BROOKINGS

Report

The oracle at Luxembourg: The EU Court of Justice judges the world on surveillance and privacy

Cameron F. Kerry Monday, January 11, 2021

In a July 2020 judgment, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield Framework, the main vehicle to allow transfers of personal data from the European Union to the United States. This decision focused on transatlantic transfers, but it has reverberations for EU digital trade everywhere.

This ruling was the second time in five years that the CJEU considered U.S. intelligence surveillance on the basis of the EU's Charter of Fundamental Rights, which enshrines both "private life" and "protection of personal data" into basic law. In 2015, the CJEU invalidated the predecessor of the Privacy Shield, the U.S.-EU Safe Harbor agreement, faulting the European Commission for failing to assess the potential impact of American government surveillance on personal data transferred from the EU. After the U.S. Department of Commerce and European Commission arrived at the Privacy Shield to address the CJEU's first judgment, the CJEU ruled that legal authorities, limitations, and remedies for surveillance under U.S. law do not comply with those required by the Charter and invalidated the Privacy Shield as well.

The CJEU's Privacy Shield decision (known as *Schrems II* after the Austrian lawyer-activist Maximilian Schrems who initiated the series of cases) reflects the CJEU's use of its authority as the final arbiter of EU legislation and Commission decisions as an instrument to curb government and private sector surveillance. The court has accorded privacy and data protection primacy among EU fundamental rights, comparable to American reverence for the First Amendment to the U.S. Constitution (or the Second Amendment by some lights). Even though the Charter and the EU's foundational treaty both circumscribe the

EU's authority over member states in matters of national security, in *Schrems II* the CJEU invoked the Charter to interpret EU data protection legislation as applying to U.S. surveillance of communications for national security and law enforcement purposes.

"In all, the *Schrems II* judgment extends the bounds of the EU's exceptionalism regarding data protection."

In all, the *Schrems II* judgment extends the bounds of the EU's exceptionalism regarding data protection. It overrode the Commission's accommodation of EU interests in sustaining the Union's most important trading relationship, sovereign interests of the U.S. and other governments in protecting security, and differences between American and European legal systems. The outcome sets a high bar for any new data transfer arrangement between the U.S. and EU.

The judgment also raises questions for other mechanisms widely used by companies in Europe to transfer personal data all over the world. Regulators have begun to address these questions and their actions indicate that, while data flows may continue to certain countries and in some circumstances, others may be deemed too risky. This perception of risk will lead regulators and companies to keep the data within the EU—de facto and at times explicit data localization. The resulting trade friction will be felt in EU relations not only with the United States but also with other trading partners.

JUDGING THE "ADEQUACY" OF THE UNITED STATES

The CJEU has greater leverage over U.S. intelligence practices than those of member states by virtue of the EU's far-reaching General Data Protection Regulation (GDPR). The GDPR generally limits transfers of personal data from EU member states to non-EU states, or "third countries," unless the Commission has issued an "adequacy" decision—a finding that the legal protections afforded to the transferred data in the third country are "essentially equivalent" to those in the EU.

The Privacy Shield and its predecessor, the 2000 Safe Harbor framework, were more limited adequacy decisions tailored to the U.S. Because the U.S. has only sectoral federal privacy and various state laws with no comprehensive federal privacy law comparable to the GDPR, the European Commission and U.S. Department of Commerce filled in the gaps with principles that reflect EU data protections. Subscribing companies incorporated these principles into their privacy policies, making them legally enforceable by the U.S. Federal Trade Commission. This enabled such companies to transfer EU personal data to the U.S. without an across-the-board adequacy determination.

The challenges to the Safe Harbor and Privacy Shield reflect intense European reaction to the Edward Snowden leaks about U.S. surveillance. The 2015 case amounted to a hypothetical opinion—based on bare allegations derived from news stories about the leaks, with no party appearing to contradict these allegations. In its decision, the CJEU postulated that legislation permitting collection of "all the personal data of all the persons whose data has been transferred from the European Union to the United States" or not providing "any possibility for an individual to pursue legal remedies in order to have access to personal relating to him" would clearly violate the "essence" of the fundamental rights of private life and data protection. Rather than finding that U.S. legislation is actually so sweeping, though, the court faulted the Commission for failing to investigate and exclude such possibilities in approving the Safe Harbor framework.

The second time around, the CJEU was presented with extensive facts. For its decision approving the Privacy Shield in 2016, the European Commission developed a sophisticated understanding of U.S. law, and incorporated submissions from the U.S. that describe in detail legal authorities, practices, and safeguards for government surveillance. The late and revered Giovanni Buttarelli, as the EU's top data protection official, later called these disclosures a "remarkable" statement unlike anything another government has done.[1] In addition, multiple parties joined the case, including Facebook (a defendant), an international array of business and civil society organizations, and the U.S. government. The record before the CJEU included hundreds of pages of testimony from experts in U.S. law and lengthy findings from the referring court in Ireland.

“For its decision approving the Privacy Shield in 2016, the European Commission developed a sophisticated understanding of U.S. law”

Against this backdrop, the CJEU ruled, first, that legal authorities for U.S. governmental intelligence collection “cannot be regarded as limited to what is strictly necessary” in accordance with a Charter requirement that restrictions on fundamental rights be “necessary and proportionate in a democratic society,” and second, U.S. law does not provide a judicial remedy for individuals to challenge or investigate surveillance that involves them.

At the time of this decision, some 5,300 U.S. and European companies were using the Privacy Shield to transfer data to the U.S. Even more relied on “standard contractual clauses” (SCCs), also addressed in the CJEU judgment, which attach legal obligations to personal data exported to third countries without adequacy decisions. These are the most widely used mechanism for data transfers, employed by a great majority of companies doing business in the EU, with European companies comprising 75% of the users. In the absence of the Privacy Shield or any replacement, U.S. companies and others will have to rely on SCCs and similar mechanisms for data transfers to the U.S.

The CJEU upheld the basic validity of the SCCs. But there is a catch: companies themselves have to evaluate the risk that data will be subject to government surveillance. The CJEU interpreted the GDPR as obligating companies that use SCCs to export and import personal data from the EU to any third country without adequacy must consider, on a case-by-case basis, whether they are able to comply with SCCs in light of third country laws on governmental access. If not, these companies—and ultimately member state data protection authorities—are obligated to suspend or terminate the data transfers involved.

The CJEU blithely concluded that giving immediate effect to its invalidation of the Privacy Shield would not result in any "legal vacuum." Nonetheless, the combined reality of abruptly throwing Privacy Shield transfers into legal limbo and the need for wholesale review of SCCs by regulators as well as companies leaves data exporters dangling as they sort through how to square their data transfers with *Schrems II*. Since then, EU data protection commissioners, the European Commission, and U.S. government all have sought to provide this case-by-case assessment, but these are not final and many companies lack the resources and capacity to evaluate the laws of foreign countries.

Both the U.S. and the European Commission have responded matter-of-factly, announcing that they are discussing an "enhanced" data transfer framework to replace the Privacy Shield. As the EU's lead negotiator subsequently put it, there are "no quick fixes." In the meantime, however, the CJEU's rulings on existing U.S. intelligence collection authorities, remedies, and subsequent actions by data protection authorities raise doubts about whether compliance with SCCs for many transfers to the U.S. are possible.

"the CJEU's rulings … raise doubts about whether compliance with SCCs for many transfers to the U.S. are possible."

First, the Irish Data Protection Commissioner initiated a proceeding that question whether Facebook—and perhaps any company—can store personal data from EU residents in the U.S. Then, the French data protection regulator recommended against storage of a national health data aggregation on Microsoft's Azure cloud service on the basis of *Schrems II* and, while the French State Council allowed the contract, it relied largely on a contractual agreement by Microsoft not to transfer health data outside the EU and the government's announcement that it wants to transition to a provider from France or elsewhere in the EU. The EU's data protection law and *Schrems II* have been described as "soft data localization"; the French health data case steps over into hard data localization.

Finally, the collective body of EU data protection authorities, the European Data Board (EDPB), issued recommendations on "additional safeguards" that the GDPR and *Schrems II* permit for transfers to countries without adequacy determinations. This complex bundle of compliance steps, use cases, and suggested contractual measures leaves a door open for some transfers to the U.S. and elsewhere provided the data is secured with tools like encryption. But it also lays out scenarios that "would not be effective" and twice cites the CJEU's ruling that Section 702 of the Foreign Intelligence Surveillance Act (FISA) "goes beyond what is necessary and proportionate in a democratic society" in terms that imply that any transfer where there is the slightest risk that data transferred might fall into the hands of governments agencies would violate EU law, including a range of cloud services hosted in the U.S. that are used in the clear.

This categorical approach appears at odds with proposed revised SCCs that the Commission issued one day after the EDPB's recommended measures, which incorporated a more nuanced risk-based approach. To inform risk assessment, the U.S. government earlier issued a white paper to give some clarity on categories of data that are unlikely to be targets of surveillance and on safeguards under FISA. The EDPB may have been reacting to these in dismissing "subjective factors" such as the likelihood of government access to particular data.

The GDPR confers decisionmaking power on adequacy and any new EU-U.S. framework on the Commission, and this would not be the first time the Commission and the data protection regulators have disagreed. In both *Schrems* cases, though, the CJEU has sided with the regulators. In this light, their restrictive interpretation has to be regarded a harbinger of how the CJEU is likely to treat data transfers to the U.S. as well as other nations with active intelligence programs.

In the end, the continuation of important data flows across the Atlantic will require a new U.S.-EU framework to take the place of the Privacy Shield. Arriving at a framework that can satisfy the CJEU will challenge both the European Commission and the U.S., but neither can afford a third strike in court. Even if the U.S. and European Commission are

able to reach a political agreement on a framework before January 20, 2021, the process of review and final adoption will carry over into 2021 and will be high on the agenda for U.S.-EU relations for the Biden-Harris administration.

APPLYING ADEQUACY TO THE WHOLE WORLD

The United States is not alone in dealing with the impact of the *Schrems II* decision. The ruling gives rise to uncertainty for many EU trading partners and any EU companies involved in international commerce.

"The ruling gives rise to uncertainty for many EU trading partners and any EU companies involved in international commerce."

Countries that have existing adequacy determinations and also operate intelligence programs (such as Argentina, Canada, Israel, and New Zealand) have already faced reviews of these determinations in the wake of the 2015 decision. Now such reviews will be shaped by *Schrems II*. In addition, both South Korea and the UK (now that it is separate from the EU) are currently pursuing adequacy determinations, a path which India and other countries also have been exploring. Any further adequacy decisions will require the same scrutiny of government intelligence programs. For Canada, New Zealand, and the UK, this inquiry will encompass their cooperation with the U.S. in the Five Eyes intelligence alliance.

The decision also raises open-ended questions for transfers of data from the EU to most of the rest of the world, which also rely on SCCs and other mechanisms subject to the same obligations. Under the GDPR, these enable cross-border data transfers in the absence of an adequacy determination. Even so, the CJEU's ruling declared that companies and data protection authorities must ensure that these mechanisms sustain "a level of protection essentially equivalent to that guaranteed within the European Union …." This grafts the

same high standard for adequacy determination onto mechanisms that, by their terms, are meant for transfers to countries that have *not* been found adequate—thereby injecting the EU's adequacy requirement into all data transfers to all countries in the world.

Transfers to China, Russia, and other repressive and authoritarian states raise obvious questions. The EU, notably, is China's largest trading partner. The resulting data flows can include the personal data of EU employees of Chinese companies, of travelers, and of the increasingly global users of WeChat, TikTok, and other applications developed in China. It is difficult to assess foreign laws, especially those that are state secrets, and it is absurd to expect that any data exporter can achieve a fraction of the understanding necessary, or that an importer in China or Russia will declare that its government's intelligence collection inhibits compliance with SCCs. Yet China's surveillance state has become so notorious that it would take willful blindness on the part of an EU data exporter to avoid questioning if it can protect that data from the Chinese government. EU companies and regulators have to consider the extent to which data flows to such countries are sustainable in light of *Schrems II*, and language in the EDPB's recommendations about taking into account "technical, financial, and human resources" at governments' disposal seem directed at China or Russia as much as the United States.

The CJEU also altered the decisionmaking process for adequacy decisions. In the Safe Harbor decision, it took pains to say its "essentially equivalent" standard to judge adequacy does not equate to "a level of protection identical to that guaranteed in the EU legal order." In *Schrems II*, however, adequacy equated to "compliance" with provisions of the Charter of Fundamental Rights. In addition, as leading EU privacy expert Christopher Kuner has pointed out, although the GDPR delegates adequacy decisions to the European Commission, the CJEU shifts this decision for SCCs from the Commission to the companies that export and import data, and ultimately the data protection authorities.

Furthermore, *Schrems II* has implications for EU member states that engage in surveillance of their own. The CJEU found that judicial warrants issued under FISA for authorizing "programs" based on selection criteria rather than targeting of specific individuals, and the U.S. reservation of the potential to collect "bulk" signals intelligence in circumstances where it cannot target as too open-ended "cannot be regarded as limited to what is strictly

necessary." Yet a thorough review by the EU's Fundamental Rights Agency (FRA) shows that many EU member states conduct national security and law enforcement surveillance at least as broad as that of the U.S., and often with fewer safeguards. These include "large-scale technical collection of intelligence," collecting streams of communications to which they apply "search terms" and "catchwords" rather than target specific individuals.

The CJEU considered such practices this October in cases involving legislation in Belgium, France, and the UK. Each case involved large-scale government data collection from providers of electronic communications, and all presented arguments from a majority of member states that, because the surveillance was for national security or law enforcement reasons, was a matter left to the sole responsibility of the member states under the EU's constitutional order. In each case, the CJEU held that EU law governs what information member states can require communications providers to turn over and precludes "general and indiscriminate" government collection and retention of traffic, location data, and other metadata.

This ruling was enough to preclude UK intelligence agencies' wholesale collection of communications data communications providers to identify and analyze previously unknown threats, consistent with its treatment of "bulk surveillance" in *Schrems II*. The court gave this broad principle more nuanced application in the cases of Belgium and France, however, allowing for exceptions according to the nature of the threat and the safeguards in place to limit collection and retention to what is necessary to address that threat. Such safeguards would allow states to conduct general and indiscriminate data collection for a sufficiently severe and immediate threat as well as to investigate "serious" crimes that are limited in time or location and targeted to objective and non-discriminatory categories of people, all subject to independent judicial or administrative review.

The cases provide notable counterpoints to the Privacy Shield case. First, the kinds of bulk surveillance allowed in Belgium and France more closely resemble the pre-Snowden collection of bulk domestic telecommunications metadata, which the United States eliminated with the USA FREEDOM Act in 2015, than any of the continuing U.S. programs the CJEU discussed in connection with the Privacy Shield. Second, the court's more

nuanced consideration of surveillance reflected greater deference to the member states' sovereign interests and to safeguards against abuse of surveillance. It referred to jurisprudence of the European Court of Human Rights (ECHR) in Strasbourg on government surveillance that affords states a "margin of appreciation" in deciding how to balance the protection of order and national security with necessary guardrails. In contrast, in *Schrems II* the CJEU rejected that jurisprudence as inapplicable and brushed aside ways that the U.S. employs safeguards like those discussed in the Belgium and France cases.

It is tempting—but futile—to say the CJEU got it wrong. As Supreme Court Justice Robert Jackson famously said of his court, though, "we are infallible because we are final." The CJEU has spoken—and the EU, the U.S., and the many companies that transfer EU personal data across the Atlantic and elsewhere around the world must deal with it.

"The CJEU has spoken—and the EU, the U.S., and the many companies that transfer EU personal data across the Atlantic and elsewhere around the world must deal with it."

WHAT COMES NEXT

As the U.S. administration and European Commission negotiate another data transfer arrangement, the stakes on both sides are significant. With transatlantic data flows vital to both economies, the EU cannot afford to become a data island, nor the U.S. a data pariah. Together, the U.S. and EU comprise more than one-third of the world's GDP, and the EU member states collectively are the largest U.S. trading partner. The U.S. and EU are also the most digitally-interconnected regions of the world, with cross-border data flows 50 percent greater than those between the U.S. and Asia and almost double those between

the U.S. and Latin America. The global digital economy has kept growing even when the overall economy has not and, in the wake of the COVID-19 pandemic, this growth and connectivity matter more than ever.

The U.S. and EU also need each other in other ways—despite distrust of multilateral organizations on the part of the Trump administration or ambitions for "strategic autonomy" on the part of some European leaders. Amid a changing world order, each could be the other's most potent ally on pressing global issues, with the two unions by themselves creating a strong coalition of likeminded countries. As former U.S. Ambassador to the EU Anthony Gardner argues, the U.S. and EU are "essential partners." A robust and stable U.S.-EU agreement on data flows will help to put this key relationship on a stronger footing.

Achieving such an agreement is likely to require U.S. legislation. It may be possible to put in place additional safeguards and remedies through a combination of executive orders, administrative regulation, and interagency agreements that can be accomplished more easily than legislation. In the long run, though, such steps are likely to face the same fate as the Privacy Shield. As civil law judges, the CJEU in *Schrems II* took as complete and definitive statutory text described in the Commission's Privacy Shield decision and expected legislation to "lay down clear and precise rules" for safeguards. As a result, the judgment gave short shrift to U.S. executive orders or regulations (which the court's Advocate General's advisory opinion dismissed as "internal administrative directives [that] do not constitute law") and found FISA and Executive Order 12333 (EO 12333) lacking in clear and precise rules for "minimum safeguards" required under the Charter of Fundamental Rights.

Despite this constrained view of U.S. law, the CJEU's more recent prescription of safeguards for member states that conduct "general and indiscriminate" surveillance presents a clear roadmap to legislation. It clarifies that bulk surveillance can be permitted if it is based on demonstrably serious threats and is sufficiently circumscribed. It provides guidance on national legislation and remedies in the EU. In 2015, in the private practice of law, I led a transatlantic team of lawyers who examined surveillance authorities in various member states (including the UK, Belgium, and France) with a view to establishing an "EU

benchmark" by which to compare the U.S. under the CJEU's "essentially equivalent" standard for adequacy. Now the CJEU has provided authoritative benchmarks to point to in future litigation.

"the CJEU's more recent prescription of safeguards for member states that conduct 'general and indiscriminate' surveillance presents a clear roadmap to legislation."

Meeting this standard should be achievable because the United States already has clear and precise rules that provide important safeguards described in these benchmarks. The layers of executive orders, regulations, and administrative procedures that have fleshed out FISA and EO 12333 include regulations from the Attorney General and Department of Defense and agency administrative controls aimed at ensuring compliance and preventing abuses of surveillance powers. In turn, the Foreign Intelligence Surveillance Court (FISC) approves procedures to select targets and supervises compliance with these procedures. In the wake of the Snowden leaks, intelligence agencies have radically increased transparency, declassifying much of these procedures and FISC opinions and posting on the Tumblr website *IContheRecord*.

In 2014, moreover, President Obama's Presidential Policy Directive 28 (PPD-28) declared that "all persons should be treated with dignity and respect, regardless of their nationality or where they might reside." In extending the protections for U.S. persons to others outside national borders, this declaration established a new international norm. As a group of international experts (funded by the EU) found in 2015, "few if any countries—democratic or otherwise—offer the kinds of protections for foreign nationals subject to their intelligence gathering operations that are now being demanded of the US government," and "the US now serves as a baseline for foreign surveillance standards."

Putting this baseline into law by codifying PPD-28 and major elements of the regulations and procedures that govern intelligence agencies would underscore this leadership. Legislation should make clear that FISC approval of targeting criteria and procedures for data minimization encompasses non-U.S. persons, clarify the aims of surveillance, and codify in broad terms existing processes for documenting and approving the reasons for individual targeting, retention and dissemination of information, and supervision by the Department of Justice and the FISC. These should include the requirement of a "reasonably articulated suspicion" as a basis for targeting specific queries, a standard derived from constitutional law under *Terry v. Ohio*. Expressing such requirements in legislative text should demonstrate that targeting is done, in the words of the CJEU, "on the basis of objective and non-discriminatory factors," limited to what is necessary in relation to the threats presented, and subject to judicial oversight.

Amending surveillance authorities is relatively complex and sensitive, and passing any legislation is never easy and perhaps even less so where it involves making nice to Europeans. Nonetheless, Congress has acted before to change U.S. law to enable transatlantic data flows, extending the federal Privacy Act to EU citizens in 2015 as an explicit condition of an "umbrella agreement" on privacy and data protection for personal data exchanged by law enforcement agencies. Codifying existing procedure rather than extending new protections scarcely amounts to a concession.

Moreover, there are reasons to revisit U.S. surveillance authorities independent of data flows from Europe. FISA was enacted in 1978 and EO 12333 signed by President Reagan in 1983. Since then, FISA has been amended from time to time, but EO 12333 scarcely at all. Four years ago, in a thoughtful agenda for surveillance policy in the next administration, the Center for New American Security wrote that "surveillance reform is a work in progress rather than a product." This work has seen little progress since. With billions of devices revealing everything about individual lives constantly connected to digital communications networks, the global reach and acuity of surveillance has grown beyond anything imagined when FISA and EO 12333 were adopted. It is time to update these authorities for the 21st century and "submit facts to a candid world" about how U.S. intelligence surveillance actually operates.

“With billions of devices revealing everything about individual lives constantly connected to digital communications networks, the global reach and acuity of surveillance has grown beyond anything imagined when FISA and EO 12333 were adopted.”

While codifying existing safeguards into law would express on the face of statutes how surveillance has operated and clarify protections for people outside the U.S., establishing an individual judicial remedy for unlawful surveillance would extend new protections both to people outside the U.S. and to U.S. persons. Although there are statutory remedies that can apply to unlawful surveillance, the constitutional requirement to show concrete injury in order to establish standing to sue in federal court, combined with the secrecy of U.S. intelligence agencies, ultimately makes it hard to prove surveillance in individual cases. The CJEU called these constraints on remedies “a lacuna” insufficient to satisfy EU fundamental rights.

Here again, the CJEU’s October 2020 judgment on member state surveillance laws is instructive. The *Schrems II* judgment appeared to conflate two different data protection remedies. One is access and rectification, a right to see and correct individual records, and the other is judicial recourse to challenge the lawfulness of the processing of personal data. In the member state cases, the CJEU described notification of individuals who are subject to surveillance as necessary to enable both access and rectification of personal data and judicial review.

The member state judgment makes clear that administrative remedies can provide an avenue for access and rectification while protecting the secrecy of ongoing investigations or operations. The French Internal Security Code reviewed in the judgment enables individuals to ask an oversight board whether any unlawful intelligence surveillance has been used against them. The board then verifies the legality of any surveillance that has

occurred "without confirming or denying" its existence (similar to the function that was performed by the Privacy Shield ombudsperson). The court also made clear that neither notification nor access and rectification of surveillance data is unconditional in the national security context. Individuals need to be notified "to the extent that and as soon as it is no longer liable to jeopardize the tasks for which authorities are responsible," and only when they are specifically identified for analysis.

Although U.S. legislation that provides similar remedies for intelligence surveillance would be a significant extension of existing rights, it would find roots in existing U.S. law. The Fourth Amendment and the Wiretap Act require subsequent notification of wiretaps regardless of whether they result in a prosecution, and various provisions of FISA require notification if the government intends to use the information in a court proceeding. The U.S. Court of Appeals for the Ninth Circuit has held that the Fourth Amendment notice requirement extends to surveillance under Executive Order 12333 as well. Such notification affords individuals the opportunity to vindicate their Fourth Amendment protection and exercise their Sixth Amendment right to confront evidence against them. Similarly, notification to persons who have been identified by surveillance would not jeopardize ongoing intelligence collection and would address what has been the greatest obstacle to judicial review of surveillance: a concrete basis to believe the plaintiff has been subject to surveillance. And where notification is not in order, the availability of independent administrative review that peeks behind the curtain without disclosing what is there could provide a check on the lawfulness of surveillance.

Prior judicial review of the scope of surveillance of non-U.S. persons and subsequent review of individual cases should be limited by a reciprocity requirement, applying only to people whose governments extend equivalent rights to U.S. nationals. This restriction is comparable to the way the Judicial Redress Act operates for rights under the federal Privacy Act—and the CLOUD Act does for government access to electronic evidence stored on offshore servers. Such reciprocity would underscore the new norm the U.S. is setting and push other governments—the EU included—to adopt this norm. It also would ensure that the United States does not need to treat North Korea, say, the same way it does the EU.

Although neither *Schrems* case addressed privacy in the U.S. private sector, passage of separate comprehensive federal privacy legislation also would help enable a new U.S.-EU data transfer framework. The United States is currently the only advanced democracy without such a law. Instead, it has a matrix of sectoral laws covering health information, financial records, student records, video viewing, and many other specific applications. But this approach leaves much of the constant streams of data from smartphones, computers, and other connected devices unprotected, allowing many companies to set their own rules for what data they collect, how they use it, and who they share it with.

Because of this gap in privacy protection and the reach of government and corporate information collection, the United States is widely perceived as an outlier in protection of personal information—a digital Wild West. By enacting a comprehensive law, Congress can help change this perception, filling the growing gap between existing laws and the explosion of data and affirming America's longstanding privacy values. It is conceivable that, coupled with the changes to surveillance law discussed above, baseline privacy legislation could open the door to a full adequacy determination for the U.S. that would put an end to unstable gap-fillers.

AMERICA'S OWN CHALLENGE

The European Union's data protection exceptionalism stems in part from perceptions —a narrative of its own history, attitudes toward the U.S. and technology, and cognitive dissonance in how Europeans think about law compared to Americans. Despite these perceptions, America has privacy values deeply embedded in our law and culture. In turn, rights affecting privacy have been subjects of a transatlantic conversation going back to revolutionary times when Thomas Jefferson helped with the drafting of France's Declaration of the Rights of Man and the Citizen as his compatriots were debating a new constitution and bill of rights. Louis D. Brandeis is credited with first articulating a legal right to privacy, not only in the U.S. but also in European legal thought, even though he himself drew on French and German sources. The U.S. Fair Credit Reporting Act in 1969 is one of the first national privacy laws anywhere, the U.S. Department of Health, Education & Welfare developed the fair information practices that evolved into EU data protection law, and some GDPR provisions trace their origin to U.S. privacy practices.

“It is time for the United States to reassert leadership; diminish the differences between it, the EU, and the more than 100 countries that have adopted similar laws”

In recent years, the EU has taken the initiative in privacy and data protection. It is time for the United States to reassert leadership; diminish the differences between it, the EU, and the more than 100 countries that have adopted similar laws; align itself with likeminded democracies that treat privacy as a fundamental right; and lead an honest discussion with these counterparts on norms for surveillance necessary to protect democratic states. The U.S. needs to ensure that technologies and data are used in ways that respect human dignity and autonomy and sustain the international data flows and trust in American companies essential to competing in a global digital economy. Reaching a stable framework for transatlantic data flows is an essential step, and the United States should prepare to pass legislation that will pave the way.

Report Produced by **Center for Technology Innovation**

Footnotes

1. 1 Author’s notes from panel discussion preceding International Conference of Data Protection and Privacy Commissioners, Brussels, October 23, 2018.