3-10-2021

EU Privacy Law and U.S. Surveillance: Solving the Problem of Transatlantic Data Transfers

Peter Margulies
Roger Williams University School of Law

LAWFARE

CROSS-BORDER DATA

EU Privacy Law and U.S. Surveillance: Solving the Problem of Transatlantic Data Transfers

By **Peter Margulies**, **Ira Rubinstein** Wednesday, March 10, 2021, 11:51 AM

The July 2020 decision of the Court of Justice of the European Union (CJEU) in *Data Protection Commissioner v. Facebook Ireland, Ltd. and Maximilian Schrems* (*Schrems II*) was both a landmark in privacy law and a major obstacle for international trade. The *Schrems II* court cited the breadth of U.S. surveillance in holding that the EU-U.S. Privacy Shield agreement on transatlantic data transfers failed to provide adequate safeguards for the privacy of EU persons' data. This meant that Privacy Shield violated the EU's robust privacy law, the General Data Protection Regulation (GDPR). Both the European Commission—the EU's executive arm—and the United States are now seeking a resolution that will allow data transfers while protecting privacy.

The viability of transatlantic data transfers is a pressing and pervasive problem. Tens of thousands of companies depend on transatlantic data transfers. A halt to data flow would undermine the business models of countless firms.

Unfortunately, most current approaches to resolving the EU-U.S. conflict fall short. The Trump administration sought to wish away the conflict, as in this white paper by the Department of Commerce. The approach of the European Data Protection Board (EDPB) insists on rigid technological fixes that will severely hinder most transatlantic transfers of personal data. In a new article, we offer a hybrid approach that incorporates both substantive and institutional safeguards and a pragmatic assessment of the real-world risk of U.S. surveillance for particular data. Here, we'll describe some of the suggestions we make in the paper and the dynamics that underlie the problem.

The CJEU's concerns started with Edward Snowden's 2013 revelations about U.S. surveillance. In the EU, worry about the scope of U.S. surveillance centered on two U.S. measures: § 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333. U.S. surveillance officials may target the communications of persons or entities reasonably believed to be located abroad to obtain "foreign intelligence information." Section 702's definition of "foreign intelligence information" includes attacks on the United States, espionage, sabotage, international terrorism, proliferation of weapons of mass destruction, along with a more amorphous category: information "with respect to a foreign power or foreign territory that relates to … the conduct of the foreign affairs of the United States." Review of this surveillance is limited. In 1978, as part of the original FISA, Congress established the Foreign Intelligence Surveillance Court (FISC), which issues court orders under FISA's "traditional" framework, authorizing surveillance of agents of foreign powers in the United States. The FISC, which comprises life-tenured Article III federal judges, approves targeting procedures under § 702 but does not approve each individual target in advance.

On its face, Executive Order 12333 requires even fewer institutional or substantive checks. The executive order itself, which dates back to the Reagan administration, does not expressly limit targets, except for the general requirement that these targets be located abroad. The FISC has no role in reviewing targeting protocols.

After the Snowden revelations, President Obama issued Presidential Policy Directive-28 (PPD-28), which limited the purposes of surveillance. In a nod to the growing global focus on privacy, PPD-28 acknowledged that "[a]ll persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information." Accordingly, PPD-28 limited U.S. bulk collection under Executive Order 12333 to a defined set of goals. Under bulk collection, the U.S. can collect a wide range of communications from communications providers and internet hubs, some through algorithms. Software and intelligence officials sort through these communications for those that match certain categories, including countering espionage, sabotage, terrorism, cybersecurity threats, proliferation of weapons of mass destruction, and transnational criminal threats such as money laundering and evasion of U.S. sanctions. (The guidelines recently posted on the intelligence community's blog, IC on the Record, track these limits in more detail.)

But PPD-28's institutional checks do not match these substantive limits. PPD-28 provided no role for the FISC, leaving Executive Order 12333 vulnerable to the same concerns that critics have levelled at § 702: The framework lacks an independent review mechanism that would ensure that the U.S. intelligence community stays within the constraints that PPD-28 imposes.

As the name suggests, *Schrems II* is the CJEU's second encounter with assessing whether U.S. law provides adequate safeguards for EU persons' data. In *Schrems I*, the CJEU in 2015 held that the then-extant data transfer agreement, Safe Harbor, failed to hedge against the scope of U.S. surveillance. After the ruling, the European Commission and the United States negotiated a new agreement—Privacy Shield—which tasked an ombudsperson at the U.S. State Department with fielding EU persons' privacy complaints. *Schrems II* found that the ombudsperson role failed to cure the problems with adequacy that the CJEU had discerned in *Schrems I*.

Schrems II cited substantive and institutional deficits in Privacy Shield that echoed its earlier ruling against Privacy Shield's predecessor, Safe Harbor. The CJEU relied on the EU's core doctrine of proportionality, which requires tailoring of government measures to actual threats. Analyzing U.S. surveillance, the court found a lack of tailoring, particularly given the apparent breadth of both Executive Order 12333 and § 702's "foreign affairs" prong. The court also expressed concern that the FISC did not approve in advance all designated selectors—discrete data points, such as email addresses, social media handles, or cell phone numbers that match individuals linked to espionage, terrorism and so forth.

Institutionally, the CJEU stressed that EU persons' privacy complaints must be reviewed independently. The court viewed the State Department ombudsperson established under Privacy Shield as inadequate, noting that the ombudsperson was subject to dismissal by the U.S. secretary of state. For the CJEU, independence required either a court—the preferred option—or an independent executive agency whose members were protected from dismissal.

Citing the breadth of U.S. surveillance, the *Schrems II* court also raised questions about a common work-around implemented after *Schrems*: so-called standard contractual clauses (SCCs). Through SCCs, companies that transfer personal data can agree to additional safeguards against government surveillance. In theory, "appropriate" safeguards can compensate for substantive and institutional deficits in a surveillance regime. The CJEU did not rule out reliance on SCCs but warned that they were not effective against a surveillance regime that featured both broad legal authority and technical sophistication. The efforts of private parties through SCCs might be futile against such a formidable regime. Underscoring its wariness, the CJEU suggested that broad discretion and technological expertise were both central to U.S. intelligence collection.

A very recent decision by the CJEU, *La Quadrature du Net and Others*, expressed a more comprehensive understanding of the national security imperatives driving U.S. surveillance. In *Quadrature du Net*, the CJEU recognized that some bulk collection of information on the duration and location of communications might be necessary to ferret out evidence of existential threats such as terrorism. However, *Quadrature du Net* observed that the core EU values of proportionality and independent review still controlled how governments picked specific real-time surveillance targets. Along these lines, Theodore Christakis and Kenneth Propp have described France's efforts to revise the EU ePrivacy Directive to bypass the CJEU's regulation of national security surveillance by EU member states.

In addition, *Schrems II* opened the door for companies transferring data in-house or with contractual partners to derogate—that is, grant a limited exception—under Article 49 of the GDPR. Under Article 49(1)(b), a transfer to a country without adequate protections for data can still take place, even without "appropriate safeguards" such as effective SCCs. But a transfer must meet one of several conditions. For example, a transfer of personal data could be "necessary for the performance of a contract between the data subject" and the transferor—which could be true of, say, a U.S. company with an EU office that is transferring data about an employee. Judge Thomas von Danwitz of the CJEU has suggested that Article 49 derogations were worthy of exploration for companies that required a measure of flexibility. But the Article 49 contractual exception would not fit other contexts, such as Facebook's myriad uses of its users' personal data for targeted advertising. In other words, Article 49 offers help to firms trying to navigate EU privacy law after *Schrems II*, but Article 49's narrow scope will limit its application.

The narrow relief provided by Article 49 derogations becomes even more problematic in context of the broad reading of *Schrems II* adopted by an important EU privacy body, the European Data Protection Board. The EDPB's Recommendations on Supplementary Measures, adopted on Nov. 10, 2020, take a de facto absolutist stance that would effectively bar most transatlantic data transfers—sending EU-U.S. trade into a tailspin. For example, the EDPB requires technical measures such as sweeping encryption. Under the EDPB's guidelines, a data exporter may have to

encrypt data in such a way that a data importer is unable to decipher it, rendering the data transfer all but pointless. Furthermore, an EU firm may store encrypted data with a U.S. cloud service provider, but only if the encryption mechanism precludes the service provider's access to transferred data.

This guideline pits privacy against data security. The board's steep encryption requirements bar cloud services from checking data transfers for malware or other cyber intrusions, which has the effect of imperiling the security of all data users. This counterintuitive result exalts privacy rights as a matter of formal law but in practice sacrifices the actual privacy of users. In a world of persistent cyber threats, the EDPB's guidance on this score seems particularly shortsighted.

A case study in the EDPB's recommendations exemplifies its rigid approach. In sending EU persons' data to a "third country"—one outside the EU, such as the United States—the company must ensure that "the encryption algorithm is flawlessly implemented" and "the existence of back doors … has been ruled out." On the surface, this recommendation seems entirely appropriate. Digging deeper, though, questions arise. First, the recommendation subjects data security to an impossibly high standard. While encryption is often effective, even the best encryption can suffer some flaws in implementation. Moreover, given the resourcefulness and persistence of hackers, no encryption method can absolutely "rule out" the existence of back doors that will facilitate unauthorized access to data. The Snowden revelations make this clear.

Second, the EDPB's recommendation defeats the purpose of a great deal of data transfers. Imagine that a U.S. firm with EU employees transfers data to its U.S. parent company, which needs the data to implement its human resources policies. If the data were flawlessly encrypted and merely transited the U.S. in a packet impervious to inspection, no one at the parent company would be able to access the data—rendering the transfer useless. In sum, the EDPB's recommendations are either unrealistic, even for state-of-the-art data security, or undermine the very rationale of secure data transfers.

The EDPB's absolutist approach stems from an unduly broad reading of *Schrems II.* But narrow readings of the decision—including those offered by the U.S. government and distinguished American commentators—also provide flawed guidance. During the Trump administration, the Commerce Department—following the Obama administration's approach—stressed the checks in U.S. surveillance law. In a white paper issued in September 2020, the department argued that "[m]ost U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the CJEU in *Schrems II*." Writing in *Lawfare*, Alan Charles Raul argued that § 702 barred the United States from intercepting messages from the email systems of U.S. firms, even if those emails were sent or received by foreign nationals outside the United States.

Unfortunately, these narrow readings fail to pass muster. While U.S. surveillance law includes checks and balances, the CJEU focused on the absence of systematic FISC review of individual § 702 selectors—and that absence will continue to be telling, despite the presence of other limits on U.S. surveillance. Similarly, as a practical matter the risk may be low that the United States will seek to intercept emails from foreign national employees of U.S. firms. However, that is a back-of-the-envelope risk assessment, not a definitive statement of law. The CJEU signaled in *Schrems II* that exclusive reliance on risk assessment is not sufficient in the absence of concrete changes in the U.S. legal framework.

Looking to intelligence community privacy officers to review EU persons' privacy complaints is also not an adequate response to the CJEU. Privacy officers in agencies such as the National Security Agency do extraordinary work, building and maintaining a rule-of-law culture within the intelligence community. However, since privacy officers work in executive branch agencies directly answerable to the president, those officials lack the independence that the *Schrems II* court regarded as essential. Privacy officers can play a role, but their efforts are not a complete response to the CJEU's concerns.

Given the problems with both the broad and narrow readings of *Schrems II*, we propose an alternative: a hybrid strategy that pairs more detailed and methodical risk assessment with new institutional and substantive checks on U.S. surveillance.

To craft a more nuanced risk assessment, we look to U.S. export control law. U.S. law imposes a graduated system of controls on U.S. exports of technology and other goods, depending on conditions in the receiving state. This graduated approach may also allow for more efficient safeguards on data transfer.

EU and U.S. controls on "dual-use items"—goods, technology, or software with both civilian and military applications—are similar in most relevant respects due to European and U.S. participation in multilateral exports regimes. Export controls serve national security and foreign policy goals and deter proliferation of weapons of mass destruction. Specifically, national security controls limit foreign access to the most sensitive U.S. weapons and technology. These controls reflect the Cold War assumptions of the Coordinating Committee, a multilateral organization formed at the end of World War II by the U.S. and other NATO members to stem the flow of Western technology to the Soviet Union, its Warsaw Pact allies and China.

Several U.S. agencies participate in export controls. Most U.S. exports are shipped abroad under general export licenses from the Department of Commerce, which require no application or prior approval for their use. The Commerce Department can also issue an individual validated license to a particular firm, authorizing exports of specific items to a particular country of destination and for specific end users and end uses.

The State Department regulates the export of items specifically designed for military purposes —categorized as munitions—under a far more restrictive regime, requiring firms to register as arms exporters and obtain individual licenses for all destinations. Many more countries are restricted as compared with Commerce Department licensing, and there are fewer exemptions. Finally, the Department of Treasury administers foreign asset controls or embargoes, which prohibit virtually all financial and trade transactions with embargoed countries such as Iran and North Korea. These are subject to limited exceptions for humanitarian aid and informational materials.

The Commerce Department's graduated approach provides the closest analogy to a comparative assessment of data protection. The department's Bureau of Industry and Security (BIS) organizes countries into four country groups (A, B, D and E) based on particular reasons for control. For example, Country Group A is the least restrictive group and includes key U.S. allies and members of NATO, among others; Country Group B is a catch-all for more restrictive controls; Country Group D covers about 40 countries (including China, Russia and Yemen) that raise national security, nuclear, chemical-biological or missile technology concerns; while Country Group E is the most restrictive and includes countries subject to comprehensive embargoes (Cuba, Iran, North Korea, Sudan and Syria).

Like the GDPR, which serves the dual objectives of safeguarding fundamental rights to data protection and the free flow of personal data within the EU, export controls seek to limit access to strategic goods and technologies by potentially hostile countries without unduly burdening international trade. BIS controls establish general licenses for exports to many countries without the need for a license application or government approval—another echo of the GDPR, which permits data exports with appropriate safeguards to countries that have not received an adequacy determination. Finally, just as the EDPB recommendations require a firm to determine whether safeguards are "effective in light of all circumstances of the transfer," firms under the export control regime determine for themselves whether a proposed export of a dual-use item is eligible for a general license to some or all destinations or requires an individual validated license. Exporters must understand the specific conditions and restrictions of the various general licenses, how they apply to the proposed export and when the use of such licenses is prohibited.

Dual-use export controls have practical advantages. They permit firms to classify themselves based on their own experience and expertise, which curbs heavy-handed government regulation and promotes efficiency. But the regime reserves for the government vital policy questions such as the identification of particularly sensitive export items and high-risk countries.

To adapt this process to assessments of the adequacy of data protection, EU officials—ideally accompanied by member state representatives—should conduct bilateral meetings with officials of importing countries, including the United States. Officials at the meetings would conduct comprehensive reviews of foreign surveillance laws and practices. They would also assess judicial oversight and international commitments.

The meetings would take on several specific tasks to achieve these goals. Officials should identify which of an importing country's surveillance laws permit government access to transferred data and determine what, if any, categorical legal protections exempt specific end users and end-use scenarios from the reach of these laws. They should share information about the actual practices of intelligence agencies, together with company disclosures of various statistics related to government requests for user data, records or content. And, finally, they should consider implementing a wider array of supplementary measures along with notification procedures.

For example, imagine an agreement on guidelines under which any data exporter that relies on a risk-based assessment of third-country access as the basis for data transfers would—except in cases barred by law—receive a notice when a data importer or service provider becomes subject to a foreign government access request. This would allow the entity to revoke encryption keys and immediately suspend transfers pending the outcome of the request. The firm could also reassess the risks of relying on SCCs to accomplish such transfers.

Applying the export control model to data transfers would make risk assessment far more granular, comprehensive and reliable. Instead of the amorphous risk assessments offered by government agencies and commentators in the wake of *Schrems II*, EU data regulators could rely on a more systematic and dynamic approach, capable of shifting quickly based on changing circumstances. This approach would be a useful alternative to the EDPB's unmanageable absolutism.

Pairing with this more methodical approach to risk assessment, our hybrid model proposes institutional and substantive reforms in U.S. surveillance law. In the institutional realm, Congress should establish an Algorithmic Rights Court that will field EU persons' privacy complaints. The court would be staffed by life-tenured federal judges and aided by a full-time public advocate who would push back on government positions. It would provide gold-standard independent review, as the CJEU requires. As a fallback position if establishing the court is too heavy a political lift, the United States could delegate review of EU persons' privacy complaints to either the FISC—as Kenneth Propp and Peter Swire propose here—or an independent multimember executive branch agency such as the Federal Trade Commission or the Privacy and Civil Liberties Oversight Board, whose members have "for-cause" protections against dismissal.

As a substantive check, Congress should enact a statutory presumption against collection of the communications of foreign employees of U.S. firms located abroad. Since a great deal of transatlantic data transfer concerns such employees, a statutory presumption would install legal protections against unchecked surveillance of such persons. The government can overcome the presumption with specific evidence of a foreign employee's conduct. Furthermore, Congress should also revise the "foreign affairs" prong of FISA § 702 to limit surveillance to actions of foreign officials. The reduced scope of the "foreign affairs" prong will reassure EU bodies that the United States is taking global privacy protections seriously.

A hybrid approach would also make derogations under Article 49 of the GDPR more practicable. Derogations to fulfill contractual duties would be more sustainable, given a granular risk assessment and added U.S. safeguards. Some commentators read Article 49 as authorizing only occasional data transfers. The assurance added by a heightened risk assessment and further U.S. safeguards could justify more regular use of Article 49. This shift would increase the flexibility of data protection regulation without sacrificing privacy.

The hybrid model may not satisfy all stakeholders, and both broad and narrow readings of *Schrems II* will continue to attract acolytes. But the hybrid model acknowledges the core insights in *Schrems II* while enabling essential economic activity. That is a scenario worth pursuing on both sides of the Atlantic.

Topics: Cross-Border Data, Data Protection, Cybersecurity

Tags: Max Schrems, Schrems v. Data Protection Commissioner

Peter Margulies is a professor at Roger Williams University School of Law, where he teaches Immigration Law, National Security Law and Professional Responsibility. He is the author of Law's Detour: Justice Displaced in the Bush Administration (New York: NYU Press, 2010).

Ira Rubinstein is a Senior Fellow at the Information Law Institute. His research interests include Internet privacy, electronic surveillance law, big data, voters' privacy, EU data protection law, and privacy engineering. Rubinstein lectures and publishes widely on issues of privacy and security and has testified before Congress on these topics on several occasions.