Extraterritorial Application of The GDPR - Lessons from Recent Developments

November 8, 2018 – The TMCA
by Ron Moscona and Clint Conner

The EU General Data Protection Regulation (GDPR), billed as the most important development in data privacy regulation in at least 20 years, arrived with a bang in May of this year and companies have been scrambling to implement compliance measures that will avoid its stiff penalties.

Some uncertainty relates to how and to what extent the GDPR will be enforced outside the EU. The GDPR expressly applies to any organization outside the EU that processes personal data of individuals in the EU in connection with offering goods or services to such individuals or monitoring their behavior, and the GDPR requires such organizations to designate a representative within the EU (seemingly intended to facilitate enforcement). As a practical matter, it is unknown how its requirements will actually be enforced against entities outside the EU and there is as of yet no regulatory guidance on this issue.

A recent development out of the UK highlights the extraterritorial enforcement issue. In July, the Information Commissioner's Office (ICO), which is the UK's data protection regulator, issued its first ever GDPR "enforcement notice" against an entity located outside the UK. That entity is AggregateIQ Data Services Ltd ("AIQ"), a Canadian company.

The ICO investigated AIQ's involvement with Cambridge Analytica's alleged use of EU citizens' Facebook data for analytics for the Brexit political campaign. AIQ disputed allegations that it is affiliated with Cambridge Analytica and refused to fully cooperate with the ICO's investigation, taking the position that it is not subject to the ICO's

Related People

- Ron Moscona

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

jurisdiction. Nonetheless, based on the evidence it was able to collect, the ICO found that AIQ violated the GDPR by, among other things, processing personal data of EU citizens in a way that the individuals were not aware of, for purposes which they would not have expected, and without a lawful basis.

The ICO's GDRP enforcement notice ordered that AIQ stop processing "any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes" within 30 days of the notice date. Failure to comply with such a notice could result in the ICO issuing a fine of up to 20 million euros or 4% of the company's annual worldwide revenue, whichever is greater.

AIQ appealed the enforcement notice to the first-level tribunal arguing that the ICO did not have jurisdiction over the company, the GDPR did not apply because the alleged conduct had taken place before the GDPR was in force, and the notice was too broad. The ICO thereafter issued an amended enforcement notice that, according to the ICO, clarifies the steps AIQ must take in order to comply with the notice. The ICO's amended notice orders AIQ to delete any UK personal data on AIQ's servers that the company had told the ICO it held in May 2018. AIQ has since withdrawn its appeal and indicated it will comply with the amended enforcement notice.

It is important to note that Canada's Office of the Privacy Commissioner and British Columbia's Information and Privacy Commission ("BCIP") had been working in close cooperation with the ICO in the investigation of AIQ since late 2017. Canada has its own privacy laws applicable to AIQ's alleged conduct – Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which will come into effect on November 1, 2018, and the Personal Information Protection Act (PIPA) applicable in certain provinces.

This suggests that Canadian authorities might be willing to assist with GDPR enforcement against Canadian companies, at least in high-profile cases that impact Canadians (even if indirect). The Canadian government's willingness to do so likely relates to the fact that Canada has its own privacy laws similar to GDPR that it must enforce and to the close historical ties between Canada and the UK. This case also suggests that a non-EU company would likely comply with a GDPR enforcement notice in cases where that company's government assists the EU's investigation.

However, there are still many outstanding questions regarding extraterritorial enforcement of the GDPR. This case provides little insight regarding the extent to which other non-EU countries would assist with executing a GDPR investigation or enforcement notice against one of their own companies, and does not forecast what a non-EU company served with a GDPR enforcement notice would do in situations where local authorities do not get involved.

Presumably, non-EU companies with significant assets in the EU that the EU government is able to seize, or having business interests in the EU that they wish to pursue, would feel compelled to satisfy GDPR enforcement notices in order to avoid the

stiff GDPR penalties or repercussions in terms of their freedom to conduct business. But what about other companies located in countries that, unlike Canada, would not get involved in a GDPR investigation or enforcement? So far, the international community has not developed a system for cross-border enforcement of privacy rights. It is unlikely that such a system will be put in place at least until a reasonable level of harmonization is achieved in the approach to data protection adopted across different jurisdictions. As long as countries continue to take very different approaches to data protection and privacy, it is likely that the existing international arrangements for the mutual recognition and enforcement of judgements will not be very effective in relation to enforcement orders and penalties imposed by national authorities for the infringement of such rights.

For the same reasons, it remains unclear how GDPR enforcement would play out in the United States. The U.S. currently has no federal law similar to the GDPR. The Trump administration is discussing a U.S. version of the GDPR that would have provisions similar to provisions in the GDPR, but the passage of such a law is not imminent. To the extent the U.S. enacts such a law, the U.S. might be incentivized to assist with GDPR investigations or enforcement against U.S. entities at least to the extent consistent with the terms of the U.S. law for purposes of encouraging reciprocal comity with the EU. However, given the Trump administration's foreign policy stance, it is highly unlikely that the U.S. would assist in enforcing violations of any GDPR provisions that go beyond the U.S. law.

In June, California enacted the California Consumer Privacy Act of 2018 ("CCPA"), which is similar in some respects to the GDPR. It remains to be seen whether the California Attorney General's office would assist with a GDPR investigation of a California company to encourage reciprocal comity with the EU in connection with enforcement of their respective data privacy laws.