Safe Harbor Ruling Leaves Data Center Operators in Ambiguity

BY YEVGENIY SVERDLIK ON OCTOBER 9, 2015

Europe's annulment of the framework that made it easy for companies to transfer data between data centers in Europe and the US while staying within the limits of European privacy laws has caused a lot of uncertainty for businesses that operate data centers on both sides of the Atlantic.

US cloud services giants have taken steps to make sure they continue to provide services legally using means other than the Safe Harbor framework, but actual consequences of the European Court of Justice ruling earlier this week remain unclear.

David Snead, an attorney and co-founder of the Internet Infrastructure Coalition, a US advocacy group whose members include Google, Amazon, and Equinix, among many others, said there were currently two "schools of thought" on the subject.

"One is that Safe Harbor is dead," he said." The other, which I think is actually the accurate answer, is that the European Union, and the European Commission in particular, need to figure out how to interpret the ruling."

Internet businesses will continue to operate in ambiguity until the commission issues its interpretation.

"It is unrealistic to think that all transatlantic data is going to have to stop as a result of this decision," Snead added. "The European Commission is likely to figure out a way to accommodate it, and the US is as well."

Safe Harbor, created in 2000, is a uniform set of rules for handling personal data of citizens of member states of the European Union, including rules around moving that data to facilities in the US and storing it there. If a service provider complied with the rules, they could be confident that they were not breaking any European privacy laws.

Former NSA contractor Edward Snowden's public disclosure of the US spy agency's covert electronic surveillance practices, however, eroded trust in Safe Harbor. The court's ruling this week that Safe Harbor led to privacy violations was a culmination of a process that started with a lawsuit by Austrian privacy advocate Max Schrems in Ireland against Facebook, charging that the social network was violating his privacy rights by complying with the NSA.

The court in Ireland sided with Facebook, citing Safe Harbor. Schrems's appeal with the EU court resulted in this week's ruling.

Model Clauses Not for Everyone

Choosing not to wait for the European Commission's interpretation of the ruling, Amazon, which operates the world's largest cloud services business with customers around the globe, has obtained an approval from EU data protection authorities for a data protection agreement and so-called "model clauses," which according to the company enables it to continue serving its European customers legally.

"With our EU-approved [Data Protection Agreement] and Model Clauses, AWS customers can continue to run their global operations using AWS in full compliance with EU law," an AWS spokesperson said in an emailed statement. "The AWS DPA is available to all AWS customers who are processing personal data, whether they are established in Europe or a global company operating in the European Economic Area."

Other US cloud giants, including Salesforce, Microsoft, and Google, have also taken the model-clause route.

Model clauses are model data privacy agreements individual EU members can make with companies to give them assurances that they're operating within legal limits. While any company can use this approach, it is a cumbersome process, Snead said. They sometimes have to be negotiated, and not all EU members have model clauses approved.

Service Providers Left Fending for Themselves

Operating in Europe without Safe Harbor is going to be a lot more complicated. Model Clauses or not, privacy rules in countries like Germany, for example, are very strict, and now that there isn't a blanket compliance framework, service providers are left fending for themselves in each European market.

"This is an unfortunate and costly ruling and undermines the long-standing commitment that infrastructure providers have used to implement data protection methods for customer data," Andreas Gauger, chief marketing officer and co-founder at ProfitBricks, a German cloud services company, said in an emailed statement. "Quality IaaS providers provide customers with secure, cloud-based virtual infrastructure, and are flexible enough to … give customers control over their data, encryption methods, and data transfer methods."

Service Providers Not the Only Ones Affected

While cloud service providers are the most obvious category of businesses affected by the ruling, it can be disruptive for any international organization that has some part of its operations in the EU, Cliff Moyce, with Data Art, a New York-based software development and consulting company, said in an email.

Such organizations, including banks, for example, "will need to review their business processes, systems, controls, and agreements (including customer, supplier and personnel agreements) to ensure compliance for any data sharing and data transfer activity that crosses borders," Moyce said.

'Data Transfer' an Antiquated Concept?

The concept of "data transfer" is an old-fashioned one, Moyce added. Today, data is accessed rather than transferred. "Modern systems infrastructures mean that data can be accessed from anywhere," he said. "The secret to compliance is control of access, not control of 'transfer.'"

The Need for a Global Discussion on Surveillance

Fundamentally, the ruling should be a wakeup call to US Congress that "the world still cares about US surveillance activity, and that US needs to continue to show that it respects the privacy of the world's internet users," Snead said.

The conversation shouldn't be limited to the US, since government surveillance is an international issue, he added. "The reality is that you want to be safe from any governmental spying. No contract is going to keep the German government from spying on you or compelling your German data center to provide access to them without notifying you."

It is important to stop saying internet surveillance is a US government problem, a German government problem, or a Chinese government problem, Snead said. "This is a global problem, where governments are seeking access to data in ways that users don't know."

Original article — http://www.datacenterknowledge.com/archives/2015/10/09/safe-harbor-ruling-leaves-data-center-operators-in-ambiguity