Cybersecurity and Information Security Newsletter

Issue 23 | December 1, 2022

Table of Contents

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

President Biden signs an Executive Order to implement a new privacy framework with respect to "Signals" Intelligence

On October 7, 2022, President Biden signed Executive Order 14,086 to address privacy concerns surrounding U.S. signals intelligence activities. *E.O. 14086*, available here. Signals intelligence refers to the collection of foreign intelligence from communications and information systems (usually from electronic sources) to support U.S. government activities. *Signals Intelligence (SIGINT) Overview*, available here. The Executive Order maintains the necessity of providing signals intelligence operations to advance U.S. national security interests. However, it also reaffirms U.S. policy that "signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside." *Id.; see generally Presidential Policy Directive -- Signals Intelligence Activities [Archived from President Obama's White House page]*, available here.

The Executive Order establishes new safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate to the U.S. national security objectives against the backdrop of protecting the privacy interests of all persons. *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*, available here

Background

Although the internet opened opportunities for businesses and individuals to share information across the world, many countries have different data protection requirements that regulate the transfer of certain data (e.g., personal data) across borders. In particular, the EU enacted the General Data Protection Regulation (GDPR) in 2016, which put strict constraints on the transfer of personally identifiable data of EU residents. Switzerland has its own comprehensive data protection regime, the Federal Act on Data Protection (FADP). To address the need for a harmonious legal mechanism for data transfers, the EU-U.S. and Swiss-U.S. Privacy Shield Framework was developed to provide businesses with a mechanism to comply with data protection regulations when transferring personal data from the E.U. and Switzerland to the U.S. (which lacks a federal level comprehensive data protection regulation). *Privacy Shield Overview*, available here.

The Fall of the EU-U.S. and Swiss-U.S. Privacy Shield

The European Commission and the Swiss Government both approved the EU-U.S. and Swiss-U.S. Privacy Shield Framework in 2016 and 2017, respectively. However, on July 16, 2020, the Court of Justice of the European Union (CJEU) invalidated the European Commission's Decision that had previously implemented the EU-U.S. Privacy Shield Framework. *ECLI:EU:C:2020:559 [Court of Justice of the European Union]*, available here. The CJEU found that the U.S. implementation of its surveillance program did not adequately protect EU subjects' personal data transferred to the U.S. Specifically, the Court noted that the U.S. surveillance program did not implement the principle of proportionality required under EU law, where the collection of information ought to be limited to what is strictly necessary. Finally, the CJEU concluded that EU individuals did not have a right to present allegations of unlawful surveillance operations in a U.S. court. The Court found that the EU-U.S. Privacy

Shield Framework was incompatible with the EU Charter of Fundamental Rights, and it invalidated the cross-border data transfer framework.

On September 8, 2020, the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland concluded that the Swiss-U.S. Privacy Shield failed to provide adequate levels of data processing protection for Swiss nationals under Swiss's FADP, which provides statutory data processing protections for Swiss nationals. *Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 Para. 1 Swiss Federal Act on Data Protection*, available here. Although the FDPIC did not invalidate the Swiss-U.S. Privacy Shield, the FDPIC's position paper made it clear that data processors transferring Swiss personal data to the U.S. cannot rely on the Swiss-U.S. Privacy Shield to meet fully FADP requirements. To support its findings, the FDPIC highlighted (1) the lack of ability for Swiss nationals to pursue an "enforceable legal remedy" against unlawful data access by U.S. officials and (2) that the lack of transparency surrounding the Swiss-U.S. Privacy Shield ombudsperson mechanism prevented a proper assessment of its decision-making powers and its independence from the U.S. Intelligence Community.

Establishment of the Trans-Atlantic Data Privacy Framework

Without a legally recognized cross-border data transfer agreement in place, multinational companies faced regulatory difficulties when attempting to transfer and process personal data from Europe to the U.S. In response, on March 25, 2022, the White House and the European Commission announced their commitment to a new Trans-Atlantic Data Privacy Framework that addressed concerns from both the CJEU's decision and the FDPIC's position paper. *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, available here. Specifically, the Trans-Atlantic Data Privacy Framework committed the U.S. to three main goals:

- Strengthen the privacy and civil liberties safeguards governing U.S. signals intelligence activities;
- Establish a new redress system mechanism with independent and binding authority; and
- Enhance existing U.S. oversight of signals intelligence activities.

President Biden's October Executive Order follows from the Trans-Atlantic Data Privacy Framework by implementing regulations that meet the Framework's commitment.

Implementation of a New Signals Intelligence Activities Policy

On the same day President Biden signed Executive Order 14,086, the White House issued the National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, in a likely preparation for issuing an updated Presidential Policy Directive 28 (PPD-28) that aligns with the Executive Order. *National Security Memorandum on Partial Revocation of Presidential Policy Directive 28*, available here.

PPD-28 outlined the U.S. government's policies on implementing signals intelligence activities that take into account of privacy and civil liberty interests of all persons. *See Presidential Policy Directive -- Signals Intelligence Activities [Archived from President Obama's White House page]*, *supra*. It was analyzed and mentioned with concern by both the CJEU and the

FDPIC when determining whether U.S. signals intelligence activities conflicted with the data protection laws of the EU and Switzerland.

Following the Executive Order, the U.S. Department of Justice (DOJ) announced a regulation that established a new redress mechanism for foreign nationals to submit complaints of alleged violations of U.S. law concerning U.S. signals intelligence activities. *Data Protection Review Court [Federal Register], 87 FR 62303*, available here. The new redress mechanism will be comprised of two levels. At the first level, the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI CLPO) will review and investigate incoming private complaints and take appropriate remediation to qualified complaints. At the second level, the Data Protection Review Court (DPRC) will review any appeals from the complainant or a member of the U.S. Intelligence Community to reexamine ODNI CLPO's determinations. The DPRC's decision will be final and binding for each complaint, but it will not establish "precedent" for other complaints. *Id.* at *PART 201—DATA PROTECTION REVIEW COURT, § 201.9(g)*, available here.

DOJ's Office of Privacy and Civil Liberties has been designated to provide administrative support for the DPRC. As of this newsletter's publication, no specific timelines have been announced for the establishment of the DPRC.

Analysis

The new Executive Order attempts to address concerns raised by both the CJEU and the FDPIC to reestablish a Privacy Shield framework. It affirms that U.S. signals intelligence activities will be conducted in a manner that is proportionate to the U.S. intelligence needs while striving to achieve an appropriate balance between the need for signals intelligence collection and the protection of privacy and civil liberties of all persons. The DOJ's regulation on the establishment of the DPRC provides transparency into the assessment process of reviewing complaints against alleged unlawful violations stemming from signals intelligence activities. At first glance, the Executive Order seems to pave the way for a new Privacy Shield agreement that can reopen trans-Atlantic data transfers to facilitate commerce.

Max Schrems, the Austrian lawyer who successfully challenged the legality of the EU-U.S. Privacy Shield under European law, has noted that the new Executive Order fails to address concerns raised by the CJEU decision against the Privacy Shield. *Schrems: round three [The Tech Brief]*, available here. Schrems argues that the new Executive Order does not adopt the definition of "proportionality" under EU law, but instead the understanding based on U.S. law.

According to the Executive Order, many legal determinations are to be examined under "applicable United States law," and the DPRC will examine alleged complaints under U.S. law. Schrems is correct that the new U.S. signals intelligence policies, including those applying the concept of "proportionality," will be examined and implemented from the U.S. legal perspective. From a policy perspective, it is not likely that the U.S. will adopt a foreign understanding of fundamental legal concepts unless there is a treaty establishing that approach.

Schrems noted that he would likely challenge the new Privacy Shield framework because it still fails to guarantee the same level of data protection for European data subjects, whose data reside in the U.S.—an extraterritorial argument. However, the CJEU has already constrained this kind of extraterritorial reach of the GDPR, potentially making Mr. Schrems'

challenge to the new Privacy Shield framework a difficult one. *See, e.g., ECLI:EU:C:2019:772 [Court of Justice of the European Union],* available here.

Based on the review of the CJEU's decision and the FDPIC's position paper, the Executive Order *prima facie* did address all the main concerns expressed by the European authorities. Although the Executive Order's implementation needs to be observed, it may be likely that the new policies for U.S. signals intelligence activities could be seen as compatible with legal policies adopted by the European Union and Switzerland. At least under EU law, government surveillance is permissible as long as it is "provided for by law and be necessary and proportionate." *Surveillance [European Data Protection Supervisor]*, available here. The text of the new Executive Order seems to follow closely with the EU's surveillance approach.