CENTRE FOR EUROPEAN REFORM

Adrift: The impact of the ECJ's Safe Harbour ruling

by Camino Mortera-Martinez and Rem Korteweg

On October 6th, the European Court of Justice (ECJ) suspended the 'Safe Harbour' transatlantic agreement on data flows. In doing so, the Court overstretched its competence by answering a question it was not asked, and in the process changed the way the internet is governed. The decision has created legal uncertainty about whether companies can move data from the EU to the US.

To avoid costly and wasteful bureaucracy inhibiting online commerce, the EU urgently needs to strike a new transatlantic deal on data flows. The Commission hopes to secure a new Safe Harbour agreement with the US. However, this agreement would not be immune from legal challenge in Europe. The US will insist that a new agreement has a national security exemption, meaning that the US National Security Agency (NSA) may continue to examine EU citizens's data for security purposes. Therefore, a transatlantic agreement establishing when European countries and the US may violate privacy is required in addition to a new Safe Harbour agreement.

The ECJ's decision came after Maximilian Schrems, an Austrian law student, took legal action against Facebook for breaching EU data protection laws. The Safe Harbour agreement allows EU citizens' data to be transferred to other countries if their laws ensure an adequate protection of privacy. In 2000, the European Commission recognised that the US met that requirement. (Similar agreements exist with 11 countries, including Canada, Argentina and Israel). Companies that certified their compliance with Safe Harbour's privacy principles were allowed to transfer data from Europe to servers located in the US. Schrems argued that Edward Snowden's revelations about the NSA's surveillance programme proved that the US violated EU privacy rights. He demanded that Facebook stop transferring his data to American servers. The Irish upper court (Facebook has its European headquarters in Ireland) referred the case to Luxembourg. It asked the ECJ to establish whether Safe Harbour gave national data protection authorities the power to examine a potential breach of privacy rules.

The ECJ ruled that national authorities may do so. But it also decided to examine whether the US met the Safe Harbour principles. The EU judges decided that the US did not, because of Snowden's disclosures. This may or may not be true, but what is surprising is that neither the US government nor Facebook were part of the proceedings. Their positions were not heard

and the Court took its decision on the basis of third party allegations. This was wrong and has justifiably sparked ire in the US.

The ECJ ruling entails several bad consequences for Europe. It creates regulatory uncertainty for those 4,500 companies that rely on transatlantic data flows for some or all of their activities, including IT and internet firms, as well as banks, retailers and manufacturers.

The regulatory burden arising from the ruling will be more easily borne by large digital incumbents, which are mostly American, precisely at a time when the Commission hopes to give a boost to European digital start-ups. After the ruling, the Commission issued guidelines explaining how companies can continue to send data legally to the US. But the guidelines give few details.

In the meantime, businesses have to rely on cumbersome ways to work around the problem. These include 'model contracts': clauses agreed with EU authorities on data transfers between EU and non-EU companies, or individuals. But these contracts could also be open to legal challenges. Then there are 'binding corporate rules' – bespoke agreements adopted by corporations, and requiring EU approval – which govern data transfers between a company's operations in different countries. These rules are costly to draft and the EU must agree them with every company separately. The most wasteful, but possibly more legally robust solution, would be for companies to build data storage centres in Europe to hold EU citizens' data, rather than transferring it to the US. In November, Microsoft unveiled plans to set up such a centre on German soil. Only large companies can afford this approach.

The ruling may also erect barriers to data flows within the EU. The ECJ has allowed all 28 national data protection authorities to review the adequacy of privacy standards in countries outside the EU. National data watchdogs may interpret these non-EU standards differently, leading to a situation where data could be transferred legally to America from one member-state but not another.

The Court's decision could contribute to the fragmentation of the internet. One of the internet's main benefits for citizens and companies is the free flow of information across the globe. An open internet is in Europe's interest. By contrast, China, Russia and other authoritarian countries are seeking more national control over it. The EU has been co-operating with the US and others at multilateral forums, like the Freedom Online Coalition, to keep the internet open. But Europe's credibility is now tarnished, as the ECJ has questioned the exchange of data between two of the staunchest proponents of a global internet.

The disagreement over transatlantic data flows may also undermine the continuing transatlantic trade talks: while TTIP is intended to reduce transatlantic trade barriers, the ECJ is raising them. European officials have hinted that TTIP might cover data protection – negotiations are underway on e-commerce and other sectors that require transatlantic data flows – but the Schrems ruling means that a solution cannot wait that long. And it is possible that the recently concluded trans-Pacific trade deal, TPP, will allow US digital firms to expand more easily in Asian markets than in Europe. In Asia, US data standards are likely to be more readily accepted, while Europe's cumbersome data protection landscape may inhibit the roll-out of new services.

The privacy of European citizens must be protected, but the EU should refrain from the damaging posturing shown in the Schrems ruling. A new Safe Harbour agreement is in the works. However, the new agreement could be delayed beyond January. The Commission has said it will not investigate cases of non-compliance with the ECJ ruling until then, but if negotiations drag on, US companies could become liable to penalties. And a new agreement is unlikely to assuage the ECJ's concerns. The deal's national security exemption will probably give the NSA continued access to data from European users.

The irony is that, after the Snowden affair, the US has increased judicial scrutiny of the NSA, while some European countries, such as France, the Netherlands and the UK, have given more powers to their intelligence services with limited legal oversight. What is needed, beyond a new Safe Harbour agreement, is for Europe and America to agree on principles governing intelligence gathering – through a bilateral agreement setting limits on unwarranted surveillance, for example. They should also explore the possibility of adopting a treaty on commercial data transfers, which may be possible should the US adopt a federal data protection law to replace its out-dated 1974 Privacy Act. Till then, the ECJ has put many firms in legal limbo, and it has inhibited Europe's digital ambitions.

Camino Mortera-Martinez
Research fellow, CER
Rem Korteweg
Senior research fellow, CER

This article is part of a longer paper sponsored by OSEPI.