CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

WEDNESDAY, NOVEMBER 18, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 226

How invalidation of EU-U.S. Safe Harbor framework may affect U.S. companies

It's very unusual for a decision of a foreign court on a technical subject such as data transfer to make headlines in the United States, but an October ruling by the Court of Justice of the European Union, Europe's highest court, has resulted in dozens of articles in newspapers like the New York Times and Wall Street Journal and in technology-focused and industry-specific publications.

While many of the articles don't even mention the case by name, the CJEU's decision in *Schrems v. Facebook* may have a significant impact on both U.S. and European companies. In *Schrems*, the CJEU called into question the legality of trans-Atlantic data transfer practices and sparked alarm in American companies that have relied on the now-invalidated EU-U.S. Safe Harbor framework since its adoption in 2000.

Thousands of companies — both in the United States and abroad — have had to assess the adequacy of their data transfer practices and, in many instances, will have to adopt new measures to achieve ongoing compliance with the EU Data Protection Directive.

The CJEU's decision in *Schrems* also opens the door for the potential invalidation of other modes of data transfer previously viewed as legitimate. Warnings of the death of cross-border data transfers may be premature, however, since neither the European Union nor the United States want to dam the flow of transnational data on which countries, companies and individuals have come to rely.

American and European regulators are working to forge a new framework to replace the invalidated EU-U.S. Safe Harbor.

At the same time, the *Schrems* decision has turned the spotlight on the U.S. data security and consumer privacy landscape and will likely result, perhaps sooner than later, in changes that will impact all companies that collect, use or store consumer data, whether they engage in cross-border data transfer or not.

Background on the ruling

Although data privacy has become an increasingly pressing issue in the U.S., Europe approaches privacy as a fundamental right — and this approach has produced legislation more protective of data privacy and security laws. (Indeed, last year's "right to be forgotten" ruling was another headline-grabber, holding that individuals possess a right to have information such as news stories removed from search engines when the information is inadequate, irrelevant or excessive.)

The EU Data Protection Directive allows the transfer of personal data to countries outside of Europe only upon the condition that the country receiving the data transfer offers adequate legal protections to safeguard that data.

EU data authorities have given officials in the U.S. Department of Commerce and the European commission until Jan. 31 to put into place a revamped framework ...

Because the European Commission regarded American privacy laws as inadequate, the commission worked with the U.S. Department of Commerce to create a Safe Harbor framework that would allow U.S.-based companies to engage in trans-Atlantic data transfers. To receive protection under the framework, companies had to self-certify that their data protection practices adequately address the European commission's core privacy principles (exceeding what may be required under existing U.S. laws).

The *Schrems* decision followed a dispute between an Austrian citizen and the Irish Data Protection Authority, in relation to concerns about the transfer of the claimant's personal data by Facebook's Irish subsidiary to servers located in the United States. The claimant asserted that, notwithstanding Facebook's self-certification under the Safe Harbor, the social media company could not ensure adequate data protection.

In particular, the claimant focused on Edward Snowden's leaks of NSA surveillance activities, maintaining that U.S. privacy laws do not protect personal information from government surveillance and that U.S.-based companies, such as Facebook, can therefore not ensure the privacy of their users. The CJEU was asked to determine whether the Data Protection Authorities of EU member states are bound by the European commission's ruling on the adequacy of the Safe Harbor framework.

The CJEU held that it was the ultimate authority for determining whether a European commission's decision is valid, and data protection authorities, in addressing a claim brought by an EU citizen, are not bound by the European Commission's determination. The court went on to hold that the Safe Harbor framework was inadequate to ensure the data privacy of EU citizens, in part because of the potential for government and law enforcement intrusions on privacy and the lack of judicial redress in the United States for affected EU citizens.

What's the real impact?

The decision affects any company that previously relied on the Safe Harbor — large and small companies across a range of industries. Most obviously, the decision affects U.S.-based social networks and providers of data hosting, storage, cloud services and data analytics.

But EU-based companies are also affected if they engage the services of American companies in a manner that involves data transfer, such as European cloud services that manage the data of EU citizens but use servers in the United States.

The ruling also affects multinationals, regardless of industry, if they transfer data internally across borders, whether the data relates to customers or employees. About 4,000 companies have self-certified under the Safe Harbor framework and must now reconsider

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.

their data privacy practices and compliance plans.

While the CJEU's decision justifiably has incited anxiety among companies relying on the Safe Harbor, there are reasons to give pause before investing substantial compliance resources. Legally, the CJEU ruling did not in fact hold that Facebook violated the claimant's privacy rights. Rather, the court invalidated the Safe Harbor as a defense against liability and sent the case back to Ireland.

The point here is that the collapse of the Safe Harbor did not equate to instant liability for every company self-certifying under the framework. In the wake of the decision, the data privacy community immediately looked to company-specific solutions — particularly, contractual solutions to replace the Safe Harbor as a defense against liability.

EU data authorities have given officials in the U.S. Department of Commerce and the European commission until Jan. 31 to put into place a revamped framework before they will initiate any enforcement actions.

And on Oct. 26, less than three weeks after the CJEU released its ruling, the EU commissioner announced that EU and U.S. regulators had reached an "agreement in principle" with expedited negotiations ongoing to work out "how to ensure that these commitments are binding enough to fully meet the requirements of the court."

Regulators on both sides of the Atlantic recognize that cross-border data transfers are critical and that a near-immediate "fix" is necessary to ensure that fundamental privacy rights are protected without derailing U.S-EU commerce.

Regulators in the United States have called for a regime that is effective and transparent. The FTC, in particular, has exercised its enforcement powers around the Safe Harbor framework, and in a recent speech, FTC Commissioner Julie Brill emphasized the agency's role in prosecuting unfair and deceptive practices, including a company's failure to live up to its avowed privacy policies.

Lawmakers and technology industry representatives also seem to recognize that, although a new EU-U.S. data transfer framework is critical, the United States will soon need to enact stronger data security and privacy laws.

In separate hearings on Nov. 3 before the House Energy and Commerce Committee and the House Judiciary Committee, members of the House, representatives from tech industry trade groups and privacy advocates reportedly called for stronger national data security standards, federal consumer privacy legislation and reforms to government surveillance practices, including those that influenced the CJEU's decision to invalidate the Safe Harbor.

Given all this, the regulatory landscape surrounding data privacy and security is certain to evolve over the coming weeks and months, although the full impact of the Schrems decision remains to be seen.