ELB Blogpost 35/2022, 12 September 2022
Tags: CLOUD Act, DMA, DSA, EU Cybersecurity Act
Topics: Data protection and digital governance

European Cybersecurity Regulation Takes a Sovereign Turn

By Kenneth Propp

Over the past year, the European Union's ambitious digital regulatory agenda has steadily advanced. The EU adopted the far-reaching Digital Markets and Digital Services Acts, and it is completing negotiations with the United States on a revised data transfer regime, christened the Transatlantic Data Privacy Framework (TADPF), that was necessitated by the *Schrems II* judgment of the Court of Justice of the European Union (CJEU). These developments have had a significant impact on transatlantic economic relations, even stimulating legislative initiatives on privacy and antitrust in the United States. One might think that resolving such contentious topics would set the stage for a quieter, more harmonious phase in the transatlantic technology policy relationship.

As EU regulatory activity resumes this fall, a lesser-known initiative – creating an EU-wide certification framework for ICT products and services (EUCS) – could cause renewed disturbance between Brussels and Washington, however. Under the EUCS proposal being developed by the EU's cybersecurity agency ENISA, cloud service providers would be compelled to localize their operations and infrastructure within the EU and to demonstrate their 'immunity' from foreign law.

Europe's concerns about the security of U.S. cloud services providers are in fact closely intertwined with its worries, expressed in *Schrems II*, about the privacy of Europeans' information entrusted to these companies. In both cases, European policymakers fear the perceived extraterritorial reach of U.S. national security surveillance and law enforcement authorities. New cybersecurity regulation thus is seen as another way to safeguard Europe's 'sovereign' interest in protecting data from foreign government access. It also would reinforce separate European efforts to bolster smaller, home-grown cloud service providers, including through the GAIA-X project to create an

interoperable network "explicitly based on principles of 'sovereignty-by-design,'" as a leading European technology lawyer has characterized it.

La Souveraineté en Nuage

This thinking originated in Paris. In 2016, France's Information Security Systems Agency (ANSSI) launched a certification and labeling program, known as SecNumCloud, to establish minimum levels of security for French public entities procuring cloud services to host data and information systems. Compliance with the standards initially was voluntary. Since then, ANSSI has certified as 'trusted' only five services provided by three companies, all of which are headquartered in France.

In 2021, the French government issued the *Doctrine for the use of cloud computing by the State* ("Trusted Cloud Doctrine") making SecNumCloud certification mandatory whenever a French government agency procures cloud services that would handle sensitive data, including personal data of French citizens and economic data relating to French companies. These requirements also apply to private operators of essential services. Under France's Trusted Cloud Doctrine, qualifying cloud service providers must be "immune to any extra-EU regulation". In addition, such companies must commit to storing and processing data within the European Union, and to administering and supervising the service within the EU. Further, foreign-headquartered cloud service companies cannot achieve certification if they are more than 39% foreign-owned.

These latest revisions, which took effect in March 2022, effectively force foreign-headquartered cloud companies either to enter into joint ventures with French providers in which the foreign participant owns a minority and non-controlling interest, or else to license their technologies to a certified local vendor. Several have done so. Google joined with the French company Thales to create a new company compliant with the SecNumCloud requirements; Microsoft formed a venture with Capgemini and Orange, both French companies.

The director general of ANSSI, Guillaume Poupard, strongly endorsed these new requirements as promoting digital sovereignty. Europe needs "a rule that only European law is applicable on cloud products certified in Europe," he said. "This is about…having the courage to say that we don't want non-European law to apply to these services," Poupard added. "If we're not capable to say this, the notion of European sovereignty doesn't make sense."

Scholars have argued that mandatory localization actually harms cybersecurity by blocking the international data flows pervasively used in cybersecurity measures such as incident reporting and threat intelligence. Such measures not only undermine integrated company management of cybersecurity risks; they also can have the effect

of depriving users of the stronger protection measures utilized by foreign cloud providers.

Clouds Over Brussels

The EU's Cybersecurity Act, adopted in 2019, established the legal basis for EU-wide certification of cloud providers, to be elaborated through secondary law by its cybersecurity agency ENISA. In December 2020, ENISA began a public consultation as the first step towards a revised set of rules. A technical working group is preparing a proposal, expected to be presented to member state experts and to the European Commission thereafter. The new requirements could be finalized by the end of the year.

The European Commission, in a working document, identified cloud services as a "strategic dependency", expressing concerns that the EU cloud market is led by a few large cloud providers headquartered outside the EU. In July, 2021, France, joined by Germany, Italy, and Spain, submitted a proposal to the ENISA-led working group aimed at generalizing French national requirements across the EU. (Germany has since reserved its position.) It proposed to add four new criteria for companies to qualify as eligible to offer 'high' level services, including immunity from foreign law and localization of cloud service operations and data within the EU. Although the EU-level cyber certification requirements currently are conceived as voluntary, they could be made mandatory as the result of the recently-agreed Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive).

A cross-party group of members of the European Parliament, with heavy French representation, has weighed in to support the French proposal at ENISA. Member states' reactions, on the other hand, have been mixed. Seven of them – Denmark, Estonia, Greece, Ireland, the Netherlands, Poland, and Sweden – submitted a non-paper to the Council of the European Union questioning the need for sovereignty requirements in the new cyber certification standards and calling for further study of their potential interaction with the General Data Protection Regulation (GDPR), non-personal data regulations, and EU international trade obligations. In addition, these governments have sought a political-level discussion of the subject in the Council before the new standards are finalized. Several trade associations, including the German BDI and Europe-wide financial clearinghouses, have chimed in.

Affected companies have even begun to question whether ENISA has the authority under EU law to impose non-technical governance measures with such a sweeping impact. A Dutch member of the European Parliament who was closely involved in drafting the NIS2 Directive told Politico that the current draft cyber certification scheme does not comport with the letter or spirit of that legislation. In addition, an unusual editorial note attached to the leaked draft acknowledges that it has not yet

been the subject of legal review and that some proposed requirements may be "a potential source of legal issues".

On September 1, U.S. Trade Representative Katherine Tai raised concerns about the French and EU cybersecurity certification schemes in a call with European Commission Executive Vice President Valdis Dombrovskis, who is responsible for trade – an indication that the issue now has risen to a high level of official concern for the U.S. government.

'Immunity' from Foreign Law

Insisting that its cloud service providers be 'immune' from foreign law is part of a larger European effort to escape the long arm of U.S. national security surveillance and law enforcement authorities. In the national security realm, the U.S. government has two means of obtaining foreign-located information. One authority is Section 702 of the Foreign Intelligence Surveillance Act (FISA), under which the National Security Agency (NSA) may target the communications of non-U.S. persons located outside the United States, subject to prior authorization by the Foreign Intelligence Surveillance Court. In 2013, Edward Snowden publicly revealed the existence of two NSA programs that operated under the authority of Section 702, PRISM and UPSTREAM. The second is direct NSA interception of telephone and Internet traffic from internet cables and switches, which takes place under the authority of Executive Order 12333. These programs were the subject of attention in the *Schrems II* case and are addressed in the new Transatlantic Data Privacy Framework (TADPF).

U.S. law enforcement may exercise a separate unilateral authority to obtain foreign-located information relevant to criminal proceedings. This power, now codified in the 2018 CLOUD Act, permits a federal judge to issue a warrant, based on probable cause, compelling a provider of electronic or remote communications services, including a cloud service provider, to turn over to U.S. law enforcement agencies any data within its "possession, custody, or control", even when that data is "located … outside the United States". Not only U.S.-headquartered providers are subject to this requirement; it applies equally to any provider subject to U.S. jurisdiction, wherever its headquarters may be. A person, including a corporation, is within U.S. jurisdiction if it has "minimum contacts" with the United States, such as by conducting business there.

Just as U.S.-based companies cannot exempt themselves from the reach of these U.S. laws and programs, neither can foreign companies operating in the United States. Several French cloud companies certified under SecNumCloud, including OVH, 3DS Outscale, and WorldLine Cloud Services, have U.S. operations. OVH, in fact, explicitly concedes that its U.S. affiliate "will comply with lawful requests from public authorities". The company maintains, however, that since OVH US does not possess or control data held by its affiliates in other countries, including OVH France, the U.S.

Department of Justice would not be able to successfully demand data they hold outside the United States.

It is a legally and factually complex question whether any cloud services company operating in the United States – American or European – can escape the reach of these U.S. legal authorities. In the case of the CLOUD Act, the question may well turn on corporate structure and the choices of customers on the jurisdiction in which to store their data. The viability of an 'immunity' requirement in French or EU law thus ultimately will depend on how courts view company attempts to separate themselves from domestic jurisdictional reach. Because so many EU-based companies conduct at least some business in other countries, including through online services, an "immunity" requirement in French or EU law thus could result in numerous disqualifications from cybersecurity certification.

Cyber Certification and International Trade Law

Establishing standardized cybersecurity frameworks for procurement of cloud services is a legitimate and important policy objective for any government. France and the EU are not alone in pursuing this path with some urgency. The United States itself operates a government-wide program to standardize security assessment and authorization, the Federal Risk and Authorization Management Program (FedRAMP). The Department of Defense (DoD), which participates in FedRAMP, requires that cloud providers bidding for defense contracts keep national security-related data in the United States – as France does under its SecNumCloud counterpart program. However, DoD does not – unlike SecNumCloud or the proposed new ENISA rules – demand majority domestic ownership as a prerequisite to competing for a defense cloud computing contract. If the EU were to exclude majority foreign-owned cloud providers, there could be pressure on FedRAMP to retaliate in kind.

Including majority domestic local ownership requirements may well be inconsistent with international trade obligations, a U.S.-based observer has pointed out. Two sets of rules, both promulgated by the World Trade Organization (WTO), govern cross-border provision of services: the Government Procurement Agreement (GPA), which addresses government acquisition specifically, and the General Agreement on Trade in Services (GATS), which applies more broadly.

The GPA requires that any state party treat foreign companies supplying cloud services on a cross-border basis to government entities no less favorably than locally-established suppliers (the principle of 'national treatment'). GATS contains similar national treatment commitments, as well as a right to market access in sectors including computer and related services. Both agreements allow exceptions for national security, privacy, and other public policy interests. There is little WTO precedent in applying the GPA and GATS to cloud services, however, so the outcome of any potential dispute settlement proceeding would be highly uncertain.

A Better Way Forward

Majority local ownership requirements are not only of doubtful legality under WTO rules; they are also, as previously noted, ineffective at excluding foreign jurisdiction such as that exercised by U.S. national security and law enforcement authorities. There are, however, promising consensual avenues to mitigate Europe's long-standing grievance over the extraterritorial extent of U.S. law.

The first of these is TADPF, the intended successor to the Privacy Shield data transfer framework. The United States and the European Union reached political agreement on the new Framework in March 2022; details on how Washington will implement it are expected to be released this fall. The White House has announced that the United States will adopt the same 'necessity and proportionality' standard utilized in Europe for conducting foreign intelligence surveillance. In addition, Washington will institute new administrative and judicial redress procedures for Europeans who consider their privacy rights to have been violated by the NSA. These new measures should establish essential equivalence between U.S. and EU law relating to foreign intelligence surveillance, and thereby directly address the concerns expressed by the CJEU in *Schrems II* about the reach of U.S. authorities. An important by-product of TADPF thus would be to undercut the EU's cybersecurity rationale for demanding immunity from U.S. national security law.

A second, albeit less-advanced, negotiation could substantially address Europe's objection to U.S. law enforcement's extraterritorial exercise of its powers under the U.S. CLOUD Act. In 2019, Washington and Brussels embarked on talks to reach an international agreement streamlining the procedures for government acquisition of foreign-located electronic evidence needed in domestic criminal proceedings. A separate section of the CLOUD Act empowered the U.S. Department of Justice to negotiate such executive agreements. The accord would enable law enforcement to obtain e-evidence directly from providers of communications services – rather than relying on governments to mediate the mutual legal assistance requests – but subject to new due process protections. The first CLOUD Act agreement, with the United Kingdom, has been completed.

The talks with Brussels have languished in recent years, however, while the EU struggles to finalize a new regulation it needs to enable direct access to e-evidence (discussed previously on this blog). In June, though, the outgoing French EU Presidency succeeded in brokering a tentative compromise on several contentious elements of the proposed regulation with the European Parliament and the Council of the European Union. Once the e-evidence regulation is agreed, the path would be clear for the EU and the United States to resume bilateral negotiations.

If U.S. law enforcement requests for e-evidence were made pursuant to an international agreement with the EU – as opposed to under the unilateral authority

contained in the CLOUD Act – Europe would no longer be able to claim infringement of its judicial sovereignty. Thus, as in the national security realm, its rationale for insisting that providers of cloud services to European governments be immune from foreign law would drop away. Both the United States and the European Commission therefore need to commit to restarting their e-evidence negotiation as soon as the legislative roadblock in Brussels is definitively removed.

Finally, the EU and United States should consider utilizing the Trade and Technology Council (TTC), established last year, as a venue for discussing their respective approaches on foreign provision of cloud services to governments. One of the goals of the TTC's Global Trade Challenges working group is to share information on "discriminatory treatment of foreign companies and their products and services in support of industrial policy objectives," according to Annex V of the TTC's inaugural joint declaration. Although this language was probably written with China in mind, it does provide a potential "early warning" opportunity for restrictions in the transatlantic market as well. Since ENISA's cyber certification measure is still being debated within the EU, the TTC working group could serve as a useful bilateral forum for analyzing its proper extent.

Washington and Brussels should seize upon these collaborative approaches to resolve the looming transatlantic dispute over the EU's proposed cybersecurity certification measure. Otherwise, they appear doomed to yet another rancorous and difficult transatlantic technology policy conflict. At a time when government leaders on both sides of the Atlantic are concentrating on major economic challenges brought on by the Ukraine war, they should avoid adding disruption in cloud services to the list.