THE SECOND COMING

That the *Schrems II* ruling would seek to impose requirements on a foreign country while not holding EU member states to the same standard smacks of hypocrisy, argues **John Dermody**

JOHN DERMODY IS A COUNSEL IN WASHINGTON DC AND A FORMER ATTORNEY AT THE DEPARTMENT OF HOMELAND SECURITY, WHERE HE ADVISED ON INTELLIGENCE, DATA SECURITY, AND PRIVACY MATTERS

FOR THOSE COUNTRIES THAT DO NOT SHARE AS CLOSE A LEGAL FRAMEWORK OR ARE NOT AS COMMITTED TO THE RULE OF LAW, THERE MAY BE FAR LESS WILLINGNESS TO ACCEDE TO THE PRIVACY DEMANDS OF THE EU

The Court of Justice for the European Union's (CJEU) recent *Schrems II* decision has unsettled the landscape for transferring data outside the EU. The decision invalidated the EU-US Privacy Shield – a key mechanism by which companies transferred data from the EU to the United States in a manner compliant with the *General Data Protection Regulation* (GDPR) – and raised questions about whether standard contract clauses (SCCs) remain a viable alternative data-transfer mechanism.

The logic underlying the CJEU's decision was that, because of the surveillance activities permitted by US law, the legal system of the US does not afford an "essentially equivalent" level of protection to EU residents as that provided by European law.

While European privacy advocates are celebrating the decision and pushing for swift and significant enforcement, the decision does no favours for member-state data-protection authorities who are now on a collision course with the US and other nations whose laws do not mirror the strictures of the EU. This conflict may well result in the reckoning that privacy advocates have long sought, but because *Schrems II* offers little room to accommodate powerful economic and fundamental national security interests, it may ultimately be privacy that suffers in the end.

In determining that US law does not ensure an essentially equivalent level of protection, the CJEU went beyond concerns with specific data-privacy protections and challenged the entire US foreign-intelligence apparatus. The CJEU specifically pointed to two authorities for electronic surveillance: section 702 of the *Foreign Intelligence Surveillance Act* and Executive Order 12333. Section 702 authorises the US Government to compel an electronic communications service provider to disclose information regarding a foreign person located outside the US.

Executive Order 12333, in contrast, authorises foreign electronic surveillance, but does not provide any authority to compel a company to cooperate with the US Government. It authorises, in layman's terms, run-of-the-mill spying that every nation engages in, including EU member states.

And because Executive Order 12333 generally authorises electronic collection outside the US, it has little relevance to the specific data protections companies rely upon in SCCs, binding corporate rules, or the now defunct Privacy Shield, to protect data that has already been transferred to the US. This makes clear that the CJEU's concern is not limited to protecting data transferred to the US, but rather the mechanisms by which the US collects foreign intelligence around the world.

Leverage point

Privacy Shield was at least a leverage point for the EU to extract privacy concessions from the US. It led to the *Judicial Redress Act* (which afforded EU residents data-access rights on a par with Americans to information held by the US Government) and *Presidential Policy Directive-28* (which set rules for the bulk collection of signals intelligence).

These steps may have been incremental and insufficient for some, but the reasoning of the CJEU leaves only the wholesale restructuring of the US national security system and, indeed, the constitutional structure of the US Government as a means to comply with its edict. To believe that such an outcome is remotely possible is to indulge in fantasies.

This is not to suggest that scrutiny and criticism of US intelligence activities are unwarranted. An activity that must, by its nature, be conducted in secret demands thoughtful adherence to rules and diligence in its performance. There are plenty of examples, both in the US and in Europe, of governments failing to meet those standards.

Many American politicians, including President Trump, have

PIC: SHUTTERSTOCK

been extremely critical of US intelligence activities – but it would be a mistake to think those critical views are borne out of a commitment to universal privacy rights or an interest in changing the constitutional structure of the US Government. The US Constitution grants prime responsibility over foreign intelligence activities to the executive branch, and there are significant limits on what matters the judicial branch can review. Regardless of political affiliation, there is scant appetite in the US to revisit these fundamental constructs.

Difficult issues

These are difficult issues touching upon core sovereignty concerns, which is, in part, why the *Treaty on the European Union* and the GDPR afford member states significant deference in national security and defence matters.

Indeed, according to the European Union Agency for Fundamental Rights, only a small fraction of member states provide their own citizens the protections and procedures that the CJEU would require of the US in order to be considered to provide an "essentially equivalent level of protection".

That the *Schrems II* ruling would seek to impose requirements on a foreign country while not holding member states to the same standard smacks of hypocrisy and undermines the decision's invocation of fundamental rights and freedoms.

And this tension now exists on a global scale because of the sweeping reasoning of the CJEU. If US law provides insufficient protections, then what is the status of other countries? For all the legislative and bureaucratic gymnastics made to bridge the divide between the US and the EU, the gap is far more significant with China, India and other nations, where companies in member states have significant operations and transfer significant amounts of personal data.

Privacy Shield was a product of good-faith negotiations between parties seeking to find common ground. For those countries that do not share as close a legal framework or are not as committed to the rule of law, there may be far less willingness to accede to the privacy demands of the EU.

On the front line

All of this leaves data-protection authorities on the front lines of a global privacy battle, with few tools to craft reasonable solutions. The CJEU's passionate intensity in pursuing privacy protections without consideration of other concerns – which, to be fair, was their charge – now means that data-protection authorities are likely stuck between harsh universal enforcement, abdication of their obligations under *Schrems II*, and arbitrary enforcement against the largest and most powerful data exporters. This will place enormous pressure on companies, who will, in turn, place enormous pressure on politicians, both inside and outside the EU to develop solutions.

Data localisation may mitigate some concerns, but is not an adequate solution for a global-information economy predicated on the mobility of personal information. The far more likely outcome is coordinated international pressure from countries demanding that the EU amend fundamental aspects of the GDPR, or even more foundational documents.

The GDPR has been transformational in advancing privacy protections for EU residents and in laying the groundwork for other progressive privacy efforts, like the *California Consumer Privacy Act*, which provides GDPR-like protections to residents of California. But the unyielding approach of *Schrems II* removes the ability of data-protection authorities to navigate competing interests, creating tensions that may result in compromises being codified in underlying data-protection laws.

Privacy advocates may be celebrating the intractable conflict that *Schrems II* has set in motion, but the fate of fundamental privacy protections is far from assured. g