CRS Reports & Analysis

Legal Sidebar

Judicial Redress Act 101 – What to Know as Senate Contemplates Passing New Privacy Law

01/21/2016

Update: The Senate Judiciary Committee delayed the markup on S. 1600, the Judicial Redress Act, previously scheduled for January 21, 2016.

Reports indicate that the Senate may soon vote on the Judicial Redress Act (JRA), a bill that could have major implications on transatlantic data flows and the global economy. The House of Representatives passed the JRA (H.R. 1428) in October (for the House Report on the JRA, see here), and the Senate is currently considering an identical version of the JRA (S. 1600). To understand why the JRA is important, it's first worth discussing the underlying legislation that the JRA would amend: the Privacy Act of 1974.

The Privacy Act generally regulates how the federal government collects, uses, and discloses "records" – a term of art defined by the Act to refer to information possessed by a federal agency that contains individual identifying information. The Privacy Act provides for civil remedies by private parties to help enforce its provisions in four situations:

1. when an agency refuses to amend an individual's record;
2. when an agency refuses to provide access to an individual's record;
3. when an agency has failed to maintain certain records in an accurate, relevant, timely, and complete manner, resulting in an "adverse effect" on an individual; and
4. when an agency fails to comply with "any other provision" of the Act or rule promulgated pursuant thereunder resulting in an "adverse effect" on the individual.

The Privacy Act as currently written is limited to the records of an "individual," a term the Act defines as a "citizen of the United States or an alien lawfully admitted for permanent residence." As a result, a foreign national who is not lawfully admitted for permanent residence and believes a federal agency is failing to comply with the Privacy Act with respect to his record currently has no judicial recourse under the 1974 law.

The JRA generally would amend the Privacy Act to expand the number of eligible Privacy Act plaintiffs under certain, narrow circumstances to a limited group of foreign nationals. The JRA would **not** allow every foreign national to obtain civil relief under the Privacy Act; instead the JRA would expand the Act to cover foreign nationals from countries **specifically designated by the Attorney General** because of formal or informal information sharing arrangements respecting transnational crime. Moreover, even if a foreign national is from a designated country, **not all** four categories of Privacy Act civil actions are made available by the JRA; instead the proposed legislation would allow foreign nationals to proceed under categories (1) or (2) only if the information at issue was possessed by a **designated federal agency** that receives information from the foreign national's home country because of a formal or informal information sharing agreement between the United States and the home country. In addition, the JRA would allow a covered foreign national to pursue one specific cause of action under category (4)—the JRA would allow a plaintiff to recover actual damages if a plaintiff can prove that a federal agency has **intentionally or willfully** disclosed a covered record without written consent. Finally, the JRA does not allow a covered foreign national to pursue claims with respect to ***any*** **record**; instead the bill would only cover records that have been transferred by an entity within the foreign

national's home country for the purpose of "preventing, investigating, detecting, or prosecuting criminal offenses."

Attention has centered on the JRA following a major ruling by the European Court of Justice of the European Union (CJEU) invalidating the U.S.-E.U. Safe Harbor Agreement, which generally permitted companies to transfer personal data from the E.U. to the U.S. The decision centered on an interpretation of the E.U.'s 1995 Data Protection Directive (Directive) which requires member states to establish privacy laws that would bar the transfer of personal data to non-E.U. countries that fail to provide an "adequate" level of privacy protections. The Directive permits the European Commission (EC), an executive body within the E.U., to make general determinations regarding whether other countries offer the needed level of protection in their domestic laws or international commitments. To ensure compliance with the Directive, in the late 1990s, the Department of Commerce and the EC negotiated the Safe Harbor agreement which permits an American company to receive E.U. citizens' data if it meets certain privacy principles. In order to join the Safe Harbor, a U.S. company typically must self-certify to the Department of Commerce that it will abide by the Safe Harbor principles. Companies that do so were formerly assumed to meet the Directive's adequacy standard for privacy protection. The EC approved the Safe Harbor agreement in 2000.

On October 6, 2015 the CJEU invalidated the 2000 EC decision approving the Safe Harbor agreement. The Court first determined that even when the EC has concluded that a non-E.U. country has adopted procedures satisfying the adequacy requirements of the Directive, the EC's determination does not prohibit individual E.U. countries' data authorities from examining claims that that country nonetheless is failing to provide an adequate level of protection of personal data. Second, the CJEU, interpreting the adequacy standard to necessitate that a non-EU country receiving E.U. data have privacy laws that are the functional equivalent to those in the E.U., raised several concerns about the Safe Harbor agreement, including recent disclosures about the U.S. government's surveillance activities and the lack of judicial redress in U.S. courts for European citizens' whose data has been collected by the government. Ultimately, the CJEU found that the EC's decision approving Safe Harbor did not comply with the Directive because the Commission did not determine whether the United States ensures an adequate level of protection for personal data. While supporters of the JRA hope that providing legal redress in U.S. courts for European citizens whose data is collected by U.S. companies may be a step toward providing the adequate privacy standards required by E.U. law, the question remains whether the JRA, which is focused on providing a limited number of foreign nationals a cause of action under the Privacy Act for information transferred with respect to transatlantic criminal investigations, would satisfy the CJEU's broader concerns about United States privacy law.

In addition to the Safe Harbor agreement, the JRA is seen as integral to ongoing negotiations between the United States and Europe concerning data transfers in the context of ***law enforcement*** investigations. To that end, the parties have been negotiating the so-called "Umbrella Agreement," which will regulate all personal data exchanged between the United States and the European Union for the purposes of "prevention, investigation, detection, or prosecution of criminal offenses, including terrorism." A critical issue for the E.U. in these negotiations has been access to judicial redress in U.S. courts for European citizens, a provision that was included in the recently released draft agreement. However, it appears that the agreement will not be signed and formalized unless the United States enacts the JRA or a functional equivalent.

Currently, requests and transfers of data between the United States and the member-states of the European Union for purposes of law enforcement investigations are primarily governed by Mutual Legal Assistance Treaties (MLATs) or letters rogatory. Additionally, various other international agreements, such as the Terrorist Finance Tracking Program (TFTP) and the Passenger Name Record (PNR) Agreement, regulate the request and transfer of data between the United States and Europe in the context of law enforcement investigations. The Umbrella Agreement, which is intended to "supplement" but "not replace" these existing international agreements, would create rules governing, among other things, the purpose and use of collected data; transfers to third-party countries; security measures to protect destruction, loss, or disclosure of data; notification of security breaches; and administrative and judicial redress.

(For a more detailed discussion and analysis of the CJEU Safe Harbor decision and the JRA, CRS has published a general congressional distribution memorandum that is available upon request).