January 18, 2016

The U.S. Privacy and Data Protection Framework: Basic Characteristics and Recent Reforms

This briefing paper is intended to assist EU data protection authorities (DPAs), EU and Member State government officials, and others in their evaluation of the legal framework for privacy and data protection in the United States.

The United States has a decentralized, yet robust, legal framework for privacy and data protection.

- **Constitutional protections.** The U.S. Constitution, above all the Fourth Amendment (protecting against government "searches and seizures"), and well-settled U.S. Supreme Court law grounded in the Bill of Rights provide strong baseline protection for privacy and personal information.

- **Federal statutes.** Several federal privacy laws regulate the collection, use and disclosure of information on a sectoral basis, including information in the finance and health sectors; information about children; and information related to consumer credit, insurance, housing, employment, and commercial email. Additionally, the Privacy Act of 1974 protects against the improper use of personal data by government agencies, the Electronic Communications Privacy Act (ECPA) regulates the interception of electronic communications, and the Computer Fraud and Abuse Act (CFAA) imposes criminal penalties on unauthorized access to information stored on computers.

- **Federal Enforcement Authority.** The Federal Trade Commission (FTC) has broad authority under the FTC Act to address "unfair or deceptive acts or practices in or affecting Commerce," and it has used this authority in a variety of privacy and data security contexts to protect consumers by bringing enforcement actions against companies engaging in unfair practices harmful to consumers regarding the collection, use and disclosure of information.

- **State law protections.** There are numerous additional privacy protections under U.S. state law providing an expanded scope of privacy protections, including explicit provisions relating to a right of privacy in several state constitutions, and laws to protect individuals' privacy in various areas, including requiring companies to disclose details of their data sharing with third parties, limiting employer access to employee social network accounts, and security breach notification laws requiring companies to disclose any computer breaches resulting in unauthorized access to consumers' personal data.

Privacy protections extend to surveillance by law enforcement and national security agencies.

- **Protections under U.S. federal case law.** Courts have routinely interpreted the Fourth Amendment and other legal provisions to: (1) restrict the scope and circumstances of law enforcement wiretaps; (2) require a warrant before a national security wiretap; (3) exclude evidence obtained from illegal police searches; and (4) require a warrant before police may search cell phones or use tracking devices, among other protections.

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org

- **Foreign Intelligence Surveillance Act (FISA).** Congress passed FISA in 1978 to govern surveillance activities, including to: (1) establish a Foreign Intelligence Surveillance Court (FISC) (staffed with independent judges with life tenure); (2) require a warrant issued by a FISC judge for electronic surveillance, to ensure high-level approval of narrowly-tailored and targeted requests; and (3) create the Senate and House Intelligence Committees, to provide oversight of the Executive Branch.

- **Section 702 of FISA provides additional protections regarding surveillance of non-U.S. persons.** Section 702 contains important limitations, oversight, and accountability provisions, including FISC approval of surveillance requests only after several safeguards have been met, including that the government: (1) have a valid "foreign intelligence purpose;" (2) follow FISC targeting procedures; (3) use specific identifiers to limit collections and avoid overly broad queries; and (4) employ minimization procedures to destroy raw data between two and five years after collection. Application of these protections to the "PRISM" and "Upstream" programs ensures that collection efforts thereunder are targeted, individualized, and narrowly tailored (e.g., by the government demonstrating the use of "selectors" such as email addresses to ensure collection is not indiscriminate).

The United States has recently implemented several reforms to provide additional protections and safeguards with respect to U.S. surveillance activities.

- **Independent review mechanisms.** Since 2013, the Review Group on Intelligence and Communications Technology ("Review Group") and the Privacy and Civil Liberties Oversight Board ("PCLOB") have provided independent, expert recommendations on how the United States can reform its approaches to surveillance to respect privacy and civil liberties while advancing national security.

- **Presidential Policy Directive-28.** In 2014, President Obama issued Presidential Policy Directive-28 (PPD-28), which requires that all signals intelligence agencies: (1) prioritize the protection of privacy, civil liberties, and personal information of people outside of the United States; (2) provide similar retention and dissemination policies for non-U.S. persons; and (3) limit bulk collection of signals intelligence.

- **USA Freedom Act.** In June 2015, Congress passed the USA Freedom Act, which, among other things: (1) prohibits bulk collection of intelligence information under Section 215 of the PATRIOT Act and other authorities; (2) increases transparency reporting by both companies and the U.S. government, by permitting companies to publish statistics on the national security requests they receive and requiring robust reporting by the U.S. government; (3) codifies the Administration's practice of systematically declassifying FISC decisions; and (4) provides for "expert[s] in privacy and civil liberties" to advise the FISC.

- **Judicial Redress Act.** The Judicial Redress Act, which has passed the House of Representatives and is calendared for consideration in the Senate, extends to EU citizens the same rights that U.S. citizens enjoy under the Privacy Act of 1974 with respect to the data protection obligations of U.S. government agencies.

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org