

February 1, 2017

Privacy Implications of President Trump's Immigration Order

On Wednesday, January 25, President Donald J. Trump [directed](#) federal agencies, “to the extent consistent with applicable law,” to ensure that “their privacy policies exclude persons who are not U.S. citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.” That directive, Section 14 of an Executive Order that expands enforcement of U.S. immigration laws, is a departure from how the federal government previously has treated personally identifiable information (“PII”) of those who are not U.S. citizens or lawful permanent residents (“non-U.S. persons”) in many contexts, including the processing of visas and immigration records.

The Privacy Act of 1974 requires federal agencies to meet specific minimum privacy standards with respect to PII in databases they maintain. The Privacy Act is frequently recognized for promoting the Fair Information Practice Principles (“FIPPs”), which have become a widely accepted framework for evaluating and considering systems, processes or programs that impact individual privacy. The FIPPs have served as a model for the privacy laws of many U.S. states, foreign countries and international organizations.¹

Although the Privacy Act only requires that federal agencies apply minimum privacy standards to the PII of U.S. citizens and lawful permanent residents,² many agencies historically have applied the same standards to the PII of non-U.S. persons as well.³ In addition, the Judicial Redress Act of 2015⁴ gives the Attorney General discretion to extend the rights and remedies of the Privacy Act to citizens of specific regional economic integration organizations and foreign countries to the extent they are so designated in the Federal Register. Pursuant to the Judicial Redress Act, outgoing Attorney General Loretta Lynch [officially designated](#) the EU and most EU member countries as “covered” countries whose citizens are afforded Privacy Act protections, effective February 1, 2017.⁵ As a result, the Privacy Act now covers the processing of personal data of EU citizens by federal agencies in the United States. Nothing in Section 14 changes this coverage, because the Executive Order does not trump the Judicial Redress Act or the Federal Register designations.

A. Initial Privacy Impact

In order to comply with Section 14, federal agencies will need to revise their privacy policies to exclude non-U.S. persons. In the short term, these changes primarily will impact non-U.S. persons who are citizens of countries outside of the EU, because any changes must be consistent with the Judicial Redress Act, which extends the protections of the Privacy Act to EU citizens based on the current Federal Register designations.

Pursuant to their revised privacy policies, however, agencies lawfully may ignore the FIPPs when processing the PII of non-U.S. persons who are citizens of countries outside of the EU. For example, agencies may disclose the PII of such non-U.S. persons without their consent to other agencies or third parties. While disclosures of this sort

¹ See, e.g., United States Department of Homeland Security, [Privacy Policy Guidance Memorandum](#) (Dec. 29, 2008).

² See 5 U.S.C. § 552a(a)(2).

³ See, e.g., Department of Homeland Security Privacy Policy Guidance Memorandum No. 2007-1 (2007) (“As a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.”).

⁴ Pub. Law No. 114-126 §2(d).

⁵ The designations will become effective simultaneously with the U.S.-EU Data Protection and Privacy Agreement (DPPA). Congress passed the Judicial Redress Act in order to implement the redress right provisions of the DPPA.

presumably include the Executive Order's proposed publication of lists of crimes committed by aliens,⁶ the ability to share information freely appears to sweep more broadly. Agencies may no longer be able to:

- provide non-U.S. persons who are citizens of countries outside of the EU with access to PII concerning them that is maintained in agency databases;
- devote resources to ensure that PII of such persons is accurate, relevant, timely and complete; or
- consider requests from such persons that their records be amended.

As a result, non-U.S. persons from countries outside the EU may be unable to confirm that data held about them is correct, or request that mistakes in such data be corrected.

B. Longer-Term Privacy Impact

Although some European commentators have voiced concern that the Executive Order threatens the viability of the recently enacted EU-U.S. Privacy Shield framework for regulating transatlantic data transfers, the EU Commission reportedly indicated in an [emailed statement](#) that such concerns are unfounded. The Commission added that the U.S.-EU Data Protection and Privacy Agreement, which establishes a set of protections, including specific judicial redress rights, for PII exchanged between the United States and the EU for law enforcement purposes, also will remain in place.

Once confirmed, the new Attorney General will have some discretion under the Judicial Redress Act to remove the designations of the EU and most EU member countries as "covered" countries whose citizens are afforded Privacy Act protections. Nonetheless, the new Executive Order does not require such removal explicitly. Unless the European Commission decides to reconsider whether the privacy rights afforded EU citizens under the Judicial Redress Act adequately protect their PII, it is too soon to say whether the Executive Order specifically will impact the Privacy Shield status quo.

⁶ See Section 9(b) of the Executive Order.