BertelsmannFoundation

November 15, 2016

The EU-US Privacy Shield Framework – A New Paradigm for an Evolving Digital World*

by Michael McKeon

In the age of Instagram, Facebook, Twitter and Gmail – when one can peruse strangers' selfies and read personal emails of presidential candidates on an iPhone – the very notion of privacy seems obsolete. The Charter of Fundamental Rights of the European Union enshrines respect for one's private life, home and communications, and protection of personal data as basic entitlements for all European citizens. In the United States, legal doctrine has established privacy as a penumbral right, derived, by implication, from protections in the Bill of Rights. When Edward Snowden leaked classified information about the surveillance practices of the National Security Agency (NSA) – some of which included mass collection of U.S. and EU citizens' personal data – public officials and private stakeholders alike were outraged and demanded radical change. The effects of the revelations were widespread and consequential, and still challenge U.S.-EU relations nearly four years later.

Shortly after the Snowden leaks in 2013, the European Commission entered discussions with the United States about acceptable access to and use of European citizens' data. Later that year, Austrian law student Max Schrems filed a case against Facebook Ireland Ltd for the company's alleged involvement in PRISM, an NSA mass surveillance program. The case reached the Irish High Court, which referred the matter to the Court of Justice of the European Union (CJEU). In essence, the case before the CJEU was about whether the U.S.-EU Safe Harbor agreement – a legal framework that had been in place since 2000 to govern the transfer and management of data exchanges across the Atlantic – provided adequate protection of European citizens' personal data, as required by EU law. In October 2015, the CJEU found that Safe Harbor was insufficient in this regard, and consequently rendered the framework invalid.

Over the next four months, the U.S. government and European Commission devised a new framework that would place stricter obligations on U.S. companies that transfer European citizens' data across the Atlantic, create effective redress mechanisms for Europeans who feel that their data have been misused, and limit U.S. public authorities' access to this commercial information. The agreement, dubbed the EU-U.S. Privacy Shield, was made public at the end of February 2016, and was subjected to analysis and scrutiny by European institutions, national Data Protection Authorities (DPAs), industry stakeholders and nongovernmental organizations (NGOs). The European Commission declared in July that the Privacy Shield would provide an adequate level of protection for European citizens' personal data, and U.S. companies began to certify their commitment to its principles shortly thereafter.

An Urgent Search for Improvement

U.S. and EU authorities had no choice but to move quickly to develop a new legal framework for data transfers after the CJEU invalidated Safe Harbor. Beyond the Charter of Fundamental Rights, the EU mandates a high degree of protection of personal data through Directive 95/46/EC. The EU Data Protection Directive, as it is otherwise known, requires entities that process data to do so fairly and lawfully; to collect data for specific and legitimate purposes and not to process them in a way that is incompatible with those purposes; and to maintain

data in a form that allows for identification of the subject for no longer than is necessary to achieve the purpose for which the data were collected. Since 95/46/EC is a directive – an EU legal act that requires a certain end without dictating the means of achieving it – the method and extent of its implementation are left to the member states. Such a scheme allows for nonuniform application of the directive's principles, and thus creates legal uncertainty for companies that transfer and process data outside of Europe. EU and U.S. officials recognized the need to ensure continued commercial access to the European market for U.S. businesses, as well as sufficient personal data protection for European citizens who use American internet sites and platforms.

Furthermore, the trans-Atlantic digital economy is far too large and consequential to have been put on hold while U.S. and EU officials worked to correct the deficiencies of Safe Harbor. The EU-U.S. economic relationship is the largest in the world, with annual goods and services trade exceeding $1 trillion and total investment stocks worth approximately $4 trillion, much of which is brokered and managed via the internet. Unsurprisingly, data flows between the United States and European Union are the largest globally, as well. Both regions export digitally deliverable services valued in the hundreds of billions of dollars, with each serving as the primary consumer market for the other. The free flow of data across the Atlantic is critical not only for internet giants like Google, Amazon and Facebook, but for countless small- and medium-sized enterprises (SMEs). According to eBay, 95 percent of U.S. SMEs that use the online platform to sell their goods and services export to four or more continents; by comparison, less than 5 percent of U.S. businesses that export offline claim the same reach.[1] Though highly unfeasible, halting or even slowing trans-Atlantic data flows to a significant degree – even if only for a brief period to ensure adequate protection of personal data – would create tremendous negative economic consequences, both in and far beyond Europe and the United States.

Finally, European and American officials renegotiated the data protection framework with urgency to allow for the continuation of certain intelligence-gathering activities of the U.S. government. Although the 2013 revelations regarding the reach and indiscriminate nature of some U.S. surveillance programs were a key impetus behind the dismantling of Safe Harbor, U.S. and European officials alike recognized that some intelligence programs were both legitimate and necessary for countering terrorism, organized crime, human trafficking and other threats. Wholly restricting access to online data was a nonstarter for the United States. The European Commission and EU member states such as the United Kingdom and France, which actively share intelligence with the United States and rely on its reciprocity, did not want to lose this invaluable resource either. U.S. and EU leaders sought to strike a balance by maintaining intelligence programs that had a clearly definable purpose while, at the same time, protecting the rights and civil liberties of European citizens.

New Obligations and Unprecedented Commitments

In short, the Privacy Shield is a legal framework codified through the European Commission's Implementing Decision of July 7, 2016 and explanatory notes and commitments from the U.S. Department of Commerce, Department of State, Department of Transportation, Federal Trade Commission and the Office of the Director of National Intelligence. The framework lays out a set of Privacy Principles that entities must follow when processing European citizens' personal data. The principles ensure greater transparency for users and create new obligations for data processors, both in relation to their own activities and vis-à-vis onward transfers, or the passage of personal data to other organizations for further processing and/or storage. The principles also establish oversight mechanisms to ensure that entities abide by the Privacy Shield rules, and threaten sanctions for noncompliance.

Although participation in the Privacy Shield is voluntary, once a company certifies as compliant with the framework, its obligations are legally binding. An entity must commit to follow the principles and publish its adherence to the Privacy Shield on its website, and provide links to government sites that further explain the framework, users' privacy rights and access to redress mechanisms. Companies registered under the Privacy Shield framework are also responsible for how their partner organizations process or store personal data. If an entity transfers data to a third party, it must ensure that the party follows the principles as well, and is legally liable if the partner organization does not. Under the Privacy Shield, a U.S. company must provide its own redress mechanism to users who feel that their data have been mishandled. This is the first of several recourse mechanisms available to European citizens, and obligates companies to respond to complaints within 45 days.

If direct redress with an offending entity is unsuccessful, an individual may bring his complaint to an independent dispute resolution body – either in the United States or the European Union – that is predesignated by the company to investigate and resolve complaints and provide recourse options free of charge to the claimant. As part of its compliance review procedures, the U.S. Department of Commerce will verify that U.S. companies operating under the Privacy Shield have, in fact, registered with the independent dispute resolution bodies that they claim.

A European citizen who believes his data have been compromised or mishandled may also file a complaint with one of the national DPAs, which oversee execution of the EU Data Protection Directive in the EU member states and the European Economic Area. In cases related to human resources data, U.S. entities are legally obliged to cooperate fully in the DPA investigation and resolution of a complaint. The recommendations of DPAs are delivered through informal DPA panels established at the EU level. Litigating parties may comment and provide evidence, if they wish, and the panel will deliver its recommendations for action within 60 days of receiving a complaint. DPAs may also forward a European citizen's claim directly to the U.S. Department of Commerce or the Federal Trade Commission for investigation and enforcement action. If none of the aforementioned redress mechanisms resolve a European citizen's complaint, the data subject may invoke binding arbitration by the Privacy Shield Panel, made up of three arbitrators out of a pool of at least 20, selected by the U.S. Department of Commerce and the European Commission.

Perhaps the most significant feature of the Privacy Shield framework is written assurance from the U.S. government that access to personal data by public authorities is subject to clear limitations, safeguards and oversight mechanisms. U.S. President Barack Obama has directed the U.S. intelligence community, working through two legal instruments – Executive Order 12333 (EO 12333) and Presidential Policy Directive 28 (PPD-28) – to scale back signals intelligence operations in a number of meaningful ways. Intelligence collection must be based on statute or presidential authorization, for example, and must include safeguards for the personal information of all individuals, regardless of nationality or country of residence. These legal instruments seek to focus intelligence collection as precisely as possible, in order to prevent the type of mass, indiscriminate accumulation of personal data that compelled the CJEU to reject Safe Harbor in the first place. In the event that the United States does deem the bulk collection of signals intelligence to be necessary, PPD-28 limits such action to six national security purposes related to the detection and countering of threats such as espionage, terrorism and weapons of mass destruction. Furthermore, European data subjects can challenge the collection and use of their data through the Privacy Shield Ombudsperson, a newly created office within the U.S. Department of State that will field and address such complaints.

Presidential Policy Directive 28 provides that signals intelligence collection in bulk is limited to:

- Detecting and countering certain activities of foreign powers
- Counterterrorism
- Counterproliferation
- Cybersecurity
- Detecting and countering threats to U.S. or allied armed forces
- Combating transnational criminal threats, including sanctions evasion

The lengths to which the U.S. government has gone to guarantee a high level of protection for European citizens' personal data affirms the importance it places on the trans-Atlantic economic relationship. The Privacy Shield creates new obligations for the U.S. government and grants non-U.S. citizens access to information and agencies in an exceptional way. Furthermore, the framework places new burdens on U.S. businesses, some of which may prove to be costly, time-consuming and unpopular. The potential consequences of interrupting data flows across the Atlantic were too great to ignore, and the Obama administration responded creatively to continue engagement within both U.S. and EU law.

Uncertainty Ahead

As of mid-October 2016, more than 1,500 companies had submitted self-certifications to the U.S. Department of Commerce to operate within the framework, and more than 500 had been approved and added to the department's public Privacy Shield List. Although these numbers seem promising, since registration opened only a few months ago, they are far below the approximately 4,500 companies that had operated under Safe Harbor.

According to an August 2016 survey by the International Association of Privacy Professionals, only 34 percent of companies polled reported intent to register with the Privacy Shield, preferring to rely on other data-transfer mechanisms such as standard contractual clauses or binding corporate rules. Some companies may be slow to register out of an abundance of caution, in order to ensure that they meet the new standards and obligations before self-certifying, and thus avoid liability for unforeseen or accidental mishandling of data. Others, particularly small businesses, may not consider participation in the Privacy Shield to be worth the effort of registering with dispute settlement bodies, having to respond to and comply with European DPAs, or taking on the risk of potentially costly arbitration. Still others may be waiting to confirm that the Privacy Shield can withstand legal challenges. Critics of the framework, including Schrems and organizations such as Digital Rights Ireland and the European Consumer Organization (BEUC) claim that the Privacy Shield operates on uncertain legal grounding and does little to prevent U.S. authorities from using loopholes to collect mass data. Furthermore, the legal instruments limiting U.S. intelligence agencies' access to Europeans' personal data (EO 12333 and PPD-28) are not legislative acts, and therefore can be dismantled by the next U.S. administration with relative ease.

Regardless of how effectively the Privacy Shield or any other framework protects European citizens' personal data, it is certain to be highly scrutinized and challenged by stakeholders on both sides of the Atlantic. The 2013 revelations about U.S. surveillance activities linger in the minds of consumers, business competitors and political leaders, and have sown distrust of the U.S. government and internet companies among European citizens. The EU's legal landscape for digital issues is changing as well, most notably through the European Commission's General Data Protection Regulation (GDPR), which is expected to become law in May 2018. The GDPR – notably a regulation, which, as opposed to a directive, must be implemented in the member states as it is written – will strengthen data protections for European citizens and standardize practices across the EU member states. It will almost certainly have implications for the export of Europeans' personal data, and will therefore bear directly on the Privacy Shield.

Although uncertainty remains regarding the legality and potential longevity of the Privacy Shield, most policymakers, industry actors and civil society stakeholders agree that an effective scheme to govern the transfer and management of data between the European Union and United States is necessary, and that the current framework is a step in the right direction. Trans-Atlantic trade and investment underlie the global economy, and must operate within fair and clear legal frameworks for businesses and consumers alike. Realistically, the United States must collect intelligence to protect and advance its own interests and those of its allies. And, at the root of the Privacy Shield debate, citizens' rights – whether explicit or implicit – must be upheld to the greatest extent possible. The framers of the Privacy Shield sought to strike this balance and must be prepared to respond to the inevitable challenges ahead.

Michael McKeon is project manager for transatlantic relations at the Washington, DC-based Bertelsmann Foundation. *Michael.McKeon@bfna.org*

*This is the first in a series of upcoming analyses by the Bertelsmann Foundation on the digital economy.

[1] eBay 2015 US Small Business Global Growth Report, available at http://www.ebaymainstreet.com/sites/default/files/2015-us-small-biz-global-growth-report.pdf