SAFE HARBOUR NOT SAFE ENOUGH: DATA TRANSFERS FROM E.U. TO U.S. OUT TO SEA

Posted on October 17, 2015

Categories: Insights, Publications

The transfer of personal information from the European Union (EU) to the United States (US), and potentially other non-EU nations, just became a lot more complicated.

The Decision

On October 6, 2015, the Court of Justice of the European Union (CJEU) released its decision in *Schrems v Data Protection Commissioner*.[1] The Schrems decision will have a significant impact on the ability of businesses to transfer personal data from the EU to the US, and potentially to other non-EU countries as well. The decision contains two important holdings: (1) that companies can no longer rely on compliance with safe harbour principles to transfer personal data from the EU to the US, and (2) that the supervisory authority in each EU Member State has the right to review whether non-EU countries provide adequate data-protection policies to permit cross-border data transfers.

The EU Data Protection Directive requires that transferred information maintain the high degree of protection that exists under EU law.[2] The requirement to protect EU-based data is especially problematic when data is transferred to the US, which has not adopted a general privacy law comparable to what exists in the EU. This problem was traditionally solved by the adoption by the EU Commission Decision 2000/520, which permitted transfers where businesses independently pledge to comply with particular safe harbour principles. However, *Schrems* invalidates this solution.[3]

Importantly, the CJEU also ruled that while the supervisory authority of each Member State cannot invalidate an EU Commission decision acknowledging the existence of adequate protections, it has the right to examine such findings on adequacy with respect to complaints before it.[4] This finding deviates from the traditional view that a decision by the EU Commission that a particular non-EU nation has adequate data protection laws is conclusive. The CJEU clarified that supervisory authorities are indeed equipped to conduct their own adequacy analysis.[5]

In *Schrems*, the complainant filed a complaint with the Irish Data Protection Commissioner alleging that his personal information would not be adequately protected when transferred to the US, given the US surveillance activities that were revealed by Edward Snowden.[6] The revelations with respect to the indiscriminate surveillance activities of US intelligence agencies demonstrate the ability of public agencies to lawfully access data within their jurisdiction. The CJEU found that such practices undermine any commitments by companies to comply with the safe harbour principles and protect personal data from unauthorized disclosure. On this basis, the court found that the surveillance ability of public agencies in the US are not compatible with Decision 2000/520.[7]

Implications for Canadians

While Decision 2000/520 relates to the transfer of personal data between the EU and the US, there are significant implications for Canadians as well. Firstly, Canadian businesses that transfer data between the EU and the US are directly impacted by the CJEU's decision.

In addition, the decision in *Schrems* gives rise to the possibility that transfers of personal data from the EU to Canada could be impacted in the future. In December 2002, pursuant to decision 2002/2/EC, the EU Commission found that the *Personal Information Protection and Electronic Documents Act* (PIPEDA) provides adequate protection for personal information, thereby enabling the exchange of personal information between EU member states and Canada (where PIPEDA applies). However, privacy and data protection laws in the EU are in the process of rapidly developing and it is arguable that a chasm is widening between PIPEDA and the EU laws. The CJEU's holding that supervisory authorities of EU Member States are entitled to examine findings of adequacy will permit supervisory authorities to conduct an independent analysis of PIPEDA's adequacy going-forward.

What happens next?

Given the global nature of businesses in today's marketplace, *Schrems* gives rise to an urgent need to implement a solution for the transfer of personal data from the EU to the US. On October 14, 2015, the European Parliament announced that it would have EU commissioners and councillors address its plenary.[8]

The European Parliament has indicated a need to ensure effective data protection for EU citizens.[9] However, at the same time, businesses need to have a practical and efficient solution to minimize disruption to international commerce.

It will be important for all businesses and privacy professionals to closely monitor developments following *Schrems*, including Canadian businesses that transfer personal information to the EU or that receive transfers

of personal information from the EU.

by Lyndsay A. Wasser and Mitch Koczerginski

[1] [2015] EUCJ C-362/14 (06 October 2015) [*Schrems*].

[2] EU Directive 95/46/EC, Art. 25(1).

[3] *Schrems* at 106.

[4] Ibid at para 66.

[5] Ibid.

[6] Ibid at para 28.

[7] Ibid at para 98.

[8] Sam Pfeifle, *Safe Harbor Fallout: Commission, Council Dabate Parliament; German DPA Takes Next Step* <https://iapp.org/news/a/safe-harbor-fallout-commission-council-debate-parliament-german-dpa-takes-next-step>.

[9] Ibid.

A Cautionary Note