Communications Daily

Counting Down

Privacy Experts Unsure About new US-EU Safe Harbor Deal as Deadline Nears

TOP NEWS | 28 Dec 2015 | Ref: 1512240011

The clock is ticking down for U.S. and EU negotiators trying to update the trans-Atlantic data transfer pact by Jan. 31, but several privacy experts who've been closely monitoring the situation said they're unsure whether a deal can be struck by that deadline. Negotiators on both sides of the Atlantic have indicated one is possible (see 1511160032), but it's predicated on several elements, namely limiting U.S. government surveillance access to Europeans' personal data and also giving individuals legal avenues through the Judicial Redress Act (HR-1428) in the U.S. if their personal information is misused. Once that informal deadline passes, national data protection authorities in Europe have said they would "take all necessary and appropriate actions, which may include coordinated enforcement actions." It means they could audit or prosecute companies for inadequately protecting personal data transmitted overseas.

The informal Jan. 31 deadline was “unrealistic” from the beginning for having all the safeguards in place, said Estelle Massé, a Brussels-based Access Now policy analyst. She referred, in part, to HR-1428, which the House passed Oct. 20 but the Senate Judiciary Committee tabled until next year. European negotiators have said the legislation is necessary to reach an updated safe harbor agreement (see 1511160032). But while the legislation would give EU citizens the right to seek redress in court if U.S. law enforcement agencies mishandle their data, Massé said it doesn’t address the issue of law enforcement agencies accessing their data that’s transferred by companies across the Atlantic.

"With holidays, immigration, terrorism and so many other issues on the table, and a very tight timetable, this has been a challenge and frustrating," David Turetsky, an Akin Gump cybersecurity, privacy and data protection lawyer, told us in an email, though officials from both sides have been working "very hard" on this agreement. While the Judicial Redress Act will need to be passed by the Senate, "it's not the only or key missing piece to conclude a new agreement," he wrote Tuesday. He said "the loss of safe harbor likely has the biggest impact on mid-sized and smaller companies because larger companies are more likely to be able to transfer data on another basis that may still be available. I think many of [the mid-size and smaller companies] are quite concerned."

"We have a tangled thorny problem where politics and economics intersect and the conflicting agendas of people need to be sorted out. It will take some time but it will get done. Too much is at stake," said privacy consultant Tim Sparapani, who was Facebook's first public policy director and is an ex-ACLU senior legislative counsel. He said Congress should also pass the Email Privacy Act (HR-699), which updates the Electronic Communications Privacy Act and could address the European Court of Justice's concern about U.S. government access to electronic communications and personal data.

The Email Privacy Act would require a law enforcement agency to obtain a warrant when it wants a company to disclose content of communications, which is the subject of an investigation, Sparapani said. It's the standard that law enforcement agencies now use, but it's not law. He lamented Congress' slow action on the bills, despite their popularity. HR-699 has more than 300 co-sponsors in the House, and similar legislation in the Senate also has significant support (see 1512030036). “Anywhere but Washington this would be done already," said Sparapani, who founded SPQR Strategies consulting firm.

Jens-Henrik Jeppesen, the Center for Democracy and Technology’s European affairs representative and director, told us Tuesday that negotiators haven’t been forthcoming with a lot of information on the talks’ progress. But he said they have no choice but to negotiate the best possible deal that can withstand scrutiny and a legal challenge “that will no doubt be raised against it.” He wrote in a blog post Monday that the federal government could make some changes administratively rather than legislatively, enabling companies to disclose “more detailed statistics about US Government intelligence surveillance demands” that would become part of the safe harbor “reporting requirements.” He wrote that the federal government could also disclose the subject matter for all certifications filed with the Foreign Intelligence Surveillance Court under Section 702 of Foreign Intelligence Surveillance Act (FISA).

He also told us long-term fundamental changes in surveillance are needed on both sides of the Atlantic. Citing a Dec. 10 speech that FTC Commissioner Julie Brill delivered at a privacy and data protection conference in Brussels, he said there needs to be a "realistic assessment" of the level of data protection in place rather than measuring the U.S. system against ideal legal standards that even some European states may not be able to meet.

Sparapani and Massé also agreed with that assessment. "Paradoxically, civil liberties are better protected in the U.S. than in Europe today," Sparapani said, saying surveillance has been stepped up among the Belgians, British, French, Germans and others since the Nov. 13 terrorist attacks in Paris. Additionally, Massé said Article 43a in the recently negotiated General Data Protection Regulation (see 1512160001) is known as the "anti-FISA clause" that was included following NSA document leaker

Edward Snowden's revelations. It's a further protection, but it's also conflicting legislation, she said. The "$10 million question" is how these laws will be reconciled and enforced, she said.

written by Dibya Sarkar
