Transatlantic Data Flows:

More Needed to Protect Human Rights

Greg Nojeim, *Senior Counsel and Director, Security and Surveillance Project*
Iverna McGowan, *Director, Europe Office of CDT*

October 2022

In a bid to preserve trans-Atlantic data flows, President Biden issued an Executive Order (EO) on October 7 seeking to satisfy the requirements that the Court of Justice of the European Union (CJEU) established when it determined that the Privacy Shield agreement between the U.S. and EU was inadequate. The EO limits intelligence surveillance directed abroad to 12 categories of purposes which, though broad, may be narrower than the purposes for which such surveillance could be engaged in before. Further, the EO, and an accompanying regulation from the Department of Justice (DOJ), establish a Data Protection Review Court (DPRC) to which persons from designated countries who allege they have been the subject of improper or unlawful surveillance may bring claims for redress.

While the EO marks a significant step forward, it does not conform in several respects to the requirements the CJEU has established, leaving continuing doubts about the extent to which the rights of non-U.S. persons abroad are being protected. In particular, absent further restrictions,

the breadth of the permissible purposes of surveillance under the EO may not meet the proportionality standard that surveillance should be limited to what is strictly necessary. In addition, the DPRC, while vested with substantial powers, is not a judicial entity independent from the Executive Branch, but rather is established as part of the DOJ. Indeed, while recognizing that "all persons should be treated with dignity and respect" and that they have "legitimate privacy interests," the Executive Order never crosses the critical line of acknowledging that non-U.S. persons abroad have privacy and data protection rights that the U.S. must honor.

Ultimately, whether the CJEU upholds a challenge to the expected adequacy decision may turn on the extent to which the CJEU gives a margin of appreciation to the surveillance regime the U.S. has put into place, given the political and legal realities in the U.S. with regard to how far the authorities could go.

We explain here how the U.S. could supplement the EO to better protect human rights of people subjected to surveillance directed abroad, and establish a legal regime more likely to receive a positive judgment from the CJEU. We recommend that:

- The Privacy and Civil Liberties Oversight Board (PCLOB) report on the extent to which the EO narrows actual surveillance activities that preceded it;
- Intelligence agencies clarify how they will interpret the EO requirements with respect to necessity and proportionality, disclose restrictions they intend to place on bulk and targeted collection, and disclose the procedures they will use for authorizing and implementing intelligence surveillance directed abroad;
- Congress considers narrowing the scope of permissible surveillance, requiring that surveillance targets be parties to communications collected in targeted intelligence surveillance, granting the DPRC subpoena power, granting complainants the right to appeal to federal court, and addressing the state secrets privilege;
- The Department of Justice permit the people the DPRC selects to advocate for a complainant's interests to communicate confidentially with the complainant; and
- The Administration reconsiders the policy of permitting bulk collection.

***

Background

The EO resulted from years of negotiations between the U.S. and the European Commission following the July 16, 2020 CJEU decision in the "Schrems II" litigation. That decision struck down the Privacy Shield agreement between the U.S. and the EU, which the European Commission had deemed "adequate." Over 5,000 firms in the U.S. relied on the Privacy Shield agreement for their compliance with the EU's General Data Protection Regulation (GDPR). The CJEU ruled that for transfers to continue, U.S. surveillance laws would need to provide essentially equivalent protections as those afforded under the GDPR (Article 45) read in light of the fundamental rights guaranteed in Articles 7, 8 and 47 of the EU Charter of Fundamental Rights. Such equivalence is a condition of cross border data flows under Articles 2(1) and 2(2) of the GDPR.

The EO is expected to be followed in approximately six months by a combined determination from EU institutions published by the European Commission that U.S. law provides "adequate" protection to Europeans' data. That determination will likely be challenged in the CJEU. If the CJEU determines the EO falls short of the requirements it established, data protection authorities in EU Member States could begin to cut off data flows to the U.S. that are essential for some Internet services.

***

Discussion

As we pointed out last year, the U.S. faced a huge challenge in light of the CJEU determination in Schrems II. It had to constrain American intelligence surveillance directed abroad in terms of proportionality and necessity, and it had to afford a process through which Europeans could seek redress at an independent "tribunal" with fair processes and strong authorities. U.S. officials claim that no EU member state imposes on its intelligence gathering the level of protections the CJEU is insisting the U.S. impose in order to meet the adequacy requirements of the GDPR. To the extent Member States are not meeting their own obligations under the EU Charter or under international human rights law, the U.S. posture ought to be to insist that Member states alter their surveillance practices to meet those obligations, rather than suggest that it is inappropriate for the CJEU to insist that the U.S. meet the data protection obligations the GDPR imposes to permit data transfers.

Necessity and Proportionality

1. Surveillance Objectives

The EO authorizes twelve (12) broad surveillance objectives, such as:

- Assessing the capabilities, intentions or activities of foreign political organizations, militaries and governments to protect U.S. national security and that of its allies and "partners";
- Assessing transnational threats that impact global security, including climate and other ecological change, public health threats and geographic rivalry;
- Protecting the integrity of elections and political processes from activities conducted by or with the assistance of foreign persons, organizations or governments; and
- Protecting against proliferation of weapons of mass destruction.

The EO also indicates that it is permissible to collect foreign private commercial information and trade secrets to protect the national security of the U.S., its allies, and "partners" when such collection furthers one or more of these objectives. The President can add to the lengthy list of authorized objectives, and do it secretly when releasing such an expansion publicly would, in the President's view, pose a risk to U.S. national security.

The EO also lists a handful of impermissible objectives of intelligence surveillance directed abroad:

- Suppressing or burdening free expression;
- Suppressing or restricting legitimate privacy interests;
- Suppressing or restricting a right to legal counsel (this is the only right specifically recognized as such in the EO);
- Disadvantaging a person based on their race, ethnicity, gender, gender identity, sexual orientation or religion; and
- Collecting foreign private commercial information or trade secrets to afford a commercial advantage to U.S. companies and businesses sectors.

Each element of the Intelligence Community, such as the National Security Agency (NSA) and the Central Intelligence Agency (CIA), must, within one year, update their policies and procedures to implement the privacy and civil liberties protections in the EO. Those updates presumably will account for these permissible and impermissible surveillance objectives.

2. Analysis of Surveillance Objectives

The list of *permissible* surveillance objectives marks an improvement over the permissible objectives for surveillance directed abroad that are laid out in EO 12333, which broadly authorizes surveillance to collect information about the activities or intentions of any foreign person abroad (Section 3.5(e)). It may also mark an improvement over the permissible objectives of surveillance that govern surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA), which permits surveillance to collect information that merely "relates to" U.S. national security or foreign affairs. 50 USC 1801(e)(2). All 12 authorized purposes reflect current national security concerns. As such, this list may be a step forward, both in terms of advancing the rights of non-U.S. persons abroad and moving U.S. policy in the right direction towards establishing stability for trans-Atlantic data flows. Establishing these permissible purposes of intelligence surveillance directed abroad may also inform the debate about reauthorizing Section 702 of FISA next year, when the scope of permissible surveillance is likely to be at issue.

The list of *impermissible* surveillance objectives in the EO is similar to the list of impermissible surveillance objectives in Presidential Policy Directive 28 (PPD-28), adopted in 2014 to govern intelligence surveillance directed abroad. The EO adds "suppressing or restricting" legitimate privacy

interests or the right to legal counsel to the PPD-28 list of impermissible surveillance purposes (Section 1(b)). Intelligence surveillance directed abroad may have the *effect* of one of these results, but such results cannot be "the purpose" of the surveillance. The government should explain how it interprets this prohibition (e.g., whether that means such results can be one purpose of surveillance directed abroad so long as it is not the sole purpose).

3. CJEU's Proportionality Test

A key area of controversy is whether the EO and accompanying regulation sufficiently cabin U.S. surveillance so it meets the proportionality requirements set by the CJEU. It is worth first briefly recalling what the proportionality test under EU law entails before analyzing whether the EO will pass this test. Proportionality is a concept rooted in international human rights law, and frequently used by both the European Court of Human Rights and the CJEU to ensure balance when derogating from any given right. In order to be lawful, a provision that would infringe upon protected rights: (i) must pursue an aim that is necessary and legitimate in a democratic society, and, (ii) must not go beyond what is strictly necessary to achieve that legitimate aim.

In Schrems II, the CJEU recognized the overall national intelligence aims as being legitimate, but stated upon examination of Section 702 of FISA and EO 12333 that they, "...cannot be regarded as limited to what is strictly necessary." The Court highlighted that both Section 702 and EO 12333 adopt a generalized approach to surveillance rather than a targeted approach. To be lawful under EU law, they would need to have a clear scope and precise rules governing the surveillance.

A clear risk is that the 12 permissible objectives of surveillance will be determined disproportionate because of their breadth, and that the short list of impermissible surveillance objectives won't sufficiently address this risk on account of their narrowness. The breadth of the permissible objectives is illustrated by the fact that neither the White House, the Department of Justice nor the Office of the Director of National Intelligence (ODNI) has given an indication that any surveillance practices occurring prior to issuance of the new EO would become impermissible as a result of these new rules. The 12 broad categories of permissible surveillance objectives set forth in the EO may be the same categories of surveillance objectives pursued prior to the EO. The Administration may need to clarify whether this is the case to provide greater assurance that the categories provide a meaningful limit on the scope of surveillance.

Although the EO does use the terms "necessary" and "proportionate," unless these are applied in practice to give more precision to the scope and rules governing the surveillance, it is not clear that use of those terms will enhance the likelihood of favorable consideration at the CJEU. The EO indicates that intelligence surveillance directed abroad can only be engaged in if "necessary to advance a validated intelligence priority" and "only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized." EO Sec. 2(a)(ii). At the same time, the DOJ Regulation makes clear that the EO should not be interpreted as importing the interpretations of the necessary and proportionate standard from international human rights law – including such law as articulated by the CJEU.

Rather, the DOJ Regulation states that the EO and its terms – including, presumably, "necessary" and "proportionate" – shall be interpreted "exclusively in light of United States law and the United States legal tradition, and not any other source of law." 28 CFR 201.10. However, the U.S has no law or legal tradition applying a necessary and proportionate standard to surveillance or other government activities. This apparently leaves elements of the Intelligence Community, and ultimately the CLPO and DPRC, free to develop their own interpretations of necessary and proportionate, which may or may not be based on existing interpretations of these terms by foreign bodies.

Another point for careful consideration, linked to the scope of surveillance, is that the EO specifically permits bulk collection of communications whenever an element of the intelligence community determines that information necessary to advance an intelligence priority cannot reasonably be obtained by targeted collection. The CJEU has been clear that legislation requiring companies to carry out *'general and indiscriminate transmission'* of data to the security and intelligence agencies for the purpose of safeguarding national security was unlawful (*Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* C-623/17, October 2020).

Indeed, in paragraph 93 of the "Schrems I" decision striking down the "Safe Harbor" adequacy determination, the CJEU noted, "In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life," which is guaranteed by Article 7 of the Charter of Fundamental Rights of the European Union. In the Schrems II ruling, the CJEU clarifies that the lack of access to judicial review, coupled with this generalized approach to surveillance, means that the bulk collection by

the U.S. is not delimited in a sufficiently clear and precise manner to be permissible. At the very minimum, there will need to be more clarity on the procedures and rules under which the intelligence community would make a determination on the necessity of bulk collection.

In addition, the U.S. would do well to tighten the scope of targeted as opposed to bulk collection. For example, FISA Section 702, which the U.S. regards as a targeted collection program, can permit the collection of information "about" a target of surveillance, rather than limiting collection only to communications to or from the target. Thus, if a communication merely mentions an identifier tied to a target, such as the target's email address, it could be collected even if the target is not a party to the communication. The NSA suspended "abouts" collection because it could not be executed technically in a lawful way, but can resume this type of collection if it fixes the technical problems and gives notice to Congress.

In summary, overall more measures are needed to better define the limitations and scope of surveillance in order to pass the proportionality test.

4. Proportionality Recommendations

To better protect the rights of persons subjected to intelligence surveillance directed abroad, and to increase the likelihood that the surveillance regime imposed by the EO and DOJ Regulation will survive proportionality review at the CJEU, we make the following recommendations:

- Incidental to its review of the policies and procedures that elements of the IC put in place to implement the EO, the PCLOB should clarify to the public the extent to which the 12 permissible objectives of surveillance rule out surveillance that has occurred in the past, and the extent to which they narrow the permissible scope of surveillance under FISA Section 702. PCLOB could also make this clarification in the report it plans to issue in connection with its review of FISA Section 702. Such a report is within PCLOB's mandate and within its own precedent: the PCLOB report on implementation of PPD-28 indicated the extent to which implementation of that directive changed intelligence community practices.
- Elements of the intelligence community should indicate in the policies and procedures they adopt to implement the civil liberties protections in the EO:

  - How they intend to implement the necessary and proportionate limitations in the EO;
  - Any restrictions they intend to impose on bulk collection, such as requirements that it be engaged in for a limited period of time unless re-authorized, that it be discontinued in specified circumstances, or that it be limited to certain defined geographic areas, such as a battlefield or a particular country or region;
  - Any restrictions they intend to impose on targeted collection activities, such as requirements that it be engaged in for a limited period of time unless reauthorized, and the circumstances in which it would be discontinued;
  - Additional precision about the scope of permissible surveillance under the 12 surveillance objectives set forth in the EO, such as clarifying how the measures taken would be proportionate to the actual risks identified; and
  - Procedures they will implement for authorizing and supervising intelligence surveillance directed abroad, storing and destroying intercepted data in accordance with applicable retention requirements, and the internal procedures they will adopt to ensure that the requirements of the EO are met.
- When determining whether to reauthorize FISA Section 702, which sunsets on December 31, 2023, Congress should consider whether to amend FISA to permit Section 702 surveillance only for the 12 permissible objectives in the EO, and narrow, where appropriate, the scope of those objectives.
- Congress should also consider outlawing "abouts" collection in the context of reauthorizing FISA Section 702 in order to focus surveillance on communications to or from targets.
- The Administration should re-examine the U.S. position on bulk collection abroad, given its gross impact on privacy and in light of the fact that it outlawed bulk collection domestically in the USA FREEDOM Act of 2015.

Redress

1. Process

The EO and the associated DOJ Regulation establish a redress system with three tiers. First, a complainant would have to bring their complaint to "the appropriate public authority" in a designated country or region. These authorities are not specified in the EO or in the DOJ Regulation,

but are likely to be national data protection authorities. Only complaints referred by these authorities will be considered in the U.S. Not all foreign individuals can trigger such referrals: only people from the states and regions the DOJ has designated can do so. A country or "regional economic integration organization" (such as the EU as a whole) can be designated a "qualifying state" if the Attorney General determines that its laws require "appropriate safeguards" for U.S. persons' personal information acquired through intelligence surveillance that is transferred to the qualifying state. Reciprocity is not required — the qualifying state need not necessarily establish, e.g., a strong redress mechanism or narrow grounds for surveillance — it need only establish "appropriate safeguards."

The complaint must allege a violation of the U.S. Constitution, applicable sections of FISA, Executive Order 12333, or the new EO or guidance implementing the new EO. It must allege that such violation occurred as a result of U.S. intelligence surveillance directed abroad and that the complainant's privacy and civil liberties interests were adversely affected. While it need not allege the "injury in fact" that is necessary to establish standing in a U.S. court, it must state the specific means by which the complainant believes their personal information was transferred to the U.S. The appropriate authority abroad verifies that these allegations have been made and the identity of the complainant.

The complaint is then referred to the Civil Liberties and Privacy Officer (CLPO) of the Office of the Director of National Intelligence. The CLPO is an element of the Intelligence Community and, though its mandate includes oversight functions, cannot be regarded as independent. It conducts fact finding and determines whether there has been a violation of the U.S. Constitution, FISA, EO 12333, the new EO, or agency guidelines issued under it. If the CLPO determines that there has been a violation, it does not inform the complainant of the nature of the violation or even that there was a violation of any kind. Likewise, it does not inform the complainant when there was no violation. It does not inform the complainant as to whether they were subjected to surveillance. In every case, the complainant receives the same determination, the text of which is set forth in the EO: *"[t]he review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation."* From the complainant's perspective, the determination is predetermined.

From the CLPO's perspective, this is not the case. The CLPO conducts fact-finding regarding the alleged covered violation and each element of the Intelligence Community is required to provide access to the

necessary information. The Director of National Intelligence (DNI) is prohibited from interfering with the investigation. The CLPO, if it finds a violation, is empowered to order remediation, including cessation of improper or unlawful surveillance and deletion of data resulting from such surveillance.

The CLPO's order binds the Intelligence Community with respect to the complainant, but the complainant will never know that such an order has been issued. The CLPO cannot order that a surveillance program be abandoned or limited because it is not empowered to issue programmatic orders. But its orders can apparently have programmatic impact if the CLPO's order to cease or limit surveillance of the complainant is based on a finding that a program operated improperly or unlawfully with respect to the complainant. The IC element operating the program would be hard-pressed to leave it in place without change after such an order was issued.

After the CLPO conveys the predetermined determination to the complainant, the complainant must decide whether to appeal the determination to the third and final tier of the redress process, the Data Protection Review Court (DPRC). Given the dearth of information provided to the complainant, it is difficult to understand how the decision to appeal will be made. Indeed, it is entirely possible that a complainant would appeal a CLPO decision in the complainant's favor because the complainant did not know that a favorable decision had been rendered.

The DPRC is a Department of Justice entity, but has a level of independence within the DOJ. It will consist of six judges chosen by the Attorney General who may not be employees of the U.S. government and who are legal practitioners with experience in data privacy and national security law, with a preference for former judges. They cannot be fired except for cause, and they serve a four-year term. The complainant and the government can both appeal the CLPO's decision to the DPRC, but if the government appeals, the complainant is not told that this has occurred. A three-judge panel of the DPRC (chosen by rotation) receives a record on appeal from the CLPO and appoints a "special advocate" whose duties include advocating regarding the complainant's interest.

The special advocate must have a security clearance and will have access to classified information. The DOJ Regulation makes it clear that the special advocate cannot be regarded as the attorney for the complainant, stating specifically that no attorney-client relationship exists. Troublingly, the DOJ Regulation bars the special advocate from communicating with the complainant directly, confidentially, or orally.

The special advocate may submit written questions to the complainant via the relevant public authority, but the CLPO, in consultation with the relevant IC elements, screens the questions for classified or "protected" information. 28 CFR 201.8(d).

Like the CLPO, the DPRC determines whether there has been a "covered violation" of the U.S. Constitution, FISA, EO 12333, the new EO, or the guidelines issued under it. If it finds a violation, it is empowered to order appropriate remediation, but only after receiving the views of the affected elements of the Intelligence Community. The DPRC is required to give "appropriate deference" to relevant determinations of national security officials consistent with deference shown in U.S. Supreme Court case law. The DPRC's decisions are binding on elements of the Intelligence Community, and they are final. The "appropriate remediation" it can order includes termination of surveillance and deletion of unlawfully acquired data. The DPRC's decision are controlling only as to the application for review; they may be considered as non-binding precedents by other DPRC panels. The Attorney General cannot overrule them.

The complainant is left in the dark about DPRC determinations. As with those of the CLPO, the complainant is not advised as to whether a violation was found, and if so, the nature of the violation. And, all the appealing complainants receive the same predetermined determination from the DPRC, *"[t]he review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."*

2. Redress Analysis

The redress procedures amount to a remarkable ceding of authority by elements of the Intelligence Community to the CLPO and the DPRC. These entities are given authority to issue orders that bind the IC elements and that cannot be overruled by the DNI or the Attorney General, respectively.

Nevertheless, complainants are unlikely to be satisfied with the redress process because they cannot participate in it meaningfully. They file a complaint and receive back the same predetermined determination that every other complainant receives. They never learn whether they were subjected to surveillance. If they somehow knew they had been

surveilled, they wouldn't learn whether the surveillance was determined to be wrongful. If they were wrongfully surveilled, they will never be told what remedial actions were taken as a result. They cannot communicate orally or confidentially with the person who is supposed to represent their interests in the DPRC proceedings. These factors make it less likely people will file complaints.

The CJEU in Schrems II indicated that to be adequate, a redress mechanism had to have the following attributes:

> (i) the power to order a stop to unlawful surveillance;
> (ii) the power to order the deletion of information unlawfully collected;
> (iii) the fact-finding capability to compel disclosure of the information necessary to the
> exercise of such powers; and
> (iv) the ability to receive complaints and hold fair hearings at an independent and impartial tribunal at which a complainant can be properly represented.

A. Powers to stop surveillance, delete data and compel disclosure of needed information

The EO and the DOJ Regulation score relatively well on the first two attributes the CJEU established for a redress mechanism in Schrems II: both the CPLO and the DPRC will have the power to order a stop to surveillance they deem to be improper or unlawful under U.S. law and the power to order the deletion of data unlawfully or improperly collected. However, as noted above, the categories of proper surveillance defined in the EO are quite broad, and it is possible that the PCLO or DPRC will find surveillance to be lawful under U.S. law even if it would not be under EU or international law.

Whether the PCLO and the DPRC will be able to compel disclosure of the information necessary to their mission is unclear. The EO pointedly directs elements of the IC to cooperate with the PCLO's and with the DPRC's requests for information. These are positive requirements that give the PCLO and DPRC authority they will need to conduct the necessary investigative activity. However, neither has the authority to compel cooperation. This authority is often given to investigative bodies in other contexts by empowering them to issue subpoenas and by empowering the Department of Justice to enforce them. Although these bodies cannot compel the disclosure of information, the PCLOB will report annually on the level of cooperation the DPRC is receiving.

Whether the PCLO and DPRC will have sufficient access to information without the ability to compel disclosure of information remains to be seen.

B. Right to A Fair Hearing and Representation

A further issue for the CJEU will be whether the EO and DOJ Regulation sufficiently meet the standards under Art. 47 of the EU Charter, cited in the Schrems II ruling. Art. 47 specifies that a person whose rights have been violated has a right to an effective remedy before a fair and impartial tribunal that must provide "a fair hearing [and] the possibility of being advised, defended and represented."

C. Representation

Although the DPRC can appoint an advocate for the complainant's interests, the "special advocate" arrangement does not have many of the hallmarks of traditional representation: they are not chosen by the complainant, the complainant and advocate do not have an attorney-client or similar confidential relationship, and they may not even communicate orally, directly, or confidentially. Although this does not preclude the complainant appointing their own lawyer, that lawyer would not have access to the proceedings or to the information that may form the basis of the DPRC's decision. Given that the right to be properly represented is a key principle of Art. 47 of the EU Charter, which the Schrems II judgment cites several times, and that the CJEU has ruled that there is a right for a complainant to freely choose their own lawyer (C-667/18), this is also likely to be a source of controversy.

D. Independence & Impartiality

The main fact-finder in the redress process — the PCLO — is not independent; it is part of the intelligence community, the conduct of which is called into question in the investigation the PCLO conducts. The PCLO's determinations can be appealed by the complainant to the DPRC, which is semi-independent and which can also engage in fact finding.

The DPRC is a court established within an executive branch agency as opposed to being established by law in the judicial system. This is an attribute suggesting a lack of independence from that agency. However, its decisions are binding on that agency and on the other elements of the Intelligence Community, which suggests independence. The DPRC relies on the cooperation of IC elements to obtain the information it needs; they are required to cooperate with its information requests, but it has no power to compel such cooperation. The DPRC also relies on the PCLO to properly document the decisions that are appealed to it. These levels of reliance suggest a lack of independence. Although the DPRC certainly

has more independence (see points on appointment and removal of adjudicators) and more authority to issue binding decisions than the Ombudsperson under the prior Privacy Shield regime, the CJEU will have to decide whether the fact that it is at base a body of the executive arm of government means the DPRC is incapable of being sufficiently independent.

Furthermore, Article 78(1) and (2) of the GDPR recognize the right of each person to an effective judicial remedy when a data protection authority (DPA) renders an adverse decision or fails to deal with his or her complaint. In the EO, it appears that the DPRC is aiming to emulate the role of a DPA, meaning that to offer 'essentially equivalent protection,' the complainant would have to be afforded an opportunity to appeal the DPRC decision to a fully independent federal court established under Article III of the U.S. Constitution. Access to judicial review was also a criterion in the Schrems II judgment with regard to the lawfulness of surveillance.

3. Redress Recommendations

To better protect the rights of persons subjected to intelligence surveillance directed abroad, and to increase the likelihood that the surveillance regime imposed by the EO and DOJ Regulation will survive review at the CJEU, we make the following recommendations:

- The DOJ should amend its regulation to free the special advocate to communicate confidentially with the complainant. Special advocates will be few in number, will hold security clearances and will be chosen carefully pursuant to regulations the Attorney General will issue. Their communications are no more suspect than are the communications of the 1.3 million other people who have top secret security clearances;
- Congress should consider giving the DPRC subpoena authority in order to compel the disclosure of information it may need to conduct its work. If Congress grants such authority, it should ensure that the DOJ has the authority to enforce DPRC subpoenas;
- Congress should consider giving complainants the opportunity, by statute, to appeal DPRC decisions to a federal court. An adverse decision by the DPRC should constitute an injury-in-fact for purposes of establishing standing. Should Congress act, it should not attempt to dictate to the court the determination it must issue: there

are circumstances in which the fact of improper or unlawful surveillance can be disclosed to the complainant without threatening national security These decisions may already be appealable as final agency actions under Administrative Procedures Act; and

- In anticipation of the possibility of appeals to federal court, Congress should consider legislation to address the state secrets privilege in order to make it more likely that a decision on the merits of an appeal can be reached.

***

Conclusion

The EO and accompanying DOJ Regulation represent significant steps forward in the protection of the rights of EU citizens and others against U.S. surveillance directed abroad. They define the scope of permissible surveillance, impose certain limitations and safeguards, and put in place a redress mechanism with the power to order stoppage of unlawful or improper surveillance.

At the same time, as this paper has highlighted, the CJEU would likely take issue with the broad scope of permissible surveillance, the limitations on the ability of the CLPO and the DPRC to compel disclosure of information for their investigations, the independence and impartiality of the CLPO and the DPRC, the lack of meaningful legal representation in those fora, and the lack of access to formal judicial review.

We have made a number of recommendations to enhance the rights of people who may be subjected to surveillance under the EO and to make it less likely the system it establishes will again be struck down at the CJEU.

***

cdt.org

cdt.org/contact

Center for Democracy &
Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

202-637-9800

@CenDemTech

CENTER FOR
DEMOCRACY
& TECHNOLOGY