

Third Time's a Charm? The Future of Privacy Shield 3.0 and Data Transfers to the U.S.

Bret Cohen
Hogan Lovells

Alex Greenstein
U.S. Department of Commerce

Laurence E. Rothenberg
Privacy and Civil Liberties Oversight Board

May 12, 2023

Speakers



Bret Cohen

Partner
Hogan Lovells



Alex Greenstein

Director, Privacy Shield
U.S. Department of Commerce



Laurence E. Rothenberg

Counselor to the Hon. Beth A. Williams
Privacy and Civil Liberties Oversight Board

- Data transfer mechanisms must afford **essentially equivalent** privacy protection to EU residents, taking into account:
 - Whether the receiving entity is subject to sufficient commercial privacy standards, or the transfer is subject to a derogation
 - Whether the receiving entity is subject to sufficient protections from undue access to personal data by law enforcement
- **Privacy Shield** = immediately **no longer lawful** because:
 - U.S. surveillance is not limited to that which is necessary and proportionate
 - EU data subjects do not have actionable redress before U.S. courts

- Surveillance is not limited to that which is **necessary** and **proportionate**
 - Focus on FISA Section 702, E.O. 12333
 - Neither consider whether “individuals are properly targeted”
 - Do not confer rights which are enforceable against US authorities
- EU data subjects do not have **actionable redress** before U.S. courts
 - No hearing before an independent and impartial tribunal
 - Privacy Shield Ombudsperson
 - No guarantees on revocation of appointment, so not sufficiently independent
 - Ombudsperson does not have power to adopt decisions binding on intelligence community

Result: EU-U.S. Data Privacy Framework



Consists of:

- Presidential Executive Order (issued October 7, 2022)
- U.S. Department of Justice regulations (issued October 7, 2022)
- Commercial principles (published in draft adequacy decision Dec 13, 2022)

From Safe Harbor to EU-U.S. DPF

U.S. ★ EU

SAFEHARBOR

U.S. DEPARTMENT OF COMMERCE



Privacy Shield
Framework

**EU-U.S. DATA PRIVACY
FRAMEWORK**

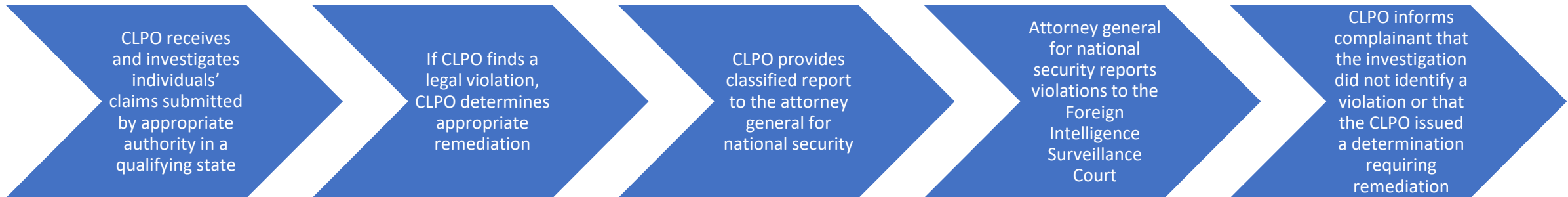
- Necessity and proportionality standard:
 - “Determination . . . that the [signals intelligence] activities are necessary to advance a validated intelligence priority”
 - “Conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which it has been authorized”
- 12 enumerated legitimate objectives, e.g.:
 - Understanding or assessing capabilities, intentions, or activities of a foreign gov’t or organization, in order to protect U.S. and ally national security
 - Understanding transnational threats that impact global security
 - Protecting against terrorism, espionage, foreign military, WMD, cyber threats, transnational criminal threats, threats to election integrity

Addressing necessity and proportionality

- Civil Liberties Protection Office (CLPO) of Office of the Director of National Intelligence must validate activities for legitimate objectives and ensure no prohibited objectives
- Privacy and civil liberties safeguards for signals intelligence:
 - Consider availability, feasibility, and appropriateness of less intrusive alternatives
 - Tailor to validated intelligence priority and not disproportionately affecting privacy and civil liberties
 - Prioritize targeted collection over bulk collection
 - Limit dissemination and retention
 - Data security and access requirements
 - Each element of Intelligence Community to update policies in consultation with the CLPO and the Privacy and Civil Liberties Oversight Board (PCLOB), publicize as widely as possible
 - Additional further review of policies and procedures by PCLOB

Addressing redress

Step 1: Civil Liberties Protection Officer (CLPO) Review



Step 2: Data Protection Review Court (DPRC) Review



Oversight

Department of Commerce consults with the intelligence community every 5 years on whether information has been declassified and can be released.

PCLOB to conduct annual review of redress process, publicly certify that it is operating as it should, and release an unclassified version of its report.

FISA Section 702 reauthorization



U.S. PRIVACY AND
CIVIL LIBERTIES
OVERSIGHT BOARD

Oversight Projects



FISA Section 702

The Board is conducting an Oversight Project to examine the surveillance program that the Executive Branch operates pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA), in anticipation of the December 2023 sunset date for Section 702 and the upcoming public and Congressional consideration of its reauthorization. The goals of the Oversight Project are to ensure that privacy and civil liberties are protected in the course of the Executive Branch's use of its Section 702 authorities, and to ensure that Congress and the public are able appropriately to assess and consider the program's value, and efficacy in protecting the nation's security and producing useful intelligence.

This Oversight Project is examining significant changes to the operation of the 702 program since the Board's *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) ("2014 Report") in order to provide an accurate description of the current program. The Board's review covers selected focus areas for investigation, including but not necessarily limited to, U.S. Person queries of information collected under Section 702, and 'Upstream' collection conducted pursuant to Section 702. The Oversight Project also includes reviewing the program's past and projected value and efficacy, as well as the adequacy of existing privacy and civil liberties safeguards.

Path to adequacy?

- Dec 13, 2022: European Commission published draft adequacy decision
- Feb 14, 2023: European Parliament LIBE Committee published (non-binding) draft resolution *against* adequacy
- Feb 28, 2023: EDPB adopted (non-binding) opinion on adequacy
 - Welcomed “substantial improvements”
 - “Expresse[d] concerns” and “requested clarifications” on
 - Law enforcement aspects: data subject rights, onward transfers, scope of exemptions, temporary bulk collection of data, practical functioning of the redress mechanism
 - Commercial aspects: exemptions to right of access, absence of key definitions, lack of clarity about application to processors, broad exemption the right of access for publicly available info, lack of specific rules for automatic decision-making and profiling
- Next step: Member state approval (need 15-of-27 & at least 65% of EU population)

Questions?



Bret Cohen

Partner
Hogan Lovells



Alex Greenstein

Director, Privacy Shield
U.S. Department of Commerce



Laurence E. Rothenberg

Counselor to the Hon. Beth A. Williams
Privacy and Civil Liberties Oversight Board