18 August 2020

The EU Is Hoist with Its Own Data-Protection Petard

Peter Chase

For 'tis the sport to have the enginer

Hoist with his own petard; and 't shall go hard

Shakespeare, Hamlet, Act 3 Scene 4

In Shakespeare's play, Hamlet looks forward to re-directing a ploy of his murderous uncle Claudius back onto him, so that the latter can be "hoist with his own petard," a reversal of an assassination plot that brings a certain poetic justice.

The European Union's efforts to protect the personal information of its citizens are of course far more noble than the motivations of Claudius. But there is a certain poetic justice in the European Court of Justice (ECJ) July 16 decision to rule the U.S.-EU Privacy Shield arrangement "invalid." In its ruling, the ECJ effectively says the United States is not democratic enough because it does not sufficiently constrain U.S. law-enforcement and intelligence agency access to Europeans' personal data. But the ruling clearly applies to all countries, and the only way the EU will be able to permit the transfer of personal data to many (China and Russia spring immediately to mind) will be to ignore the protections it has so painstakingly assembled.

Background

The EU's 1995 Data Protection Directive (DPD) explicitly prohibited the transfer of "personally identifiable information" to any third country if that data could not be adequately protected, so that the individual concerned would have control over the way the data was processed, stored, and transferred. Two articles in the DPD provided exceptions to that prohibition—the transfer could be made to a country that the European Commission certified as providing "adequate" protections (only six countries outside Europe qualify: Argentina, Canada, Israel, Japan, New Zealand, and Uruguay), or it could be transferred when it was protected by other legal mechanisms, including Standard Contact Clauses and Binding Corporate Rules. Informed personal consent was also included as an exception in this article.

The European Commission at the time refused to find the United States as "adequate" because the latter does not have a national data-protection law. To get around this, the United States and EU concluded the Safe Harbor arrangement in 2000, under which firms that pledged to abide by data processing protections reflected in the DPD would be considered as providing adequate protections even if the United States as a country did not measure up.

After the 2013 Snowden revelations about the National Security Agency's ability to access information held by companies through the PRISM program, Section 702 of the Foreign Intelligence Surveillance Act and other such activities, Max Schrems—an Austrian law student—filed a suit against Facebook in Ireland (where the company has its European headquarters), saying its Safe Harbor commitments were not sufficient to protect his information, so it should not be sent to California. The suit was sent to the ECJ to clarify how the DPD should be applied.

In 2015, the Court ruled the Safe Harbor arrangement invalid because the European Commission had not considered whether the United States had sufficient "democratic controls" against access by law-enforcement and intelligence agencies to information held by the companies that had pledged to abide by it. The ECJ ruling was "procedural" in that it was based exclusively on the Commission not having been thorough enough in its evaluation of Safe Harbor, but the Court also intimated that it doubted the United States had the necessary protections.

Critically, the ECJ explained its ruling by saying that the Data Protection Directive had to be read "in light of" the European Charter of Fundamental Rights. The Charter, which gained formal status as EU law only in 2009, provides all Europeans the "fundamental rights" of protection against unwarranted government intrusion into their privacy or abuse of their personal data. This applies to all EU and member-state government actions at all times. As such, the ECJ reasoned, foreign countries should also be assessed on this basis before they can be determined to provide adequate protections, even though the DPD explicitly did not apply to law-enforcement or national-security matters. The Court affirmed that the DPD and the Charter "prohibited" the transfer of personal data to countries that did not have "democratic controls" similar to those in the Charter.

Schrems II

The 2015 ECJ decision on its face was "merely" a process foul called against the Commission for not having done its homework on a specific adequacy finding for a specific country. Few at the time wanted to acknowledge how broad its implications might be.

To test this, Schrems filed a second case against Facebook alleging the standard contract clauses the company used to justify holding his data in the United States after the ECJ declared Safe Harbor null and void were also inadequate.

In "Schrems II" decision, the European Court of Justice was working on the basis of the General Data Protection Regulation (GDPR) that the EU adopted in May 2016 to replace the DPD, as well as the Privacy Shield arrangement that the EU and United States as the successor to Safe Harbor in July 2016. And not surprisingly, the Court reaffirms that the GDPR provisions on data transfers to third countries must still be read "in light of" the protections in the European Charter of Fundamental Rights.

Directly answering Schrems' question about the standard contract clauses, the ECJ affirms they can be used as a mechanism to allow the transfer of personal data to countries that do not benefit from an adequacy decision by the European Commission. But because those clauses only apply to the companies involved and do not constrain government action, the company exporting the data, the receiving company in the third country, and the relevant member-state data-protection supervisor must all assess whether the data can be adequately protected against government intrusion in that country. If not, the transfers must be stopped, and all information that has been transferred to the third country must be returned or destroyed.

The ECJ further ruled that, in the case of the United States, Privacy Shield could not provide adequate protections because it explicitly subordinates participating company pledges to law enforcement and national security; Section 702 and other presidential Executive Orders still give the U.S. government "disproportionate" access to personal data; and the redress available to an EU citizen who believes his/her information has been misused by the U.S. government is insufficient as the Privacy Shield ombudsperson, who sits in the State Department, is not independent and has no authority over actions by law-enforcement and intelligence agencies.

Consequences

The ECJ is the EU's supreme court; its decision is constitutional and substantive, not just procedural. It has immediate effect and applies to the transfer of personal data to all third countries.

All that said, nothing happens immediately or automatically. The ECJ judgement is directed to the Irish High Court, which in turn will instruct the Irish data-protection supervisor to inform Facebook Ireland that it may not use either Privacy Shield or Standard Contract Clauses to justify the transfer of Schrems' data to the United States. It will probably broaden that to prohibit Facebook from transferring the data of any other resident in Europe to the United States, in part to justify setting the potential fine closer to the 4 percent of total global revenues in the event of non-compliance. That non-compliance and fine would need to be adjudicated by an Irish court.

In the meantime, the European Data Protection Board (EDPB), which ensures consistency among the EU data-protection supervisors, has said that the European Commission and the U.S. government should "achieve a complete and effective framework" to ensure that Europeans' data is protected as well in the United States as in Europe. The Trump administration, however, is highly unlikely to agree to any additional constraints on U.S. law-enforcement and national security agencies beyond the truly extensive obligations undertaken in Privacy Shield, although it may be willing to tweak the redress mechanism. The EDPB has also called on data exporters and importers to determine if the law in the importing country is good enough, acknowledged that EU data-protection supervisors must suspend or prohibit transfers under Standard Contact Clauses (or anything else) where data cannot be protected from government intrusion, and reminded everyone that the final possible grounds for transfer—the derogations new to the GDPR (which include informed personal consent) which the ECJ mentions in the very last paragraph of its reasoning—can only be used on a case-by-case basis.

European Commission officials say that all the above implies that companies should adopt a risk-based approach to transferring personal data to third countries. If they have a legitimate ground for transferring, processing, and storing the data, and if they believe the likelihood of unwarranted government intrusion is

minimal (for normal employee data, for example), they can proceed. Contractual arrangements may need to be amended to require data importers to provide the European data exporter with information about government requests for data they receive (which could be problematic if the government requires such a request be kept secret), as well as evidence of internal practices for handling such requests.

Comment

All of this is to play for time. The ECJ's judgement and reasoning are clear, but so too are the implications and consequences: no personal data can be transferred to a country where the government can access that data without a warrant duly exercised before an independent judiciary acting on the basis of democratically adopted law and where democratically elected representatives have the power to oversee and if necessary rein in the activities of law-enforcement and security agencies. The United States, the ECJ has said, does not now qualify given aspects of its legal regime. But China and Russia certainly do not, and publicly available information could easily raise doubts about many other countries, such as Israel (which has an adequacy decision), Turkey… and the United Kingdom. (Complaints exist as well about many EU member state government practices, but the ECJ argues these are covered by the Charter.) And, as literally every email and every contract involves the transfer of personal information, presumably all these should be prohibited, bringing economic relations (and everything else) with these countries to a screeching halt.

That of course will not happen; even the ECJ would agree that ending all transfers of personal data to a country that has even as intrusive practices as China would not be practical, even if that is the clear meaning of its ruling. Instead, workarounds will be developed, even if that means using the derogations more broadly than they were intended or simply not enforcing the law.

The EU's data-protection piety has essentially brought us full circle: back to the reality that data can and will be transferred, processed, and stored in third countries, unless there is a specific court case against a specific company saying it cannot. That is, back to the rule of the jungle and caveat emptor—buyer beware. Hoist with its own petard indeed.

18 August 2020

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org