); Defense Intelligence Service Act § 3a.2 (Denmark) (interference with secrecy of communications of Danish persons may not be conducted if disproportionate to the significance of the case); *Laki sotilastiedustelusta* [Military Intelligence Act], 26 April 2019, Statutes of Finland n. *590/2019* §§ 5-9 (Finland), *and Laki tietoliikennetiedustelusta siviilitiedustelussa* [Civil Intelligence Act], 26 April 2019, Statutes of Finland n. *582/2019* §§ 1, 4 (Finland) (intelligence collection through foreign-focused bulk measures must be necessary to obtain important information on activities that seriously endanger national security, unable to be acquired through other methods, and subject to proportionality requirement); FCIS art. L. 801-1 (France) (authorization for intelligence collection granted only in cases of public interest necessity, within the limits set by the law, and in accordance with the principle of proportionality); Federal Intelligence Service Act § 2(4) (Germany) (intelligence measures may not cause a disadvantage that is recognizably disproportionate to the intended objective); *Decreto Legge 144/2005*, 27 July 2005, *Gazzetta Ufficiale della Repubblica Italiana*, 27 July 2005 n. 173, §§ 4, 4bis (Italy) (intelligence collection activities must be indispensable to be carried out for specified purposes); Wiv 2017 § 29(2) (Netherlands) (intelligence collection must among other things be necessary, proportionate to the intended purpose, the most targeted use of the relevant power, and show reason why less intrusive power is not sufficient); Signals Intelligence Act § 5 (Sweden) (authorization for signals intelligence collection requires, among other criteria, that purpose of gathering the information cannot be fulfilled in a less intrusive way and the expected information gathered is clearly of greater value than the intrusion of privacy that may occur).

iii. EEA countries' foreign-focused domestic intelligence surveillance

A particularly relevant factor for purposes of reviewing, pursuant to section 3(f)(i)(A) of Executive Order 14086, whether the laws of the EU/EEA "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred" from the United States to an EU/EEA country is what safeguards are required under EU/EEA countries' intelligence laws for surveillance targeting foreigners located abroad. A number of EU/EEA countries have established special "foreign-focused" surveillance programs within their territories to monitor and gather electronic communications sent from or received abroad. The privacy safeguards for those foreign-focused intelligence surveillance programs appear to differ from the safeguards applicable to surveillance of domestic communications. Through such a program, an EU/EEA country could acquire electronic communications passing through its territory that are sent from or received by a U.S. person in the United States.

The United States has also established such a program for foreign-focused intelligence surveillance within U.S. territory, through Section 702 of the Foreign Intelligence Surveillance

Act ("FISA"), which authorizes the U.S. government to acquire electronic communications sent or received by non-U.S. persons located outside the United States to obtain foreign intelligence information. While Section 702 safeguards differ from the individualized court approvals required under other sections of FISA for electronic surveillance of persons located in the United States, the Section 702 program operates only on a targeted basis, authorizing the acquisition of the electronic communications of specific persons based on written justifications, with each individual targeting decision and rationale reviewed through independent oversight.[10] Each target must meet specific foreign intelligence criteria and any information can only be collected, analyzed, and disseminated according to procedures adopted by the Attorney General and approved by the independent FISA Court. 50 U.S.C. § 1881a(j)(2)(B)-(D).

The EU Fundamental Rights Agency assessed in 2017 that EU Member States require lesser privacy safeguards for foreign-focused surveillance than for domestic surveillance. "Targeted surveillance—which applies to concrete targets based on some form of individualised suspicion—is regulated in some detail by almost all EU Member States. By contrast, only five Member States currently have detailed legislation on general surveillance of communications. Safeguards do limit the potential for abuse, and these have been strengthened in some Member States—though less so in case of foreign-focused surveillance." EU FRA Intel. Rep't Vol II. at 9. Several such foreign-focused surveillance programs in EU/EEA countries that we have

[10] The court-approved targeting procedures for acquisition of data under Section 702 of FISA require the use of individual "selectors" which refer to communications facilities such as an e-mail address or telephone number used by the specific person who is the target of the acquisition. Selectors cannot consist of general key words such as "bomb" or "attack," or even the names of individuals, because such terms would not identify a specific person's electronic communications facilities. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, at 32-35 (2 July 2014); 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, at 9 (2022), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_NSA_Targeting_Procedures-Amended.pdf ; Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence at 9-13 (September 2021), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/23rd_Joint_Assessment_of_FISA_for_Public_Release.pdf .

identified—including in Belgium,[11] Finland,[12] France,[13] Germany,[14] and Sweden[15]— authorize the collection of electronic communications of persons located outside the country without

[11] It appears that Belgium's General Intelligence and Security Service ("GISS") is authorized to access within Belgium electronic communications sent from or received abroad by foreign organizations or institutions that have been identified by the Minister of Defense, with no independent *ex ante* review or authorization. Intelligence Services Act art. 44 (Belgium). The Minister of Defense may identify a foreign organization or institution as a justified target for this surveillance in connection with the missions assigned by statute to the GISS (except for the mission of carrying out investigations for security clearances). *Id.* art. 44/1. GISS may both conduct such activities outside of Belgium and issue obligatory requests to service providers in Belgium to provide assistance. *Id.* art. 44/5. This foreign-focused surveillance differs from the *ex ante* approval from the independent Administrative Commission that is required for Belgian intelligence agencies to intercept within Belgium electronic communications between two communicants who are located in Belgium. *Id.* arts. 18 /9, 18/10 and 18/17.

[12] In Finland, it appears that the Defense Intelligence Agency is authorized to conduct technical gathering and processing within Finland of telecommunications that have crossed Finland's borders to enable automated acquisition of electronic communications with at least one non-Finnish communicant for the purpose of obtaining information in pursuit of an authorized intelligence objective, based on search terms that need not target specific subjects. Military Intelligence Act §§ 12, 68-71. The surveillance is subject to approval by the District Court of Helsinki that statutory requirements are met, including that search terms are no broader than necessary to obtain the information sought. This foreign-focused surveillance differs from surveillance for national security purposes targeting electronic communications for which both communicants are located in Finland, which must be approved by the District Court of Helsinki as targeting specific subjects, necessary to obtain important information on activities that seriously endanger national security, and seeking information that is not possible to acquire by any other intelligence method. *See Laki Poliisilaki* [Police Act], 22 July 2011, *Statutes of Finland* n. *872/2011* ch. 5a, §§ 3-4. Both types of surveillance are subject to requirements in Finnish law relating to proportionality, purpose limitations, and prohibition on discrimination. Military Intelligence Act §§ 5-9; Police Act, ch. 5a, §§ 3-4.

[13] In France, it appears that intelligence agencies are authorized to access within France electronic communications that are sent from or received abroad under the authority of the Prime Minister or his delegate. FCIS art. L. 854-2, L. 854-9 al 1, L 854-1. For some types of this foreign-focused surveillance, such as the non-individualized use of intercepted connection data, the Prime Minister may authorize the surveillance without obtaining *ex ante* review by the National Commission for the Control of Intelligence Techniques ("NCCIT"). *Id.* art. L. 854-2 II. For other types, such as surveillance targeting individuals or groups of individuals, the Prime Minister must obtain *ex ante* review by the NCCIT, *id.* art. L. 854-2 III, IV and V, and the NCCIT provides a non-binding opinion to the Prime Minister, which if contravened by the Prime Minister may be appealed by the NCCIT to the *Conseil d'Etat* for a binding ruling only if the targeted communications may be traced to a subscription number or technical identifier linked to French territory. *Id.* art. L. 854-2 V. In contrast, French intelligence agencies may conduct domestic surveillance of electronic communications between two persons located in France only after approval is received from the NCCIT or, where the NCCIT does not provide its approval, after receiving the approval of the *Conseil d'Etat*, and subject to additional safeguards such as more narrowly limiting the purposes of surveillance and limiting the availability of intelligence collection techniques. *Id.* arts. L. 801-1, L. 811-3, L. 821-1, L. 833-5, L. 851-853.

[14] In Germany, the Federal Intelligence Service is authorized to conduct two different types of foreign-focused collection of electronic communications, referred to as "strategic monitoring." First, it appears that the G-10 Act authorizes the Federal Intelligence Service to monitor international telecommunications sent in bundled transmission to Germany for purposes of collecting the content and metadata of "one-end-foreign" communications—that is, communications that are neither between two German residents nor exclusively between foreigners abroad. This surveillance requires the *ex ante* approval of the independent G-10 Commission that, among other things, the collection of the data is permissible and necessary to identify and counteract statutorily enumerated threats. *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisse* [Act on Restrictions on the Secrecy of Mail, Post and Telecommunications] ("G-10 Act"), 26 June 2001, BGBl. I S. 1254, 2298, last changed 5 July 2021, §§ 1(1) no. 2, (2), 5(1), 15(6). The collection must be based on search terms that are named in the order approved by the G-10 Commission, the search terms may not contain identifying features that lead to the targeting of specific persons' communications, and the volume of the telecommunications channels monitored is statutorily restricted to 20% of the accessible telecommunications capacity. *Id.* §§ 5(2) no. 1, 10(4).

requiring *ex ante* independent approval based on individualized suspicion or other independent supervision to ensure that the electronic communications of individuals are properly acquired to obtain intelligence information. For example, several (including Finland, Germany, Sweden) authorize collection by using search terms that are not specific to a person but rather are key words on topics of intelligence interest.[16] In some countries (including Belgium and France), senior officials such as the Prime Minister or Minister of Defense can authorize foreign-focused collection without any prior independent review or approval.[17] In contrast, where the countries' own citizens or residents are concerned, these countries generally do require *ex ante* independent approvals or oversight to ensure that the electronic communications of individuals are properly acquired for domestic intelligence surveillance.[18]

---

Separately, it appears that the Federal Intelligence Service Act in Germany authorizes the Federal Intelligence Service to collect the content and metadata of "two-end-foreign" electronic communications—that is, communications between two foreigners located outside of Germany. This surveillance requires the *ex ante* approval of the Independent Control Council that, among other things, the collection of the data is supported by factual indications of statutorily enumerated threats or other purposes. Federal Intelligence Service Act §§ 19, 26, 23. This collection must also be based on search terms, although the search terms do not need to be named in the order that is reviewed by the Independent Control Council. There is no explicit requirement that search terms not be specific to individual persons, although additional restrictions apply to targeting bodies or citizens of the European Union, or surveillance of sensitive data (e.g. data of clergy, lawyers and journalists), and there is a general prohibition on surveillance of a person's entire telecommunications traffic. *Id.* §§ 19(5), 20(3), 23(2), 23(5); *cf. id.* §§ 20 *et seq.* The volume of the telecommunications channels monitored for this collection is statutorily restricted to 30% of the accessible telecommunications capacity. *Id.* § 19(8).

These safeguards for these two types of "strategic monitoring" in Germany differ from German intelligence services' authorization to collect electronic communications between two German citizens or residents, which must always be targeted at specific persons and must be approved *ex ante* by the G-10 Commission based on different standards depending on the type of data–for example, collection of the content of German citizens' electronic communications must be based on factual indications establishing suspicion that the targeted person is planning, committing, or has committed a statutorily enumerated criminal offense. G-10 Act §§ 1(1) no. 1, (2), 3.

[15] In Sweden, it appears that the Defense Radio Establishment (DRE) is authorized for national security purposes to monitor electronic communications that have been transmitted across Sweden's borders for the purposes of collecting communications with at least one non-Swedish communicant. Signals Intelligence Act § 1, 2. 2(a). This collection by DRE in Sweden of foreign communications must be based on search terms which in general may not be associated with specific persons. This surveillance is subject to *ex ante* approval by the independent *Försvarsunderrättelsedomstolen* (Foreign Intelligence Court), which must confirm, among other things, that the information sought cannot be obtained in a less intrusive way, the expected value of the information gathered is of greater value than the intrusion of privacy that may occur due to the collection of the information, the search terms are used in accordance with the statute, and the surveillance will not be aimed solely at a specific person. *Id.* §§ 4(a), 5, 5(a). The DRE may use search terms associated with a specific person only when it is of vital importance to the operation and only for the purpose of tracking the intelligence phenomenon of interest, not for tracking the individual. *Id.* § 3. These standards for foreign-focused surveillance contrast with the standards in Swedish law for the surveillance for national security purposes when the surveillance actively targets the electronic communications of Swedish citizens or residents, in which case it must be approved by the Stockholm District Court based on a showing of a palpable risk that a specific individual will carry out certain criminal activity, such as an act of terrorism or espionage. *Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott* [Act on Measures to Prevent Certain Particularly Serious Crimes] *Svensk författningssamling (SFS)* 2007:979 §§ 1, 6.

[16] *See supra* notes 12, 14, and 15.

[17] *See supra* notes 11 and 13.

[18] *See supra* notes 11-15.

iv. EU/EEA countries' domestic bulk intelligence collection

It appears that a number of EU/EEA countries authorize the collection of signals intelligence data within their territories in bulk—that is, the collection of large amounts of electronic communications without limiting the acquisition to the communications of specific persons by using their communications account identifiers or other discriminating factors. Executive Order 14086 defines "bulk collection" as "the 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)." E.O. 14086 § 4(b).

U.S. law prohibits such bulk data collection domestically for intelligence purposes.[19] Under U.S. law, after personal data has been transferred from an EU/EEA country to a private company in the United States, U.S. intelligence agencies may compel the company to disclose the data for national security purposes only based on statutes authorizing such access, which are limited to the FISA statute, discussed above, and the "national security letter" statutes, such as section 2709 of the Electronic Communications Privacy Act, which authorize administrative requests for information not including the content of communications. Demands under FISA or through national security letters may be issued by U.S. intelligence agencies only on a targeted basis and do not permit bulk collection. *See* Letter from Christopher C. Fonzone, ODNI General Counsel (9 December 2022), annexed to European Commission's draft adequacy decision for the United States, at 3-4 (reviewing statutory prohibitions on bulk collection for the data acquisition authorized in the FISA statute and in the statutes authorizing national security letters).

Several of the special foreign-focused surveillance programs authorized in the EU/EEA countries discussed above (including those in Finland, Germany, and Sweden) inherently involve bulk collection, as that term is defined in Executive Order 14086, because they authorize the use of search terms that are not specific to individuals' electronic communications accounts.[20] The ECtHR, after surveying several bulk surveillance regimes, noted that in those cases, "bulk interception is generally directed at international communications (that is, communications physically travelling across State borders), and while the interception and even examination of communications of persons within the surveilling State might not be excluded, in many cases the stated purpose of bulk interception is to monitor the communications of persons outside the State's territorial jurisdiction, which could not be monitored by other forms of surveillance." *Big Brother Watch v. the United Kingdom*, § 344.

[19] The provisions in Executive Order 14086 governing bulk collection activities pertain not to intelligence access to data that is held by a private company or other entity in the United States, but rather only to other types of signals intelligence activities such as extraterritorial surveillance.

[20] Thus the authorization in Finland for the Defense Intelligence Agency to use automated data processing techniques within Finland to acquire cross-border communications with at least one non-Finnish communicant, both of the "strategic monitoring" authorized in Germany for collection by the Federal Intelligence Service of electronic communications, and the authorization in Sweden for the Defense Radio Establishment to collect within Sweden electronic communications that have been transmitted over cables crossing Sweden's borders, all meet the definition of "bulk collection" in Executive Order 14086. In all of these programs, the relevant EU/EEA country's intelligence agency may acquire electronic communications based on subject matter search terms and not based on communications selectors associated with specific persons, thereby resulting in the collection of data in bulk. *See supra* notes 12, 14, and 15.

Other EU/EEA countries authorize bulk collection of electronic communications within their territories not focused on communications sent from or received abroad. For example, in the Netherlands, it appears that the General Intelligence and Security Service (*Algemene Inlichtingen–en Veiligheidsdienst* or "AIVD") is authorized to collect data through signals intelligence activities in the Netherlands in bulk. This surveillance requires the *ex ante* approval of the independent *Toetsingscommissie Inzet Bevoegdheden* (Dutch Review Committee for the Deployment of Powers, or "TIB"), in three stages of approvals for bulk intelligence collection, with each stage requiring approval by the TIB. Wiv 2017 §§ 32, 48(2), 49(4), 50(2)-(4). The first stage addresses the initial gathering by the AIVD of information in bulk, the second stage addresses the pre-processing and analysis of the information gathered for purposes of optimizing both the interception and future querying and selection, and the third stage addresses the querying and selection of data and automated analysis of metadata. *Id.* §§ 48-50. For all three stages, the AIVD's request for TIB approval must set out, among other things, the reasons why the proposed measure is necessary and proportionate and why the exercise of a less drastic measure is not sufficient to achieve the intended purpose. *Id.* § 29(2).

The laws of some other EU/EEA countries appear to authorize bulk collection through broad authorizations not limited to targeted collection. For example, Danish law authorizes Denmark's Defense Intelligence Service to intercept electronic communications for purposes of obtaining information relating to matters abroad without a court order or other independent *ex ante* approval, and without specifying the method or location for carrying out the interception, resulting in acquisition, including from within Denmark, of electronic communications in bulk. Defense Intelligence Service Act § 3; *Forslag til lov om Forsvarets Efterretningstjeneste* (FE) [Proposal for the Defense Intelligence Service Act] af 27. februar 2013, nr. 163, section 4.1.1 (preparatory note referring to acquisition of several hundred million communications per year). Another example is Italy, where intelligence legislation authorizing the collection of electronic communications, as amended in 2022, appears to permit data acquisition in bulk by not requiring that data acquisition be targeted at specific persons, communications accounts, or other discriminating factors. *Decreto Legge n. 144/2005*, 27 July 2005, *Gazzetta Ufficiale della Repubblica Italiana*, 27 July 2005, n. 173, *as amended by Legge n. 197/2002*, 29 December 2022, *Gazzetta Ufficiale della Repubblica Italiana*, 29 December 2022, n. 303 – *Suppl. Ordinario n. 43*, §§ 4 and 4bis (Italy); *cf.* EU FRA Intel Rep't Vol. II at 42 (making similar conclusion about a prior surveillance law in Italy which authorized intelligence agencies to acquire communications "by electronic means [but] does not provide more details about these surveillance means.").

v. Post-Acquisition Handling of Data

Safeguards in the laws of EU/EEA countries governing post-acquisition handling of data also vary. Regarding retention of data by intelligence agencies, for example, EU/EEA countries generally require that data acquired through signals intelligence be deleted when it is no longer required for the purpose for which it was acquired, but the intervals and maximum periods for reviewing data for deletion vary substantially. *See, e.g.*, Intelligence Services Act art. 21; *Arrêté royal portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (French) / Koninklijk besluit houdende uitvoering van artikel 21*

*van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (Dutch)* [Royal Decree implementing article 21 of the Intelligence and Security Services Act of 30 November 1998], 3 July 2016, Moniteur Belge / Belgische Staatsblad, 3 August 2016, p. 47370 (Belgium) (intelligence information generally reviewed for deletion after fifty years, except recordings of electronic communications must be deleted within five years, or ten years with extension); Defense Intelligence Service Act § 6 (Denmark) (intelligence information regarding a person or entity residing in Denmark to be deleted after fifteen years where no new information has been procured within the last fifteen years in relation to the same case; raw data must be deleted fifteen years after it has been obtained); *Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä* [Act on Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security], 5 December 2018, *Statutes of Finland* n. *1054/2018* § 6.3 (Finland) (necessity of retention to be assessed on five-year intervals); Federal Intelligence Service Act § 27 (Germany) (intelligence information collected on the basis of search terms to be reviewed immediately after collection and then regularly at intervals of no more than seven years); Wiv 2017 § 27(1) (Netherlands) (intelligence information acquired by more intrusive techniques must be assessed for relevance as soon as possible, generally within one year; non-cable-based bulk intelligence information may be retained for three years); Signals Intelligence Act § 7 (Sweden) (information containing personal data must be immediately deleted if not relevant to statutory purposes).

Regarding dissemination of data, it appears that EU/EEA countries also have varying models and conditions for sharing data among intelligence agencies and between intelligence agencies and other public authorities such as law enforcement agencies. But they do generally permit such sharing where necessary, including for law enforcement purposes. *See, e.g.*, Intelligence Services Act arts. 19, 19/1 and 20 (Belgium) (allowing sharing by intelligence agencies of information with judicial and administrative authorities when needed for the performance of their missions; imposing procedural requirements for the sharing of data when it reveals a crime or is relevant for a criminal investigation; also calling for effective mutual cooperation among intelligence, police and judicial authorities, which has been effected in practice through different means such as counter-terrorism fusion centers); Defense Intelligence Service Act § 7.1 (Denmark) (Defense Intelligence Service may share intelligence information with Security and Intelligence Service where important to the performance of the activities of the two intelligence services); *id*. § 7.2-7.4 (other restrictions on disclosure to public authorities apply only to information regarding a person or entity residing in Denmark); Act on Processing of Personal Data by the Police §§ 13, 50 (Finland) (intelligence agencies may disclose data to police units for purposes including prevention or detection of an offense, providing exculpatory evidence, finding of wanted persons, or prevention of a significant danger to life, health, or liberty, or substantial damage to environment or property); FCIS arts. L. 811-3, 822-3 (France) (sharing by intelligence agency of data to another service permitted only for purposes set out in statute; recipient may use the data only where strictly necessary for the performance of its missions; if purposes differ from the purpose that justified the collection or if the recipient service cannot be authorized to use the technique for the purpose the data has been collected, the sharing is subject to the prior authorization of the Prime Minister after an opinion by the National Commission for the Control of Intelligence Techniques); Federal Intelligence Service Act § 11 (Germany) (sharing of intelligence information permitted if necessary for fulfillment of the Federal Intelligence Service's tasks or required for significant purposes of public security by

recipient agency); Wiv 2017 § 3.4.2 (Netherlands) (sharing of data by intelligence agencies subject to conditions, for example limitation on further use by the recipient, with the possibility to share data that is relevant to a criminal investigation with national law enforcement authorities), *Kamerstukken II 2016/17* [Parliamentary Papers II 2016/17], 34588 nr. 3, p 135 (Netherlands) (Explanatory Memorandum to the Wiv 2017 legislation indicating that sharing of intelligence information is generally limited to declassified official messages for lead purposes).

vi. Oversight

Regarding oversight of signals intelligence agencies, the EU FRA found in 2017 that among EU Member States the "oversight of intelligence services is organized in extremely diverse ways" and that "a single model would be an impossible objective because national oversight frameworks have to directly link to the political institutions and administrative and judicial organization of each Member State." EU FRA Intel. Rep't Vol. II at 63. In its 2023 update report, the EU FRA described five different organizational models among EU Member States for the oversight of intelligence agencies. EU FRA Intel. Rep't Update at 36-42.

All EU Member States reportedly involve at least one independent body in the oversight of intelligence activities. EU FRA Intel. Rep't Vol. II at 56. However, the practice with respect to *ex ante* authorization is more varied. The EU FRA found in this respect in 2017 that "[e]x ante authorization or approval by independent overseers is not yet common in EU Member States, but can be seen as a promising practice," and that "just over half of the Member States involve the judiciary (judges or prosecutors) in ex ante oversight, in relation to at least one type of targeted surveillance measure." EU FRA Intel. Rep't Vol. II at 94, 96. In its 2023 update report, the EU FRA found that after legislative reforms in some countries, "[i]n 19 Member States . . . judicial authorities are authorising targeted surveillance measures." EU FRA Intel. Rep't Update at 17.

Many EU/EEA countries with significant signals intelligence capabilities have established independent oversight bodies that are a hybrid of technical experts and government officials to supervise intelligence agencies' legal compliance. *See* EU FRA Intel. Rep't Vol. I at 44-46. These include the *Vast Comité I / Le Comité permanent R* ("Standing Committee I") in Belgium; the *Tilsynet med Efterretningstjenesterne* ("Intelligence Oversight Board") in Denmark; the *Commission Nationale de Contrôle des Techniques de Renseignement* (National Commission for the Control of Intelligence Techniques or "NCCIT") in France; the *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* (Review Committee on the Intelligence and Security, or "CTIVD") in the Netherlands; the G-10 Commission in Germany; and the *Statens inspektion för försvarsunderrättelseverksamheten* (Foreign Intelligence Inspectorate or "SIUN") in Sweden. *See generally* EU FRA Intel. Rep't Update at 27-29 (listing expert bodies overseeing intelligence services in EU Member States). Many of these independent oversight entities, in addition to administering oversight functions, also provide non-judicial redress functions in response to individuals' complaints, as discussed below.

The EU FRA observes that many EU Member States have also recognized the value of having not only external independent oversight but also internal compliance officers. "A number of Member States include such internal controls. Sweden, for example, has established data

representatives in charge of ensuring that personal data is processed lawfully within the signals intelligence agency (the Defence Radio Establishment)." EU FRA Intel. Rep't Vol. I at 30.

It appears that the intelligence oversight bodies in EU/EEA countries generally have access to sensitive national security information held by intelligence agencies necessary to carry out their functions. *See, e.g.*, *Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (French) / Wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse (Dutch)* [Review Act], 18 July 1991, arts. 33, 45, 48, Moniteur Belge / Belgische Staatsblad, 26 July 1991, p. 16576 (Belgium), Intelligence Services Act art. 43/3(1)-(2) (Standing Committee I has full access to intelligence agencies' records); Defense Intelligence Service Act § 17.1 *and* Security and Intelligence Service Act § 20.1 (Denmark) (Intelligence Oversight Board may require the Defense Intelligence Service and the Security and Intelligence Service to provide any information and material that is of importance to its oversight activities); *Laki tiedustelutoiminnan valvonnasta* [Act on Oversight of Intelligence Activities], 18 January 2019, *Statutes of Finland* n. *121/2019* §§ 8 and 10 (Finland) (Intelligence Ombudsman has the right to carry out on-site inspections to access all necessary premises and information systems, and to obtain from government authorities, including intelligence agencies, the information necessary for the performance of the Ombudsman's tasks irrespective of any applicable confidentiality obligations); FCIS art. L. 833-2 (France) (NCCIT has permanent, complete and direct access to intelligence information and may request all the elements necessary for the accomplishment of its missions); G-10 Act § 15 (Germany) (G-10 Commission has access to classified information, records and the premises of the intelligence services); Wiv 2017 § 107(1) (Netherlands) (CTIVD has direct access to all relevant information and systems held by intelligence services; heads of the services must on request provide CTIVD all information and assistance they consider necessary for the proper performance of its task); *Förordning med instruktion för Statens inspektion för försvarsunderrättelseverksamheten* [Instruction for the Swedish Foreign Intelligence Inspectorate] *Svensk författtningssamling [SFS] 2009:969* § 5 (Sweden) (SIUN has unconditional authority to conduct inspections and other investigations of DRE and other intelligence agencies under its supervision, including access to documents, visiting premises, and conducting searches).

It appears that oversight bodies in EU/EEA countries are also generally authorized to initiate investigations of possible violations of domestic laws at their discretion. *See, e.g.*, Intelligence Services Act art. 43/4 (Belgium) (Standing Committee I may initiate an investigation proactively or based on individual complaint); Defense Intelligence Service Act § 15 *and* Security and Intelligence Service Act § 18 (Denmark) (Intelligence Oversight Board may initiate an investigation either proactively or based on individual complaint); FCIS art. L. 833-4 (France) (NCCIT may initiate an investigation proactively or based on individual complaint aiming to verify that no intelligence technique is being improperly used against him or her); Wiv 2017 § 97 (Netherlands) (CTIVD may initiate an investigation proactively or based on individual complaint); Signals Intelligence Act § 10 (Sweden) (SIUN may initiate investigations proactively, on its own prerogative or based on an individual complaint).

It appears that EU/EEA countries' laws vary in terms of whether intelligence oversight bodies have binding authority to order intelligence agencies to take remedial action. *See, e.g.*,

Intelligence Services Act arts. 43/6, 43/8 (Belgium) (Standing Committee I may order the termination of surveillance and deletion of data wrongfully collected); Defense Intelligence Service Act §§ 16.1, 16.3 *and* Security and Intelligence Service Act § 19.1, 19.3 (Denmark) (Intelligence Oversight Board issues non-binding recommendations, which intelligence agency must report to relevant minister where, exceptionally, a recommendation is not followed); Act on Oversight of Intelligence Activities § 15.1 (Finland) (Intelligence Ombudsman may order suspension or termination of intelligence measures); Wiv 2017 § 132(1) *in conjunction with id.* § 12(3) (Netherlands) (CTIVD issues non-binding opinions for investigations undertaken on its own Initiative, but has binding powers when responding to complaints filed by individuals). In some cases where these bodies do not have binding powers, non-compliance with their recommendations can be referred to an independent authority with binding powers. *See, e.g.*, FCIS art. L. 833-8 (France) (NCCIT issues non-binding recommendations; if they are not followed, the chairman or at least three members of the NCCIT may refer the matter to the *Conseil d'Etat* for binding decision); Federal Intelligence Service Act § 52 (Germany) (an administrative control body within the Independent Control Council may complain about activities of the Federal Intelligence Service, which if not remedied by the Federal Intelligence Service may be referred to the Federal Chancellery for a comment period, and then for binding decision to a quasi-judicial control body within the Independent Control Council); Instruction for the Swedish Foreign Intelligence Inspectorate § 15 (Sweden) (SIUN holds no power over intelligence agencies under its supervision and may only notify other authorities for possible investigation of potential claims against the state or a suspected crime).

vii. Individualized redress in EU/EEA countries

The safeguards applicable to individualized redress for complaints alleging violations of the intelligence laws of EU/EEA countries also vary substantially. The EU Fundamental Rights Agency in 2017 found a wide diversity of redress for such complaints, in particular for the scenario discussed above where the individual complainant is not able to demonstrate whether his or her communications were subject to surveillance. "When an individual wishes to complain about interference with his or her right to privacy and data protection by intelligence services, the remedial landscape appears even more complex. The different remedial avenues are often fragmented and compartmentalised, and the powers of remedial bodies curtailed when safeguarding national security is involved." EU FRA Intel. Rep't Vol. II at 59.

Ensuring effective redress requires responding effectively to an individual's complaint while preserving the confidentiality of intelligence operations. As highlighted in the 2022 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, which was signed by the United States, the EU, and twenty-four EU/EEA countries: "redress mechanisms [in OECD countries] take into account the need to preserve confidentiality of national security and law enforcement activities. This may include limitations on the ability to inform individuals whether their data were accessed or whether a violation occurred." OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, pt. VII (2022). The EU Fundamental Rights Agency has likewise recognized the need for limitations: "While the right to seek a remedy is not absent in the context of secret surveillance, it is inherently limited." EU FRA Intel. Rep't Vol. II at 10.

The following discussion of individualized redress provided by EU/EEA countries for complaints alleging violations of intelligence law is divided into two subsections. The first subsection discusses redress for such complaints before the general courts of EU/EEA countries. The second subsection discusses redress before non-judicial bodies. Non-judicial redress may be administered by the same oversight bodies discussed above, by data protection authorities, ombudspersons, or by other independent specialized bodies.

1. Judicial redress

As a general matter, EU/EEA countries have strong and effective rule of law systems, and their judicial systems provide a path for individuals to bring lawsuits and receive a fair hearing when alleging violations of domestic laws.[21] However, where an individual alleges that an EU/EEA country's intelligence agencies have violated the country's domestic laws and the individual is unable to demonstrate his or her data was in fact accessed by an intelligence agency, it appears that—just as in the United States—the individual may face legal and practical obstacles before the general courts of an EU/EEA country due to secrecy requirements. As the EU Fundamental Rights Agency summarized in its 2023 update report, "[r]ecourse to courts may be hindered by strict procedural rules on evidence and legal standing." EU FRA Intel. Rep't Update at 45.

In some EU/EEA countries, it appears that courts will dismiss a complaint before reviewing its merits if the individual complainant is unable to demonstrate that his or her data has been accessed by the EU/EEA country's intelligence agencies. For example, in 2014 and again in 2016, Germany's Federal Administrative Court ruled inadmissible complaints that challenged the lawfulness of the Federal Intelligence Service's "strategic monitoring"—the foreign-focused surveillance programs discussed above in which telecommunications networks in Germany are monitored on the basis of search terms to acquire electronic communications of non-Germans located outside Germany[22]—because the complainants could not demonstrate that they had been personally affected. *Bundesverwaltungsgericht* [Federal Administrative Court], decision of 28 May 2014, reference 6 A 1.13, becklink 1032773; Federal Administrative Court, decision of 14 December 2016, reference 6 A 9.14, becklink 2005238. *See also Højesteret* [Supreme Court], BS-6391/2022-HJR, 11 January 2023 (Denmark) (requiring that plaintiff have *locus standi* (*retlig interesse*) in a case in order to initiate proceedings in a Danish court).

In some EU/EEA countries, such judicial rules on legal standing or the admissibility of complaints may be more lenient, but a complainant alleging violations of intelligence laws who

[21] The Commission's letter, for example, refers to ECtHR decisions not involving the review of an EU/EEA country's intelligence surveillance laws requiring that the country provide due process and fair trial rights for individuals, including in cases arising from challenges to overt government measures based in part on sensitive national security information. *See, e.g.*, *Ozdil and Others v. the Republic of Moldova*, Application no. 42305/18, § 68 (2019) (challenge to extradition); *Regner v. Czech Republic*, §§ 146-52 (2017) (challenge to revocation of security clearance); *Ternovskis v. Latvia*, §§ 67-68 (2014) (challenge to refusal of security clearance); *I.R. and G.T. v. the United Kingdom*, §§ 61 and 63 (2014) (challenge to security-based exclusion from country); *A and Others v. the United Kingdom,* §220 (2009) (challenge to security-based detention); *Jasper v. the United Kingdom*, § 56 (2000) (challenge to fairness of criminal trial); *Chahal v. the United Kingdom*, Application no. 2214/93, § 131 (1996) (challenge to detention and deportation).

[22] *See supra* note 14.

is unable to demonstrate that the government accessed his or her data may face other legal and practical obstacles deriving from state secrecy concerns. The EU FRA observed that "in practice, suits in the general courts are made difficult by intelligence services' claims of secrecy due to national security." EU FRA Intel Rep't Vol. I at 68. Complaints may thus be heard by a court but will likely lose on the merits for lack of proof where the court lacks the authority to compel the government to disclose sensitive national security information. For example, in Dutch civil litigation an intelligence agency may refuse a court order to disclose information based on national security concerns or protection of intelligence sources and methods. *Wetboek van Burgerlijke Rechtsvordering* [Code of Civil Procedure], § 22(1)-(2); *Kamerstukken II 1999/2000* [Parliamentary Papers II 1999/2000], 26855 nr. 3, pp. 54-55; Hoge Raad [Supreme Court of the Netherlands], 29 June 2020, ECLI:NL:HR:2020:1148 ¶ 3.15.2. (Netherlands). Similarly, in a 2000 ruling Sweden's Supreme Administrative Court declined to compel the disclosure of information pertaining to whether Swedish intelligence services had accessed an individual's personal data, in light of the risk of undermining the intelligence services' operations or damaging future operations. *Högsta Förvaltningsdomstolen* [HF] [Supreme Administrative Court], RÅ 2000 ref. 15 Yearbook of the Supreme Administrative Court (2000) (Sweden). *See also Code de la Défense* [Defense Code] arts. L. 2312 *et seq.* (France) (a court may request declassification of a document, which leads to review by and issuance of non-binding opinion from the independent National Defense Confidentiality Committee, but the court may not issue binding order to disclose a document classified as a defense secret); Συμβούλιο της Επικρατείας/*Symvoulio tis Epikratias* [Council of State] 1651/1996 (Greece) (upholding a Deputy Minister's withholding for reasons of state secrets the grounds for rejecting a U.S. citizen's request to extend a residence and work permit); *Codice di procedura penale* [Code of Criminal Procedure], *Decreto del Presidente della Repubblica n. 447*, 22 September 1988, *Gazzetta Ufficiale della Repubblica Italiana*, 24 October 1988, n. 250, Suppl. Ordinario n. 92, § 202(5) (Italy) (where the President of the Council of Ministers has confirmed the existence of state secrets, a judicial authority is prevented from acquiring and using, even indirectly, the information covered by the state secrets).

2. Non-judicial redress

Perhaps as a response to these practical and legal difficulties to individuals obtaining redress for intelligence law violations in the general courts, almost all EU/EEA countries have established non-judicial redress mechanisms. The EU Fundamental Rights Agency found that "[n]on-judicial bodies play an important remedial role in the area of surveillance, given the practical difficulties with accessing general courts." EU FRA Intel. Rep't vol. I at 75. Through these non-judicial redress mechanisms an individual who cannot demonstrate that the EU/EEA country's intelligence agencies accessed his or her data may submit a complaint alleging the intelligence agencies violated domestic laws, triggering a process through which a non-judicial redress entity reviews the lawfulness of any relevant intelligence activities, identifies any violation of law and appropriate remedial action, and issues a response to the individual confirming the completion of the review.

In some countries, for example, a data protection regulatory authority or specialized body will check on behalf of the individual whether the processing of personal data by an intelligence agency was lawful and exercise data protection rights (such as rights of access, correction and deletion). *See, e.g.*, Review Act arts. 51/1, 51/3 (Belgium); Law on the Oversight of Intelligence

Activities § 12 (Finland); State Security and Intelligence Service Act art. 6(1) (Austria). In other systems, complaints from individuals are handled directly by the same intelligence oversight bodies discussed above or other independent specialized bodies. *See, e.g.*, Intelligence Services Act art. 43/4 (Belgium) (Standing Committee I); Defense Intelligence Service Act § 10.1 (Denmark) (Intelligence Oversight Board); FCIS L. 833-4 (France) (NCCIT); Wiv 2017 arts. 114-115 (Netherlands) (CTIVD); Interception of Postal Packets and Telecommunications Messages (Regulation) Act (Ireland) § 9(3) (the Complaints Referee); Signals Intelligence Act § 10(a) (Sweden) (SIUN).

These non-judicial redress mechanisms established in EU/EEA countries are comparable in important respects to the redress mechanism established by Executive Order 14086. For example, the oversight bodies, ombudspersons, data protection authorities, or other entities administering non-judicial redress in EU/EEA countries are generally independent, with their members protected from removal other than for cause, similar to the removal protections required by Executive Order 14086 for judges on the Data Protection Review Court established at 28 C.F.R. § 201. *See, e.g.*, Review Act arts. 28, 30 (Belgium) (members of Standing Committee I are appointed by the Parliament and may only be dismissed by the Parliament for cause); Security and Intelligence Service Act § 17.1, Defense Intelligence Service Act § 14.1 (Denmark) (Intelligence Oversight Board members are appointed by the Minister of Justice following consultation with the Minister of Defense for renewable four-year terms and subject to removal restrictions); FCIS art. L. 831-1 (France) (NCCIT members are drawn from the Parliament, the *Conseil d'Etat* and the courts, appointed by those respective bodies, as well as an individual appointed upon the proposal of another independent regulator, the mandates of which may not be revoked other than by consent or for cause); G-10 Act § 15 (Germany) (members of the G-10 Commission are appointed by a parliamentary committee for the duration of the parliamentary election period and are to act independently and are not bound by instructions); Wiv. 2017 §§ 98-10 (Netherlands) (CTIVD members appointed to six-year renewable terms and protected from removal except for cause).

Additionally, similar to the redress mechanism established by Executive Order 14086, the outcome of such non-judicial redress processes in EU/EEA countries generally leads, due to secrecy requirements, to the complainant being provided only limited information. In some cases, a reasoned decision may be provided in which confidential information is redacted, while for other complaints, such as inquiries about the lawfulness of intelligence activities the very occurrence of which is a classified secret, the response is typically a standardized notification that the necessary verifications were made and any unlawful activity was addressed according to law, without informing the complainant whether his or her information was in fact subject to intelligence activities. *See, e.g.*, Review Act art. 34 (Belgium) (following investigation of individual complaint regarding processing of personal data, Standing Committee I will inform the complainant that "the necessary verifications have been made" and if possible communicate the result to the individual in general terms or with redactions); FCIS art. L. 833-4 (France) (after initial investigation of a complaint the NCCIT shall notify the complainant that the necessary assessment has been carried out, without confirming or denying the implementation of intelligence measures); G-10 Act § 15 (Germany) (upon completion of its examination, the G-10 Commission shall inform the claimant of the results of the investigation, where necessary in general terms to avoid undermining secrecy of intelligence activities); Wiv. 2017 § 124

(Netherlands) (decision of CTIVD on a complaint and grounds therefor are communicated to the claimant only insofar as permitted by state security or other vital interests); Signals Intelligence Act § 10(a), Prop. 2008/09:201 p. 115 (Sweden) (information provided by SIUN to claimant upon completion of review depends on secrecy applicable in the individual case).

In some other ways, however, non-judicial redress mechanisms vary among EU/EEA countries and differ from the redress mechanism established by Executive Order 14086. For example, it appears that EU/EEA countries' non-judicial redress mechanisms generally do not require the appointment of an advocate in each case who is authorized to access the full case record, including sensitive national security information, and is responsible for advocating for the interests of the complainant before the entity reviewing the complaint.

EEA countries' non-judicial redress mechanisms also appear to vary with respect to their access to classified materials necessary to review a complaint. Many have the full access they need. For example, the independent oversight bodies in EU/EEA countries discussed above as having full access to the sensitive national security necessary to carry out their oversight functions have the same access for purposes of providing individualized redress. These include the Standing Committee I in Belgium, the Intelligence Oversight Board in Denmark, the Intelligence Ombudsman in Finland, the NCCIT in France, the G-10 Commission in Germany, the CTIVD in the Netherlands, and the SIUN in Sweden. *See also, e.g.*, *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske* [Act on Security and Intelligence System, *Narodne novine* no. 79/2006, 105/2006, arts. 111(2), 112 (Croatia) (Council for Civil Oversight may inspect reports and other documents of intelligence agencies and conduct interviews with heads and officials of intelligence agencies when necessary to establish facts decisive for assessing the legality of intelligence agencies' activities); Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 N. 125(I)/2018 (Cyprus) (the Cypriot Data Protection Authority can access all the data held by intelligence services); *Lei Quadro do Sistema de Informações da República Portuguesa* [Framework Law of the Intelligence System of the Portuguese Republic] no. 30/84, 5 September 1984, *Diário da República no.º 206/1984, Series I*, 5 September 1984, art. 9(1)(d)-(e) (Portugal) (Intelligence Supervision Council empowered to request any information from the data centres it deems necessary to exercise its powers and to carry out inspection visits, with or without prior notice, on the operations and activities of the intelligence services).

However, some other EU/EEA countries' non-judicial redress mechanisms appear to subject access to classified materials necessary to review individuals' complaints to certain limitations. *See, e.g.*, *Закон за защита на личните данни* [Personal Data Protection Act], *4 January 2002, State Gazette, issue No. 1, with the latest amendments in State Gazette, issue No. 11 of 2 February 2023, in force from 4 May 2023,* art. 12a (Bulgaria) (authorizing a data controller or processor, which may include an intelligence agency, to refuse access by Commission for Personal Data Protection to information covered by an obligation of secrecy); *Nomos (Νόμος) 3115/2003*, *Ephemeris tis Kyverniseos tis Ellinikis Demokratias, Tefchos Proto, Arithmos Fyllou*, 27 February 2003, Series 1, Issue Number 47 (2013) art. 6(1) (Greece) (inspections by Hellenic Authority for Communication Security and Privacy of classified records of National Intelligence Service permitted only if president of the Hellenic Authority is present in person); *Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi*

*CXII. Törvény* [Information Act], Magyar Közlöny*, 26 July 2011,. Vol. 88, p. 25449*, § 71(3); *Az alapvető jogok biztosáról szóló 2011. évi CXI. Törvény* [Fundamental Rights Commissioner Act] Magyar Közlöny, 26 July 2011, vol. 88, p. 25435] § 23(2) (Hungary) (restricting the Hungarian National Authority for Data Protection and Freedom of Information from accessing specified categories of documents relating to the activities of Hungarian intelligence agencies); *Codice in materia di protezione dei dati personali* [Data Protection Code], *Decreto Legislativo 30 Giugno 2003*, Gazzetta Ufficiale della Repubblica Italiana, 29 July 2003, n. 174, Suppl. Ordinario n. 123, § 160 (Italy) (restricting investigation of allegations of intelligence law violations and related access to information protected by state secrets to a single designated member of the Data Protection Authority).

Additionally, EU/EEA countries' non-judicial redress mechanisms vary with respect to their binding authority to order remediation of violations of intelligence laws. In total, the EU FRA reported in 2017 that "[i]n 18 Member States, remedial bodies – mainly expert bodies and DPAs – may issue binding decisions on complaints relating to surveillance." EU FRA Intel Rep't Vol. II at 114; *see also* EU FRA Intel. Rep't Update at 51 ("In 2023, the situation remained largely unchanged regarding the remedial powers of non-judicial oversight bodies . . . ."). For example, some of EU/EEA countries, including some that authorize special foreign-focused intelligence surveillance or bulk collection programs as noted above, appear to have non-judicial redress mechanisms with binding authority that are fully available to U.S. persons in the United States. *See, e.g.*, Intelligence Services Act art. 16 (Belgium) (decisions of Standing Committee I are legally binding in response to individual complaints concerning more intrusive surveillance methods); Act on the Oversight of Intelligence Activities § 15 (Finland) (Intelligence Ombudsman has effective powers to issue remedial orders to intelligence agencies in response to individual complaints); *Nomos (Νόμος) 3115/2003*, *Ephemeris tis Kyverniseos tis Ellinikis Demokratias, Tefchos Proto, Arithmos Fyllou*, 27 February 2003, Series 1, Issue Number 47 (2013) arts. 6(4), 11 (Greece) (decisions of Hellenic Authority for Communication Security and Privacy are binding and enforceable including through imposition of fines); Data Protection Code § 160(2), Legislative Decree 51/2018 § 37(3) (Italy) (Data Protection Authority may issue binding compliance orders specifying to the Italian intelligence agencies necessary modifications data processing activities and may verify implementation); Wiv 2017 § 124 (Netherlands) (CTIVD authorized to make decisions in response to individual complaints ordering remedial measures legally binding on intelligence agencies).

In a number of other EU/EEA countries, however, it appears that any authority held by non-judicial redress mechanisms is advisory, or may only lead to reports of non-compliance to the government or other authorities. *See, e.g.*, Act on Security and Intelligence System art. 113(1)-(3) (Croatia) (Council for Civil Oversight not authorized to issue binding decisions but instead may only report findings of unlawful activity by intelligence agencies to the parliament, president, prime minister, and state attorney); Security and Intelligence Service Act § 19.1, Defense Intelligence Service Act § 16.1 (Denmark) (Intelligence Oversight Board lacks authority when responding to individuals' complaints to order the Danish intelligence services to implement specific remedial measures but may issue statements providing its opinion on matters such as whether the services comply with the intelligence service laws); *Ustawa o Rzeczniku Praw Obywatelskich* [Act on the Ombudsperson], 15 July 1987, arts. 15-17 (Poland) (intelligence agency to which Ombudsperson provides assessments or request must respond with

explanations within 30 days of the action taken or position adopted); Framework Law of the Intelligence System of the Portuguese Republic art. 9(1)(k) (Portugal) (Intelligence Supervision Council when responding to individuals' complaints about intelligence agencies does not issue binding decisions but may propose remedial measures to the government); *Legea nr. 35/1997 privind organizarea şi funcţionarea instituţiei Avocatul Poporului cu modificări ulterioare* [Law no. 35/1997 on the organization and functioning of the Ombudsman with subsequent amendments], as republished in the Official Gazette no. 181/27 February 2018, arts. 26-28 (Romania) (Ombudsperson when responding to individuals' complaints about intelligence agencies does not issue binding decisions but instead is authorized to recommend remedial measures, non-compliance with which may be notified by the Ombudsperson to the government and the parliament); *Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo* [Organic Law 3/1981 of 6 April on the Ombudsman], *Boletín Oficial de Estado*, 7 May 1981, núm. 109, art. 28(1)-(3) (Spain) (Ombudsman when reviewing individuals' complaints alleging intelligence law violations may propose remedial measures to the government).

Moreover, some EU/EEA countries' non-judicial redress mechanisms have binding authority but appear not to be fully available to U.S. persons seeking redress with respect to their communications sent to or from the United States. In France, for example, individuals may appeal non-binding recommendations of the NCCIT to the *Conseil d'Etat* for binding redress only for complaints concerning (i) domestic surveillance or (ii) surveillance of communications sent from or received abroad for which the communications identifiers can be linked to French territory. FCIS arts. L. 833-4, L. 833-6, L. 841-1, L. 854-1, L. 854-2 V, L. 854-9; *Conseil d'Etat*, Oct. 19, 2016, n° 397623; *Conseil d'Etat*, June 20, 2018, n° 404012, 404013; CAJ R. 773-7, R. 773-34-1 and R. 773-34-2. (However, if the Prime Minister does not comply with an NCCIT recommendation, the chairman or at least three members of the NCCIT may themselves appeal to the *Conseil d'Etat* for binding redress. FCIS arts. L. 854-9; CAJ R. 773-34-1.) Similarly in Germany, a U.S. person alleging violations of law concerning "strategic monitoring" of his or her electronic communications by the Federal Intelligence Service may invoke the binding redress of the G-10 Commission only for "strategic monitoring" authorized by the G-10 Act, which authorizes the acquisition of "one-end-foreign" electronic communications. G-10 Act §§ 5, 15(5). There is no similar binding redress mechanism in German law for complaints about the "strategic monitoring" by the Federal Intelligence Service of a U.S. person's "two-end-foreign" communications authorized by the Federal Intelligence Service Act.[23]

Furthermore, regardless of the type of communications monitoring at issue, in some EU/EEA countries non-judicial redress mechanisms appear not to be available by their terms to U.S. persons located in the United States submitting complaints alleging violations of intelligence laws. For example, in Denmark, only a person or entity residing in Denmark, and not a non-Danish citizen living abroad such as a U.S. person living in the United States, may request the Danish Intelligence Oversight Board to investigate whether the Danish Defense Intelligence Service unlawfully processed information regarding the person in question. Defense Intelligence Service Act § 10.1 (Denmark). As another example, the Estonian Data Protection Inspectorate may provide redress in response to individual complaints concerning the conduct of Estonian intelligence agencies only if the relevant intelligence activities were conducted within

[23] These two authorizations for "strategic monitoring" under German law are discussed *supra* at note 14.

the context of criminal proceedings. *Isikuandmete kaitse seadus* [Personal Data Protection Act] RT I 04.01.2019, 11; 31.10.2013, § 56(1) (Estonia).

Notwithstanding this diversity among the safeguards accompanying non-judicial redress mechanisms in EU/EEA countries for intelligence law violations, we are not aware of any specific cases in which a U.S. person has sought, but was unable to obtain, effective redress before a non-judicial redress mechanism in an EU/EEA country for a complaint alleging violations of intelligence laws. Moreover, we are not aware of cases in which a U.S. person has sought, but was unable to obtain, access to other redress mechanisms that exist, as discussed above, including judicial redress. We welcome further dialogue with EU/EEA countries to ensure that we have an accurate understanding of how redress for complaints alleging intelligence law violations is provided in practice.

viii. Applicability of EU/EEA countries' domestic safeguards to extra-territorial signals intelligence activities

EEA countries generally do not appear to have adopted detailed privacy safeguards that are globally applicable to all signals intelligence activities, as the United States has done in Executive Order 14086. Rather, EU/EEA countries' publicly available laws provide detailed safeguards only for the domestic signals intelligence activities of their intelligence agencies, within their own territory. At the same time, for the reasons discussed above with respect to the ECHR and EU law, it is reasonable to exclude from consideration in the assessment required under section 3(f)(i)(A) of the Executive Order whether the domestic laws of EU/EEA countries require appropriate safeguards for signals intelligence activities conducted outside of their boundaries. Accordingly, the focus of the above analysis of privacy safeguards in the laws of representative EU/EEA countries was on signals intelligence activities conducted within the territory of each country.

c. Assessment

The Attorney General must determine for purposes of section 3(f)(i)(A) of Executive Order 14086, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, whether the laws of the EU/EEA "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory" of a EU/EEA country. As discussed above, section 3(f)(i)(A) does not require that the laws of the EU/EEA afford identical or reciprocal safeguards to those afforded by the United States. Rather, the required safeguards must be "appropriate." The legal requirements imposed by the ECHR on all EU/EEA countries, including all EU Member States as well as Iceland, Liechtenstein, and Norway, provide a sufficient basis for this determination. Moreover, given the importance of commercial transfers of data between Europe and the United States, and the clear commitment of EU/EEA countries to privacy with respect to national security activities, as well as the specific assurances that the Attorney General has been given by Commissioner Reynders concerning privacy safeguards required by European law in the letter attached to this memorandum, it is reasonable to conclude that the laws of the EU/EEA require appropriate safeguards.

The divergence in the signals intelligence privacy safeguards provided among EU/EEA countries in their domestic laws may be reasonably accommodated under the section 3(f)(i)(A) standard, based on a number of factors. Most importantly, notwithstanding certain disparities between European and U.S. law, EU/EEA countries' commitment to privacy in this area when considered as a whole is clear, as reflected in the requirements of the ECHR to which they are all parties. Those privacy safeguards are generally consistent with the common privacy safeguards recognized by the United States, twenty-four EU/EEA countries, and the EU in the recent OECD Declaration on Government Access to Data Held by Private Sector Entities. Additionally, the United States in other contexts related to cross-border data transfers has adopted a deferential approach towards assessing foreign laws on government access to personal data for law enforcement and national security purposes. For example, the authorization in the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) to conclude agreements with foreign countries to facilitate improved cross-border access to personal data to counter serious crime does not require that the foreign country match the same privacy safeguards and standards set out in U.S. law, but rather that the foreign country's laws, viewed holistically, provide safeguards that are appropriate for a rights-respecting democratic society that follows the rule of law. *See* 28 U.S.C. § 2523(b). This deferential approach aligns with the ECtHR's approach of reviewing each country's intelligence laws and safeguards holistically and not substituting its own policy views for those of national authorities. *See Centrum För Rättvisa v. Sweden*, § 366; *Klass and Others v. Germany*, § 49. Moreover, many of the laws and practices of EU/EEA countries described above have not yet been challenged before or reviewed by European courts. In the event they are, European courts may further develop the standards required by the ECHR and require enhanced safeguards to be implemented by EU/EEA countries.

Given the complexity and variety of national legal systems in the area of national security, we would welcome the establishment of an ongoing dialogue between the European Commission, the EU/EEA countries, and the United States going forward to ensure an accurate understanding of each other's systems of privacy safeguards. A two-way dialogue to better understand the safeguards in U.S. law and the laws of the EU/EEA will help to build trust among our fellow democracies regarding government access to personal data. A strong mutual understanding of our countries' commonalities and differences in this area is important to strengthen the basis on which companies can transfer personal data with confidence that privacy is appropriately protected.

## III. Determination that the EU/EEA permits, or is anticipated to permit, commercial data transfers to the United States

The second determination to be made to designate the EU/EEA, pursuant to section 3(f)(i)(B) of Executive Order 14086, is that the EU/EEA and its member countries permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of EU/EEA countries and the territory of the United States.

On July 16, 2020, the CJEU issued its judgment in the "*Schrems II*" case. Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559 (2020). That judgment invalidated the adequacy decision issued by the European Commission in 2016 which concluded that the United States provides safeguards for government access to data,

including signals intelligence activities, that are "essentially equivalent" to safeguards afforded in the EU. With respect to the possibility of relying on other transfer instruments under EU law (in particular Standard Contractual Clauses), pending regulatory investigations and related proceedings in EU Member States have been addressing the impact of the *Schrems II* judgment, in particular how it affects the obligation of EU/EEA data exporters to evaluate whether U.S. law provides privacy protections essentially equivalent to those afforded in the EU/EEA. Accordingly, the *Schrems II* judgment is sufficient to place in doubt whether the EU/EEA and its member countries currently meet the requirement of section 3(f)(i)(B) of Executive Order 14086.

The strengthened safeguards for signals intelligence activities in Executive Order 14086 were designed to address the concerns of the CJEU as set out in the *Schrems II* decision. Based on those strengthened safeguards, the European Commission in December 2022 issued publicly a draft adequacy decision for the EU-U.S. Data Privacy Framework. The Commission is working towards finalization of the adequacy decision, which will permit the transfer of personal information for commercial purposes in reliance on the EU-U.S. Data Privacy Framework between the territory of EU/EEA countries and the territory of the United States. An essential step for the finalization of the adequacy decision is that the Attorney General designate the EU and the three additional EEA countries Iceland, Liechtenstein, and Norway as qualifying states to make the redress mechanism established by the Executive Order available to EU/EEA individuals.

Section 3(f)(i) of Executive Order 14086 authorizes designation either "effective immediately or on a date specified by the Attorney General . . . ." Further, section 3(f)(i)(B) authorizes designation if the regional economic integration organization or its member countries "permit, *or are anticipated to permit*, the transfer of personal information for commercial purposes . . . ." (emphasis added). As noted above, based on the reforms to U.S. law set forth in Executive Order 14086, the European Commission is anticipated to issue an adequacy decision for the United States. There is accordingly a sufficient basis, in light of the standard in section 3(f)(i)(B), to make a designation of the EU/EEA that is contingent on, and which will come into effect as of the date of, the adoption of an adequacy decision for the EU-U.S. Data Privacy Framework by the European Commission.

## IV. Determination that designation of the EU/EEA would advance U.S. national interests

The third determination to be made to designate the EU/EEA, pursuant to section 3(f)(i)(C) of Executive Order 14086, is that the designation would advance the national interests of the United States. Designating the EU and Iceland, Liechtenstein, and Norway is an essential step in bringing into place the EU-U.S. Data Privacy Framework, which will provide vital benefits to citizens and businesses on both sides of the Atlantic. The EU-U.S. Data Privacy Framework will enable the continued flow of data that underpins the seven-trillion-dollar U.S.-EU economic relationship and will enable businesses of all sizes to compete in each other's markets. There are accordingly sufficient grounds to conclude that it is in the national interest to designate the EU and Iceland, Liechtenstein, and Norway as qualifying states.

**DIDIER REYNDERS**
MEMBER OF THE EUROPEAN COMMISSION
JUSTICE

Rue de la Loi, 200 B-1049 Brussels
Phone: +32-2 295 09 00
Didier.Reynders@ec.europa.eu

Brussels,
Ares(2023) 6488529 s

Dear Attorney General Garland and Secretary Raimondo,

Further to your request in the context of our joint work to develop the EU - U.S. Data Privacy Framework, please find below information on the common limitations and safeguards applicable to government access to data for national security purposes across the European Union (EU) and the European Economic Area (EEA). The common requirements described below apply regardless of the nationality or place of residence of concerned individuals and are therefore also applicable to the data of U.S. persons transferred to the territory of the EU. While they are implemented in various ways in different national systems, they are comparable to the limitations and safeguards that were the subject of the negotiations between the European Commission and the United States' Government that led to the development of the new EU-U.S. Data Privacy Framework. Therefore, I believe that this information provides a strong basis to inform your determination under section 3(f)(i)(A) of Executive Order 14086 that appropriate safeguards apply in this area in the EU/EEA.

In case of relevant developments in the future that would concern the legal requirements described in this letter, a dialogue on such developments may take place in the context of the periodic reviews of the functioning of the EU-U.S. Data Privacy Framework. In addition, we may consider suggesting to the bodies responsible for the oversight of intelligence services in the US and the EEA to complement this dialogue with exchanges on relevant developments in this area, in the margins of the periodic reviews.

In the EU, government access to data for national security purposes is framed by common principles. These requirements derive in particular from adherence to the European Convention on Human Rights (ECHR), which is a precondition for accession to the EU. The ECHR is subject to the binding interpretation by the European Court for Human Rights (ECtHR) and, through their ECHR membership, all EU countries are subject to the jurisdiction of the ECtHR. Over the course of more than four decades, the ECtHR has developed a rich body of case law on the balance between privacy and national security from which the requirements described below derive.

Merrick B. Garland
Attorney General
United States of America

Gina M. Raimondo
Secretary of Commerce
United States of America

This case law has led to changes in the legal frameworks of EU countries on several occasions[1]. The same requirements apply to the three non-EU member states of the European Economic Area (EEA) – Iceland, Liechtenstein and Norway – which are all parties to the ECHR and are subject to the jurisdiction of the ECtHR.

Furthermore, fundamental rights enshrined in the ECHR, including the right to the protection of privacy, constitute general principles of EU law[2]. As an integral part of the EU Treaties, such general principles have, as clarified by the Court of Justice of the European Union (CJEU), "constitutional status"[3], with primacy over national law. In addition, these principles are particularly important as a rule of interpretation and cannot be subject to a restrictive interpretation by national courts[4]. Moreover, according to Article 52(3) of the Charter of Fundamental Rights of the European Union – which has the same legal status as the EU Treaties – the rights of the Charter that correspond to those under the ECHR must have the same meaning and scope as the ECHR, unless EU law provides more extensive protections. In other words, corresponding rights of the ECHR are considered the "minimum threshold of protection"[5]. This also applies when fundamental rights, including the right to privacy, are balanced against a competing right or public interest such as a government's interest in protecting national security.

The CJEU has also developed case law on interferences with the right to privacy and data protection in the area of national security, which is referenced below where relevant and applicable.

In addition, the principles mentioned in this letter are reflected in the Constitutional law of the EU Member States and are applied by their courts[6].

As a starting point, any interference by a public authority with an individual's right to privacy, including government access for national security purposes, must be provided for by law[7]. This not only requires that a surveillance measure has a basis in domestic law, but also refers to the quality of the law, which should be accessible to the public and foreseeable as to its consequences[8]. The law must be sufficiently clear to give individuals an adequate indication as to the circumstances in which, and the conditions under which, public authorities are empowered to resort to surveillance[9]. In particular, it must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons

---

1 See e.g. the legislative amendments in Bulgaria after the ECtHR judgment in Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application no. 62540/00; in Sweden after the ECtHR judgment in Centrum för rättvisa v. Sweden, Application no. 35252/08; and in Romania after the ECtHR judgment in Bucur and Toma v. Romania, Application no. 40238/02.

2 Article 6(3) of the Treaty on the European Union.

3 See e.g. CJEU, C-101/08, Audiolux, ECLI:EU:C:2009:626, § 63.

4 See e.g. CJEU C-174/16, Land Berlin, ECLI:EU:C:2017:637, § 44.

5 CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others ('La Quadrature du Net'), ECLI:EU:C:2020:791, § 124.

6 See e.g. the judgment of the German Federal Constitutional Court of 19 May 2020, 1 BvR 2835/17 that specifically concern the balance between the right to privacy and national security.

7 Article 8(2) ECHR and Article 52(1) Charter of Fundamental Rights of the EU; See e.g., CJEU, La Quadrature du Net, §175 in which the Court stated, "that any limitation on the exercise of fundamental rights must be provided for by law", which "implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned".

8 As regards the notions "prescribed by law" and "in accordance with the law" in Articles 8 to 11 of the Convention, the ECtHR has highlighted, that this not only presupposes that the measure interfering with these rights must have a legal basis in domestic law, but also refers to the quality of the law (see ECtHR, Herri Batasuna and Batusuna v. Spain, Application no. 25803/04, § 56). See also ECtHR, Amann v. Switzerland, Application no. 27798/95, § 50; Kennedy v. United Kingdom, Application no. 26839/05, § 151; Malone v. United Kingdom, Application no. 8691/79, §§ 66 et seq.

9 ECtHR, Malone v. United Kingdom, § 67; see also CJEU, La Quadrature du Net, § 132 in which the Court stated, that the legislation must indicate in what circumstances and under which conditions a measure providing for the processing of personal data may be adopted.

whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse[10]. Moreover, the law must indicate with sufficient clarity the scope of any discretion conferred on competent authorities and how it may be exercised[11].

Specifically, the legal basis for surveillance must, inter alia, set out the factual grounds justifying surveillance, a specification of the categories of individuals liable to be subject to surveillance, a limit on the duration of the surveillance, as well as a description of the safeguards applied to the processing of data, including the procedure to be followed for examining, storing and using the data, the precautions to be taken for data sharing with third parties, and the circumstances in which data may or must be erased or destroyed[12]. These principles apply in the same way to rules governing measures targeted at specific individuals (e.g. interception of communications) and more general surveillance programs[13].

With regard to bulk collection/interception, in addition to the elements described above, the legal basis must, set out the procedures and modalities for supervision by an independent authority of compliance with all the safeguards and its powers to address non-compliance, the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance. Moreover, regarding the sharing of information gathered through signals intelligence with foreign intelligence agencies, the law must clearly set out the circumstances in which such a transfer may take place[14].

Second, government access for national security purposes must comply with the principles of necessity and proportionality.

In particular, any surveillance measure must pursue a legitimate aim (e.g. protecting national security)[15]. In this respect, the ECtHR has, for instance, recognised espionage, terrorism, activities threatening the free democratic constitutional order, the security of (allied) armed forces and activities which are intended to undermine or overthrow Parliamentary democracy as constituting threats to national security[16]. Similarly, the CJEU has indicated that the protection of national security encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself (e.g. terrorist activities)[17]. This is reflected in various ways in the laws of EEA countries that include in the protection of national security objectives such as protection against espionage; terrorism; violent extremism; the proliferation of weapons of mass destructions; and activities that threaten the national integrity, sovereignty, or constitutional order. By contrast, objectives that may never justify collection include, for example, collection that aims at reducing or impeding fundamental rights; collection on the basis of an individual's religion, race, sexual life; and collection with the aim of achieving competitive advantages (economic espionage). Furthermore, certain types of data (e.g. data on religion, race, health; information subject to professional secrecy; journalistic sources) may,

---

10 CJEU, C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others ('Privacy International'), ECLI:EU:C:2020:790, § 68; La Quadrature du Net, § 132.

11 See e.g. ECtHR, Roman Zakharov v. Russia, Application no. 47143/06, § 230; Weber and Saravia v. Germany, Application no. 54934/00, § 94.

12 ECtHR, Weber and Saravia v. Germany, § 95; Big Brother Watch and Others v. the United Kingdom, Application nos. 58170/13, 62322/14 and 24969/15, §274.

13 ECtHR, Liberty and Others v. United Kingdom, Application no. 58243/00, § 63.

14 ECthR Big Brother Watch and Others v. the United Kingdom, § 361.

15 ECtHR, S. and Marper v. the United Kingdom, Applications nos. 30562/04 and 30566/04, § 101. See also ECtHR, Segerstedt-Wiberg and others v. Sweden, Application no. 62332/00, § 88, and, as regards EU law, CJEU, La Quadrature du Net, §§ 130-131.

16 ECtHR, Klass and Others v. Germany, Application no. 5029/71, §§ 46, 48; Kennedy v. United Kingdom, § 159.

17 CJEU, La Quadrature du Net, § 135. See also e.g. CJEU, C-439/19, B. v. Latvia, ECLI:EU:C:2021:504, § 67 referring to activities that are "intended to protect essential State functions and the fundamental interests of society".

in principle, not be collected by intelligence agencies, except under strict conditions and subject to additional procedural requirements.

A surveillance measure must be necessary and proportionate to achieve such legitimate aims. In this respect, it follows from EU law that any limitation on the right to privacy must be necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others[18]. In addition, the importance of the public interest objective pursued must be proportionate to the seriousness of the limitation to the rights of the individual[19]. Similarly, the ECtHR has interpreted the requirement of the ECHR that any interference with a fundamental right must be "necessary in a democratic society" as being fulfilled when it answers a "pressing social need", is proportionate to the legitimate aim pursued and the reasons provided by the public authorities to justify it are "relevant and sufficient"[20]. Moreover, according to the principle of proportionality, the interest of the State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his/her private life[21].

These principles are reflected in relevant national legal frameworks through different requirements, such as the requirement to choose surveillance measures/methods in function of the seriousness of a (potential) threat; to use the least intrusive measure and only resort to the use of more intrusive powers when the objective pursued cannot be met by less intrusive measures; and to take into account different factors to assess the proportionality of specific measures, including the purpose of the measure, the impact on concerned individuals and the seriousness of the threat.

Furthermore, in accordance with the case law of the ECtHR, there must be adequate and effective safeguards against abuse, taking into account factors such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided to individuals[22]. Moreover, minimum safeguards must be in place concerning, inter alia, the examination, storage, destruction, use and sharing of data, access to data by third parties and procedures for preserving the integrity and confidentiality of data[23]. In addition, the intercepting agencies must keep records of interceptions, to ensure that the supervisory bodies have effective access to details of surveillance activities undertaken[24].

While bulk collection/interception is not prohibited per se, it may only be carried out subject to specific "end-to-end safeguards"[25]. In particular, an assessment has to be made at each stage of the process of the necessity and proportionality of the measures being taken, the collection should be subject to independent authorisation at the outset, and the operation subject to supervision and

---

18 See e.g. CJEU, La Quadrature du Net, § 130.

19 CJEU, La Quadrature du Net, § 131. This follows from the general principle that "an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue" (La Quadrature du Net, § 130).

20 ECtHR, Leander v. Sweden, Application no. 9248/81, § 58; S. and Marper v. the United Kingdom, § 101. See also, as regards necessity, ECtHR, Szabó and Vissy v. Hungary, Application no. 37138/14, § 73; CJEU, La Quadrature du Net, §§ 133, 137-139, 180-182, 188-189; Case C-203/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, ECLI:EU:C:2016:970, § 119. See also ECtHR, Sidiropoulos and Others v Greece, Application no. 26695/95, §§ 40-41 and ECtHR, Herri Batasuna and Batusuna v. Spain, Application no. 25803/04, §§75,83.

21 ECtHR, Leander v. Sweden, § 59; CJEU, Privacy International, § 67; La Quadrature du Net, §§ 121 and 131.

22 ECtHR, Roman Zakharov v. Russia, § 232; Kennedy v. United Kingdom, § 153; Klass and Others v. Germany, § 50; Weber and Saravia v. Germany, § 106.

23 ECtHR, S. and Marper v. the United Kingdom, §§ 99, 103; Kennedy v. United Kingdom, § 162; Liberty v. United Kingdom, § 69.

24 ECtHR, Roman Zakharov v. Russia, § 272; as regards bulk collection see EctHR Big Brother Watch and Others v. the United Kingdom, §356

25 ECtHR, Centrum för rättvisa v. Sweden, Application no. 35252/08, § 264; Big Brother Watch and Others v. the United Kingdom, § 350.

independent ex post facto review[26]. Conversely, access to data on a generalised and indiscriminate basis ("mass surveillance"), without limitations and safeguards, is unlawful[27]. In addition, specific safeguards must apply to the use of data collected in bulk. For example, to share data collected in bulk with foreign intelligence services, it must be ensured that the receiving State has safeguards in place to prevent abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. In addition, the transfer of data to foreign intelligence service should be subject to independent control[28].

Third, any government access for national security purposes must be subject to independent oversight, normally by the judiciary[29] and, in any event, by an authority that is independent from the executive[30] and vested with sufficient powers to exercise effective and continuous control[31]. In principle, there should be prior authorisation of surveillance measures or, in the absence thereof (e.g. in cases of urgency), effective "post factum" oversight and review[32].

There is some diversity in the way relevant oversight systems are structured at national level. Competent supervisory bodies in this area include a range of actors such as judicial bodies, data protection authorities, independent specialised bodies and parliamentary committees. These bodies fulfil often complementary (and mutually reinforcing) oversight functions. They are vested with different powers, such as authorising surveillance measures, conducting investigations on the basis of complaints or on their own initiative (and, in that context, accessing relevant information), adjudicating complaints lodged by individuals and ordering remedial measures, providing advice to governmental authorities on draft legislation and issuing recommendations on the implementation of relevant legal rules and policies.

Fourth, effective redress must be available to anyone who suspects that their data has been accessed, including the possibility to obtain access to, or rectification or erasure of the data[33]. In particular, a person affected by measures taken for national security reasons, such as surveillance measures, must be able to have the measure in question reviewed by an independent[34] and impartial

---

[26] See e.g., ECtHR, Big Brother Watch and Others v. the United Kingdom, § 356, "Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society".

[27] CJEU, C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, § 94.

[28] ECtHR, Big Brother Watch and Others v. the United Kingdom, § 362.

[29] ECtHR, Klass and Others v. Germany, § 55.

[30] ECtHR, Szabó and Vissy v. Hungary, § 77 and the case law cited. As regards the criteria for independence, the ECtHR has highlighted, among others, "the manner of appointment and the legal status of the members of the supervisory body" (Roman Zakharov v. Russia, § 278), the absence of conflicts of interest (id. § 280), the powers of the supervisory body, both in terms of "access to all relevant documents, including closed materials" (id. § 281) and remedial powers (id. § 282), and that its "activities are open to public scrutiny" (id. § 283).

[31] ECtHR, Klass and Others v. Germany, § 56. As regards the remedial power, the ECtHR has highlighted, among others, the power to "stop or remedy the detected breaches of law", to hold those responsible accountable and to destroy unlawfully obtained intercept material (see ECtHR, Roman Zakharov v. Russia, § 282 and the case law cited). With respect to investigatory powers, the ECtHR has emphasised "that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required" (see id. §281 and the case law cited).

[32] ECtHR, Szabó and Vissy v. Hungary, §§ 77, 81; Big Brother Watch and others v. United Kingdom, § 350. See also CJEU, La Quadrature du Net, § 189.

[33] Article 13 ECHR and Article 47 Charter of Fundamental Rights of the EU. See also ECtHR, Klass and Others v. Germany, §§ 55-56; CJEU, La Quadrature du Net, § 190.

[34] Regarding independence, the ECtHR has held that the following criteria must be taken into account: (i) the manner of appointment of its members, (ii) the duration of their term of office, (iii) the existence of guarantees against outside pressures; (iv) whether the body presents an appearance of independence (see Kleyn and Others v. the Netherlands, Applicationsnos. 39343/98, 39651/98, 43147/98 and 46664/99, § 190; Langborger v. Sweden, Application no. 11179/84, § 32).

body empowered to examine all the relevant questions of fact and law, in order to determine the lawfulness of the measure and censure a possible abuse by the authorities[35].

Individuals should, especially when they are not notified of surveillance measures, have the possibility to obtain review by a court, without having to demonstrate that their data was in fact accessed[36]. Regarding notification, the ECtHR and CJEU have stressed that it must take place as soon as it no longer jeopardises the purpose of the measures taken by the competent authorities, to enable the persons affected to exercise their rights as well as to avail themselves of an effective remedy before a tribunal[37].

To ensure due process before a national court, the parties must have the right to inspect, and comment on, the evidence and observations made to the court[38]. While there may be restrictions on the right to an adversarial procedure, those must be strictly necessary in the light of a strong countervailing public interest such as national security[39]. Such restrictions may include withholding confidential evidence from the parties[40], or not holding oral hearings[41]. In this respect, any restriction on the adversarial principle must be counterbalanced by procedural safeguards[42]. To this end, both the ECtHR and the CJEU have stressed the importance of independent and impartial tribunals that have access to classified evidence and are empowered to examine the reasons given for non-disclosure of classified documents[43]. In addition, the ECtHR recognised that a special advocate representing the individual's interests can play an important role in counterbalancing the lack of full disclosure of evidence and the lack of open and adversarial hearings[44]. Overall, it must be ensured that the essence of the right to a fair trial is not compromised[45].

Effective redress is ensured in various ways in different national systems. For example, in some systems legal challenges can be brought by individuals before independent data protection authorities or independent specialised bodies, whose decisions can be challenged in court. In those cases, the data protection authority/specialised body will typically check on behalf of the individual whether the processing of personal data by an intelligence agency was lawful and exercise data protection rights (e.g. rights of access, correction and deletion). In other systems, complaints from individuals are handled by independent specialised bodies/tribunals and/or ordinary courts.

---

35 ECtHR, Ozdil and Others v. the Republic of Moldova, Application no. 42305/18, § 68; Chahal v. the United Kingdom, Application no. 22414/93, § 131.

36 ECtHR, Roman Zakharov v. Russia, § 234.

37 EctHR, Roman Zakharov v. Russia, § 234, 287; CJEU, La Quadrature du Net, § 190.

38 ECtHR, Regner v. Czech Republic, Application no. 35289/11, § 146; CJEU, Case C-300/11, ZZ v. Secretary of State for Home Department ('ZZ'), ECLI:EU:C:2013:363, § 55; Case C-89/08P, Commission v. Ireland and Others, ECLI:EU:C:2009:742, § 53.

39 ECtHR, Regner v. Czech Republic, § 148; Ternovskis v. Latvia, Application no. 33637/02, § 67; CJEU, ZZ, § 57.

40 ECtHR, Regner v. Czech Republic, § 148; Rowe and Davis v The United Kingdom, Application no. 28901/95, §61; Corneschi v. Romania, Application no. 21609/16, § 88 CJEU, ZZ, § 57.

41 ECtHR, Kennedy v. UK, § 188; Ternovskis v. Latvia §§65, 67; I.R. and G.T. v. UK, Application nos. 14876/12 and 63339/12, §58.

42 ECtHR, Regner v. Czech Republic, § 148; Ternovskis v. Latvia, § 67; .

43 ECtHR, Regner v. Czech Republic §§ 152, 153; Jasper v United Kingdom, Application no. 27052/95, §56; CJEU, ZZ, § 60.

44 ECtHR, A and Others v. UK, Application no. 3455/05, § 220; I.R. and G.T. v. the United Kingdom, §§ 61 and 63.

45 ECtHR, Regner v. Czech Republic, § 148; Adomaitis v. Lithuania, Application no. 14833/18, §§ 68-74.

In any case, any individual, regardless of nationality or place of residence, may, after exhausting such domestic remedies[46], bring a claim concerning a violation of the ECHR before the ECtHR[47]. Therefore, a U.S. individual can bring a claim before the ECtHR. Cases can be brought before the ECtHR claiming either that specific national surveillance measures violate the ECHR, or claiming that the national legal framework governing access to data for national security purposes violates the ECHR[48].

Finally, it is worth noting that the EU, along with the United States, endorsed on 14 December 2022 the Organisation for Economic Co-operation and Development (OECD) "Declaration on Government Access to Personal Data Held by Private Sector Entities", which, for the first time at international level, describes a set of core principles for public authorities' access to personal data in the area of law enforcement and national security that are common to OECD member countries. The Declaration reflects the type of privacy safeguards that the EU, its Member States, and the United States share in this area.

(e-signed)

Didier REYNDERS

[46] Irrespective of whether such remedies would fail on substantive or procedural grounds (e.g. admissibility).

[47] Articles 34 and 35(1) ECHR.

[48] See e.g. ECtHR, Klass and Others v. Germany, §§ 33-38; Weber and Saravia v. Germany, § 78; Roman Zakharov v. Russia, §§ 167-168.