qLegal at the Legal Advice Centre
lac@qmul.ac.uk
qlegal.qmul.ac.uk

Date produced: 18/12/2015

qLegal Legal Update
Cybersecurity & Data Protection legal update
ECJ Schrems Decision & Business Consequences

Cybersecurity and data protection have become increasingly important issues as the internet has expanded. The laws addressing these areas differ between the US and EU however, and for these reasons the risk of conflict is significant. The recent ECJ ruling in Schrems perfectly highlights how serious the consequences of differing frameworks can be, insofar as it can effects the privacy of individuals.

SCHREMS' CASE

The action initiated by Maximilian Schrems against Facebook, after Edward Snowden's revelations concerning the activities of the US intelligence services, and the consequential ruling of the European Court of Justice (ECJ) on 6 October 2015 is likely to have important implications for the current data protection framework and impact law reform both in Europe and the US.

In the case at issue, the ECJ has considered the request for a preliminary ruling from an Irish court, dealing with the powers available to the national supervisory authorities regarding the transfer of personal data to a third country and the definition of the "adequate" level of data protection. To deal with the issue, the Court started its analysis by considering the current framework, in order to clarify it. Two EU acts have been considered: Directive 95/46 ('Directive') and Decision 2000/520 ('Decision'). While the first one defines the adequacy of protection as the criteria to allow data transfer to a third country, the second, more specifically considers the US "Safe Harbour" scheme as able to ensure an adequate level of protection for data transfer in the United States in certain circumstances. The Commission's competence to adopt such decisions is set out in Article 25(6) of the Directive.

In this regard, the ECJ needed to address two different problems. The first one, related to a procedural issue, concerned whether national supervisory authorities can exercise their investigative powers in spite of the existence of a previous act of the Commission, i.e. the Decision. The second, a substantial issue, involves the validity of the Decision, taking account of the recent introduction of the Charter of Fundamental Rights of the European Union ('Charter') that in its Articles 7 and 8 expressly mentions the respect for private life and the protection of personal data.

qLegal at the Legal Advice Centre
lac@qmul.ac.uk
qlegal.qmul.ac.uk

With regard to the procedural issue, the ECJ held that the independence of national supervisory authorities must not be denied in any circumstance. This means that, as required from Article 28(1) of Directive 95/46 Member States have to set up one or more public authorities responsible for monitoring, with 'complete independence', compliance with EU rules on the protection of individuals with regard to the processing of such data.

The national supervisory authorities have a wide range of powers for that purpose that are listed on a non-exhaustive basis in Article 28(3) of the Directive. In particular, inter alia, they have investigative powers, effective powers of intervention, and the power to engage in legal proceedings. In light of this, even a Commission decision cannot reduce these expressly accorded prerogatives, preventing persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim concerning the protection of their rights and freedoms.
Furthermore, apart from the contrast with the Directive's aim, a similar situation would be contrary to the system required by Art.8(3) of the Charter and Art. 16(2) Treaty on the Functioning of the European Union, resulting in an unacceptable reduction of EU citizen rights in the third country.

The second point to consider deals with the Charter provisions, at articles 7 and 8. In this new context, legislation permitting foreign public authorities to have access on a generalised basis to the content of electronic communications, as evidenced through Snowden's revelations, as well as the lack of legal remedies for EU citizens before US courts, would compromise the Charter rights. In fact, looking at the US situation, it is evident that the absence of provisions intended to limit interference with fundamental rights, together with the adoption of a broad interpretation of the Safe Harbour scheme involving the abuse of derogations and, moreover, the fact that it is applicable only to undertakings and not to public authorities, do not constitute an "adequate" level of protection in the US.

For these reasons, the ECJ concluded thatstates on one hand the independence of national supervisory authorities required them to evaluate 'adequacy' decisions of the Commission; on the other, it considers the Decision invalid itself because it does not comply with the standard of adequacy ruled by the Directive, compromising the respect of fundamental rights of EU citizens.

Consequences for Businesses

As a result of the ECJ ruling in Schrems, data controllers can no longer necessarily rely on Safe Harbour to transfer data of EU users to US data controllers and processors.

The implications of the Schrems ruling extend further than the data protection policies of individual companies. A fundamental conflict between EU rights and US security law emerges.

This places companies whose business involves conducting transatlantic data transfers in a legal grey area. No amended Safe Harbour provisions yet exist to dictate a new standard of protection for transatlantic transfers of data.

qLegal at the Legal Advice Centre
lac@qmul.ac.uk
qlegal.qmul.ac.uk

Companies such as Facebook, Google and Microsoft also rely on the EU Model Contracts (e.g. Decision 2001/497) as a basis for the transfer of personal data to the US.

The ECJ has yet to consider the validity of the EU Model Contracts. Certain commentators view model contracts as makeshift measures to assuage the tensions of clients, and suspect they too may fall foul of the ruling. Legal scholar Timothy Edgar believes it will just be a matter of time until model contracts are struck down in the EU, especially considering some German authorities have struck them down already. Edgar thinks that a reform of US surveillance law may ultimately be needed. Alternatively, Edgar suggests that a more comprehensive Safe Harbour agreement should be reached.

Efforts are already being made at legal reform in this area however. The United States Congress is in the process of adopting the Judicial Redress Act of 2015, which would allow actions by EU citizens against US public authorities before US courts, regarding their use of EU users' data obtained from American companies. In September 2015, the EU and U.S. finalised the 'Umbrella Agreement', which will provide safeguards and guarantees of lawfulness for data transfers, and a harmonized framework for transfers of personal data between the EU and the U.S. for the purpose of prevention, detection, investigation and prosecution of criminal offences. The EU reform process is being finalised and this may create further barriers to international data flows as EU law becomes more restrictive and new issues for the ECJ to consider.

Businesses would benefit from further cooperation between authorities in the area of data protection, and from the greater clarity that a new Safe Harbour would provide to companies operating on both sides of the Atlantic.

This legal update was drafted by students from the Centre for Commercial Law Studies, Queen Mary University of London: Michael Gallagher, Kasajja Byakika, and Federica Pezza.