ppi radically pragmatic

Privacy Wars: Peril and Promise for Transatlantic Data Transfers

KEN PROPP

JUNE 2020

@ppi | @progressivepolicyinstitute | /progressive-policy-institute

Privacy Wars: Peril and Promise for Transatlantic Data Transfers

KEN PROPP

JUNE 2020

INTRODUCTION

In May 2013, Edward Snowden publicly disclosed a trove of highly-classified information about US signals intelligence programs around the world, unleashing a torrent of outrage both in the United States and abroad. Nowhere did his revelations have a bigger impact than in Europe, where the extent of activities conducted by the US National Security Agency, sometimes with the cooperation of foreign intelligence services, came as a huge shock.

European Union officials were chagrined — and a little flattered — to learn that internal conversations with their overseas delegations had been intercepted. German headlines trumpeted the alleged tapping of Angela Merkel's personal cellphone. Snowden's revelations sharply disrupted the generally cooperative character of US-EU relations. "It seemed that the entire well of US-EU relations had been poisoned by the fallout from the Snowden affair," the US Ambassador to the European Union during the period has written, citing its political impact on negotiations over a potential transatlantic free trade agreement, among other effects.[1]

In Brussels, the evident scale of NSA surveillance was perceived as a challenge to 'data protection', the extensive body of privacy law that is one of the EU's signature regulatory initiatives. Snowden's disclosures provoked an almost existential crisis in Europe about whether privacy protection even mattered. Not long after, European privacy activists went to court to challenge the legitimacy of data transfers to

the United States, in a series of cases that rumble on to this day. Their efforts have upended one US-EU data transfer agreement, the Safe Harbor Framework, and now threaten to do the same for the successor Privacy Shield, as well as for contract-based privacy protections.

The political impact in Europe of the Snowden revelations inevitably has diminished over the past seven years. Today Europeans worry as much about weak privacy standards in authoritarian countries as about US surveillance practices. In addition, as governments around the world struggle to overcome COVID-19, they see data-tracking technologies as a key part of the solution — and worry less about the attendant privacy risks. Indeed, European governments are embracing data-tracking to a far greater extent than is the United States.

The forthcoming ruling by the European Court of Justice (ECJ)in the Snowden-legacy cases — due to be handed down on July 16 — has the potential to do more than reopen old wounds. Even more ominously, it may cause disarray in transatlantic digital commerce — at a time when governments cannot afford further economic damage.

A new Democratic Administration would be forced to confront the unresolved challenges of keeping data flowing across the Atlantic. How should the US Government respond if the ECJ again finds US privacy protections against surveillance of Europeans' personal information to be insufficient? Is it finally time for the United States to directly challenge Europe's efforts to impose its privacy rules on US national security data collection? Is there still room for compromise? Could a comprehensive US privacy law be part of the solution?

I. PRIVACY RULES IN TRANSATLANTIC COMMERCE

The European Union prides itself on regulating commerce in a manner that is extremely solicitous of potential harms to individuals. It follows the 'precautionary principle', under which a product may only be introduced onto the European market if it can be proven to present no risk to consumers. Applying this standard is harder in the case of services than goods, especially when a service is provided from abroad and entails the transfer of personal data outside of Europe.

The EU's data protection law, the General Data Protection Regulation (GDPR), provides a way to minimize the risk that individuals' personal data will be misused when it is transferred abroad. It does so by establishing a 'border control' regime for data transfers from Europe.[2] An international data transfer may only occur if there is a legal arrangement in place "to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined" in other jurisdictions.[3] In other words, a European can rest assured that a company processing his or her data abroad does so in broad conformity with the EU's privacy rules.

Data has become a central commodity in transatlantic — and global — commerce of all types, not just for services which are delivered using information and communications technology. When a European consumer makes purchases a good from a US online marketplace, his or her personal data travels to America through undersea cables as part of the transaction. Multinational companies are constantly shifting personal data around the globe, for services as mundane as personnel management. Global data transfer rates expanded more than 40 times over the decade

between 2005 and 2014,[4] and continue to grow rapidly, particularly across the Atlantic. Cross-border data transfers between the United States and Europe are 50% higher than those between the United States and Asia.[5]

A company importing personal data from Europe into the United States typically chooses between two principal transfer methods, outlined in the GDPR,[6] for guaranteeing the continuity of privacy protection. One is to subscribe to the privacy principles set forth in the US-EU Privacy Shield framework.[7] More than 5300 companies — many small-and medium-sized businesses among them — have done so. The EU deems data transfers made by these companies to the United States to afford an 'adequate' basis of privacy protection. The US Commerce Department monitors signatory companies' compliance with the Privacy Shield principles, and the Federal Trade Commission (FTC) has authority to enforce against those that fail to honor their commitments.

A company's main alternative to joining the Privacy Shield is to insert into individual contracts for data transactions certain standard privacy protection clauses that have been pre-approved by European data protection authorities (DPAs). In other words, a data importer outside the EU assumes a contractual obligation to handle data in conformity with the privacy terms laid down by the exporter inside the Union. Companies, especially larger ones, widely use standard clauses to transfer personal data from Europe to many parts of the world, not just across the Atlantic. European DPAs enforce compliance with standard privacy clauses.

II. PRIVACY RULES AND NATIONAL SECURITY SURVEILLANCE COLLIDE

The Privacy Shield, while popular with companies, rests on a shaky legal foundation. It was hurriedly negotiated between Washington and Brussels after the ECJ in 2015 had effectively invalidated its predecessor, the 2000 Safe Harbor Framework. The court did so in response to a petition from Austrian privacy activist Max Schrems, who had read Edward Snowden's allegations that US social networks were providing foreigners' communications to the NSA, and believed (without any supporting evidence) that his own Facebook communications had made their way to Fort Meade.

Facebook at the time was using the Safe Harbor Framework as the legal basis for its data transfers from the Continent. Schrems pointed out that a provision in the Framework in fact excused a company from complying with its privacy protections if confronted by a US national security agency's demand for personal data. Such demands, the ECJ decided, permitted the NSA "to have access on a generalized basis to the content of electronic communications," and "must be regarded as compromising the essence of the fundamental right to respect for private life…" contained in the EU's Charter of Fundamental Rights.[8] The ECJ went on to find deficiencies in a number of other features of Safe Harbor, including its failure to provide aggrieved individuals with a right of effective redress for violation of its provisions.

Schrems' case represented the collision of two worlds — the straightforward one of companies

transferring personal data for purely commercial purposes, and the shadowy one of governments obtaining these communications for purposes of protecting national security. It shone a spotlight on the United States, not only because American internet platforms dominate the data transfer business worldwide, but also because US intelligence agencies operate on a much larger scale than do European counterparts.

The EU's negotiations with the United States to remedy the deficiencies of the Safe Harbor faced legal as well as political hurdles. Since the EU Charter of Fundamental Rights is effectively the equivalent of the US Bill of Rights, ECJ judgments applying its provisions have the character of constitutional jurisprudence. The European Commission, the EU's executive arm, must scrupulously respect the Court's holdings, and has only as much international negotiating room as the judges have allowed.

The Privacy Shield remedied some of the ECJ's criticisms of the Safe Harbor Framework. It strengthened the privacy principles, beefed up the roles of Commerce and the FTC in overseeing compliance, and created an administrative channel for Europeans to complain to an ombudsperson in the State Department if they suspected that the NSA was sifting their personal information.

The United States even sought to address European concerns about national security surveillance. A pair of letters appended to the Privacy Shield from Office of the Director National Intelligence (ODNI) General Counsel Robert Litt described recent changes to the US legal framework for signals intelligence. Litt highlighted the Obama Administration's issuance, in the Snowden aftermath, of a policy directive (PPD-28) that extended partial privacy protections to foreign nationals and limited the NSA's bulk collection of certain types of personal data. He also pushed back on the ECJ's impression that America's national security data collection efforts were vast. "Bulk collection activities regarding Internet communications that the US Intelligence Community performs through signals intelligence operate on a small proportion of the Internet," Litt wrote.[9] What US negotiators steadfastly refused to do, however, was to agree to any further limits on their government's wide-ranging legal authority to surveil Europeans' communications.

Europe's privacy activists were distinctly unimpressed by the new, improved transatlantic data transfer arrangement. Soon after the Privacy Shield took effect, a French group filed suit against it in the ECJ.[10] Max Schrems separately chose to refocus his sights instead on standard contract clauses, the alternative transfer mechanism which Facebook, like many companies, had adopted in the interval following the collapse of the Safe Harbor Framework. Schrems observed that standard clauses – like the Safe Harbor -- also excuse a company from its privacy protection obligations when confronted by a foreign national security agency's demand for personal data. He therefore claimed that standard clauses were equally deficient from the perspective of EU fundamental rights. His reformulated complaint gradually made its way back to the ECJ.[11]

Thus, the EU court was presented with parallel challenges to the two major data transfer mechanisms in use with the United States, each case posing similar underlying questions about US surveillance law and practices. At the ECJ's hearing last summer on Schrem's challenge to standard contract clauses, the lead judge in the case, Thomas von Danwitz of Germany,

also posed questions addressing the validity of Privacy Shield. Suddenly the prospect appeared of the ECJ issuing one judgment deciding the US surveillance issues common to both. US companies which depend on transatlantic data transfers realized they could be facing the perfect storm.

III. RECKONING DAY AT THE ECJ

In the first stage of deciding an important case like this, a senior court jurist known as an Advocate General (AG) issues an opinion exhaustively analyzing the issues and recommending a resolution. Some months later, the judges release a final judgment, which usually — but not necessarily — follows the AG's recommendation. The 97-page opinion of AG Henrik Saugmandsgaard Øe of Denmark, issued on December 19, 2019, generated equal measures of relief and alarm for the US government and companies.

Øe first examined whether standard contractual clauses used for transatlantic commercial data transfers measured up to the EU's fundamental rights standards. He acknowledged that they foresaw the possibility of a foreign data importer being ordered to turn over data to its host government for national security reasons. However, Øe added, the European data exporter, once notified by the foreign importer of the local government's demand, in turn could ask the relevant EU member state DPA to prohibit the affected data transfer outside the Union from happening. He therefore advised the judges not to take the "somewhat precipitous" step of reaching a broad conclusion about whether standard clauses sufficiently protected Europeans' privacy rights until a DPA had had an opportunity to consider the particular circumstances of an NSA demand to Facebook.[12] If the ECJ adopts Øe's perspective, Facebook and the many other companies using standard clauses in transatlantic commerce will, at a minimum, have bought some time, until national DPAs can assess the clauses' effectiveness in contested cases.

Had the Advocate General stopped there, his opinion would have been embraced as a reprieve for a principal means of transatlantic data transfers. But Øe then went on to analyze the validity of the Privacy Shield itself, paving the path for Judge von Danwitz and his colleagues to decide the merits of both transatlantic data transfer instruments in one combined judgment, if they so choose.

The AG did find Privacy Shield to be an improvement over the Safe Harbor Framework in certain respects. In particular, he concluded that NSA surveillance conducted under the authority of the Foreign Intelligence Surveillance Act (FISA) did not amount to 'generalized access' to the content of electronic communications, since intelligence officials must apply selection and filtering criteria before accessing personal data. If the ECJ agrees, one of the important factual errors it made in the first Schrems judgment will have been corrected.

However, Øe criticized numerous other features of US surveillance law and of the Privacy Shield. He was alarmed by the US government's extensive reliance on non-statutory surveillance authorities such as Executive Order 12333. He similarly was concerned that privacy protections for non-Americans conferred by PPD-28 could be undone by executive fiat (as indeed President Trump was rumored to be considering early in the current Administration). The AG likewise was unimpressed by the powers of the State Department ombudsperson to operate as an

administrative remedy for Europeans, pointing out that the office lacks both investigative powers and independence from the executive branch. It is hard to avoid the conclusion that the Advocate General regards data transfers under the Privacy Shield as failing fully to guarantee EU privacy rights.

The ECJ's judgment will be handed down on July 16. Most observers agree that the court will find deficiencies in the transatlantic data transfer regime, but they diverge on how far it will go. Will the judges assess only the validity of standard contract clauses, as the Advocate General urges, or will they go beyond to draw conclusions about the Privacy Shield as well? If the court finds Privacy Shield wanting, will the arrangement effectively be invalidated with immediate effect, as occurred in the case of the Safe Harbor? Or might the ECJ instead grant the European Commission a reasonable interval to renegotiate the Privacy Shield with the United States?

IV. TOWARDS A US STRATEGY FOR ENDING THE PRIVACY WARS

Ever since the Snowden allegations erupted, American companies have looked in vain for a lasting legal foundation for vital transatlantic commercial data transfers. The US Government's own frustration also occasionally has emerged into public view. In the wake of the Schrems judgment's sharp criticism of US surveillance practices, President Obama pointed to the deafening silence from European governments on the important role US intelligence plays in protecting Europe's national security:

…a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities; and that they themselves have relied on the information we obtain to protect their own people.[13]

If the ECJ again rules against transatlantic data transfer mechanisms, it is not hard to imagine a US Administration concluding that negotiated solutions with Europe have not worked and turning to a confrontational posture. It certainly has the tools. The Executive Branch could turn off intelligence sharing with European allies and wait for the yelps from their security services to reach Brussels. Alternatively, US internet platforms might be quietly urged temporarily to stop providing the services that Europeans daily depend on.

US companies surely would press the Administration to pursue a further negotiated privacy arrangement with the European Union, however. Some ECJ objections to US surveillance laws could be addressed through Congressional action and reflected in a revised Privacy Shield. But not all judicial criticisms would have a reasonable prospect of Congressional remedy – so it is important that the court not overreach.

The ECJ might, for example, find that important and long-established US surveillance authorities embedded in executive order rather than statute do not measure up to European fundamental rights norms. The court also could demand specific changes to US bulk surveillance practices, such as the methods the US intelligence community uses for selecting and filtering which tranches of personal data to scrutinize. It is difficult to foresee Congress being sympathetic to such concerns, particularly in the current turbulent era of transatlantic relations.

The ECJ might well also point to the need for the United States to strengthen the institution of the ombudsperson as an arbiter of Europeans' complaints about surveillance of their personal data. Congress should sympathetically consider making the ombudsman independent of executive branch influence and granting it autonomous investigative powers as well. There is in fact an existing agency within the US government well-suited to take on such a remedial function — the Privacy and Civil Liberties Oversight Board (PCLOB). Congress could grant the PCLOB, a small but respected independent agency currently charged with privacy oversight of US counter-terrorism laws, the additional authority and resources to scrutinize national security access to personal data transferred to the United States for commercial purposes.[14]

The ECJ additionally may confirm Advocate General Øe's doubts about the legal durability of PPD-28. Transforming privacy elements of this directive into the form of a statute would greatly strengthen European confidence that they cannot easily be undone. Congressman Eric Swalwell (D-CA) in fact proposed this step in an unsuccessful amendment to the 2018 bill reauthorizing Section 702 of the Foreign Intelligence Surveillance Act.[15] Legislating portions of PPD-28, together with strengthening surveillance oversight by an independent ombudsperson, would go a long way towards overcoming European legal objections to the Privacy Shield and standard contract clauses.

Beyond these concrete steps, the very act of the US Congress passing comprehensive privacy legislation would be persuasive evidence to Europe and the rest of the world that the United States takes seriously key privacy principles such as limits on consent and on use of data, and redress. Congress in recent years indeed has inquired into the GDPR, taking testimony from leading European privacy regulators about how their experience could inform US comprehensive legislation.[16]

Most importantly, enacting a comprehensive US privacy law would present a credible case to Brussels that transatlantic privacy protections are broadly congruent, even if they inevitably diverge in some respects. No longer would the US Government be condemned to repeated, piecemeal attempts to disprove alleged deficiencies in its system of privacy protection. Instead, the EU and the United States finally could develop a definitive regime for transatlantic commercial data transfers based on reciprocal respect for each other's legal systems.[17]

Congress showed it could exercise global leadership on international data transfers when it enacted the 2018 CLOUD Act to allow law enforcement authorities rapid and efficient access to electronic evidence located abroad.[18] Foreign authorities may only obtain e-evidence located in the United States if their requests meet due process standards comparable to the rigorous ones of US criminal law.

Ever-larger portions of the future transatlantic economy will run on data flowing in both directions. If the United States and Europe are definitively to end the privacy wars that intermittently have flared between them, the protections that accompany the transatlantic movement of personal data must become a two-way street as well.

References

1 Anthony Luzzatto Gardner, "Stars with Stripes: The Essential Partnership between the European Union and the United States" (2020), 167.

2 Dan Jerker B. Svantesson, "The Regulation of Cross-Border Data Flows," International Data Privacy Law Journal, v.1, no 3 (2011), 180.

3 Regulation 2016/679, Article 44. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FR

4 "The US-EU Privacy Shield Pact: A Work in Progress," Peterson Institute for International Economics, August 2016. https://www.piie.com/publications/policy-briefs/us-eu-privacy-shield-pact-work-progress

5 Daniel S. Hamilton and Joseph P. Quinlan, The Transatlantic Economy 2019, Chapter 3, 33. https://transatlanticrelations.org/wp-content/uploads/2019/03/TE2019_FullStudy.pdf

6 Regulation 2016/679, Articles 45-46. Other legal bases for data transfers exist, including binding corporate rules applying among entities forming a single corporate entity (Article 47), and derogations such as consent for use in specific situations (Article 49). Most transfers occur pursuant to the Privacy Shield or standard contract clauses, however.

7 EU-United States Privacy Shield Framework, February 23,2016, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg

8 Maximillian Schrems v. Data Protection Commissioner, C-362/14, October 6, 2015, paragraph 94.http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8417690

9 EU-United States Privacy Shield Framework, Letter from Robert Litt, General Counsel, Office of the Director of National Intelligence, 4.

10 La Quadrature du Net and Others v. European Commission, T-738/16, filed October 25, 2016. https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.006.01.0039.01.ENG

11 Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, C-311/18, filed May 9, 2018. http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=8417690

12 Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, C-311/18, Opinion of Advocate General Saugmandsgaard Øe, December 19, 2019, paragraph 172. http://curia.europa.eu/juris/document/document.jsf?docid=221826&pageIndex=1&occ=first&part=1&text=&dir=&doclang=EN&mode=lst&cid=8417690

13 Remarks, January 17, 2014. https://obamawhitehouse.archives.gov/photos-and-video/video/2014/01/17/president-obama-speaks-us-intelligence-programs

14 The Executive Branch might not necessarily need legislation to shift the ombudsperson from State to the PCLOB. The PCLOB might be able to build upon its existing mandate to examine terrorism-related laws, and State might be able to transfer its current responsibilities to the PCLOB by means of an interagency memorandum. However, a statutory measure would send the strongest possible message to the EU of the US commitment to policing intelligence uses of foreign-origin data.

15 FISA Amendments Reauthorization Act of 2017 P.L. 115-118, January 19, 2018. https://www.congress.gov/115/plaws/publ118/PLAW-115publ118.pdf

16 Andrea Jelinek, Chair of the European Data Protection Board, Testimony before the US Senate Committee on Commerce, Science, and Transportation, October 10, 2018, https://www.commerce.senate.gov/services/files/892b1917-02ce-4f38-8dce-c8dabcfe4180

17 Such a definitive accord already has been reached with respect to transatlantic data transfers for law enforcement purposes, in the form of the Agreement between the United States of America and the European Union on the Protection of Personal information Relating to the Prevention, Investigation and Prosecution of Criminal Offenses, June 2, 2016, TIAS 17-201, https://www.justice.gov/opcl/DPPA/download

18 The Clarifying Lawful Overseas Use of Data Act, contained in Consolidated Appropriations Act, 2018, P.L. 115-141, div. V.

ppi

The Progressive Policy Institute is a catalyst for policy innovation and political reform based in Washington, D.C. Its mission is to create radically pragmatic ideas for moving America beyond ideological and partisan deadlock.

Founded in 1989, PPI started as the intellectual home of the New Democrats and earned a reputation as President Bill Clinton's "idea mill." Many of its mold-breaking ideas have been translated into public policy and law and have influenced international efforts to modernize progressive politics.

Today, PPI is developing fresh proposals for stimulating U.S. economic innovation and growth; equipping all Americans with the skills and assets that social mobility in the knowledge economy requires; modernizing an overly bureaucratic and centralized public sector; and defending liberal democracy in a dangerous world.

PROGRESSIVE POLICY INSTITUTE
1200 New Hampshire Ave NW,
Suite 575
Washington, DC 20036

Tel 202.525.3926
Fax 202.525.3941

info@ppionline.org
progressivepolicy.org