POLITICO

U.S. to EU: Don’t scapegoat Safe Harbor over NSA

By ERIN MERSHON | 11/7/13 5:13 AM EST

EU concerns over the NSA have led to questions over a U.S.-EU data transfer mechanism. | AP Photo

U.S. regulators are urging their European Union counterparts to preserve a more than decade-old data transfer agreement amid mounting European anger over NSA spying.

An important but little-known mechanism, the Safe Harbor Framework, lets more than 3,000 companies, including Google and Facebook, process data from European citizens without running afoul of the region’s privacy laws. It has emerged as a friction point between the United States and EU as European officials move to tighten their data protection rules — an effort that has intensified in the wake of revelations about NSA surveillance. Some EU officials, alarmed by reports of the NSA’s work with Internet companies, say Safe Harbor gives U.S. tech firms a way to skirt their more stringent privacy regime.

U.S. officials, however, maintain that the Safe Harbor agreement is well-enforced and represents the best way to protect privacy across transatlantic data flows that serve millions of consumers. Compared with alternatives, the mechanism “provides more, not less, privacy protection,” argued Commissioner Julie Brill of the Federal Trade Commission in a speech last week.

Safe Harbor was formalized for the legal transfer of data between the U.S. and EU in 2000 after the EU passed a data-protection directive and determined that U.S. standards were “inadequate.” The framework consists of seven principles on topics like notice, choice and data security, broadly modeled on European standards. American firms that want to handle or store European citizens’ data have to self-certify annually with the Department of Commerce that they will abide by the standards. Breaches of that agreement are enforced by the FTC.

European regulators ramped up their criticisms of the framework following the first Edward Snowden leaks this summer, pointing out that Safe Harbor specifically provides for exemptions “to the extent necessary to meet national security, public interest or law-enforcement requirements.” European Parliament member Jan Philipp Albrecht, who authored an updated EU data protection regulation that passed out of committee last month, told U.S. officials last week that the agreement inappropriately allows U.S companies to “circumvent” democratically established law.

His draft regulation contains a so-called anti-FISA clause that would forbid U.S. companies from complying with government requests for personal data unless expressly approved by EU authorities. Since American companies can’t agree to rules that would require them to ignore lawful U.S. requests for information, the law could effectively undermine U.S.-EU data transfers.

Recent NSA revelations should not “distort” discussions about the framework, Brill has argued. Regardless of what mechanism is in place, U.S. as well as EU companies will have to comply with lawful domestic requests related to national security or law enforcement, said Jules Polonetsky, executive director of the Future of Privacy Forum, which is currently drafting a report on the Safe Harbor program.

“Europeans seem to be using [Safe Harbor] as a sacrificial lamb to express their frustration with NSA and law enforcement access to data,” he said. “There’s a lot of misunderstanding about Safe Harbor.”

If European attempts to suspend Safe Harbor are successful, U.S. companies may have to turn to alternative data transfer methods, such as “model contracts” drafted by EU commissioners or corporate privacy rules that require approval from data protection authorities in each relevant EU country. Both options are more “burdensome” and difficult to use than Safe Harbor, said Jeremy Mittman, an attorney with Proskauer Rose in Los Angeles who has experience drafting Safe Harbor certifications and EU model contracts.

None of those mechanisms is subject to FTC enforcement or annual renewal, he said. “One of the things to consider is, if you get rid of Safe Harbor, what are you really achieving?” Mittman said. “Companies are going to be transferring data and they’re going to find ways to do it.”

In addition to their critiques of Safe Harbor’s stringency, European regulators and others have attacked the agreement on the grounds that it is poorly enforced. EU officials released two reports critical of the program’s enforcement in 2002 and 2004, and the Australian consulting firm Galexia reported hundreds of Safe Harbor violations in a 2008 report that lambasted both the EU and the U.S. for not taking enforcement more seriously.

Indeed, the FTC did not bring its first enforcement under Safe Harbor rules until 2009, and its batch of seven enforcement actions that year targeted companies for falsely advertising their Safe Harbor certification, not for any failures to protect Europeans’ data. Since then, the agency has brought three Safe Harbor enforcement actions against Facebook, Google and MySpace as part of larger privacy-related investigations of the companies.

Brill said the FTC hasn’t received many Safe Harbor-related referrals or complaints from Europeans and has instead taken the initiative itself to enforce the framework. Mittman and several other U.S. attorneys versed in Safe Harbor certification said their clients had not received any Safe Harbor-related complaints following successful certification. An FTC spokesman declined to comment on the specific number of complaints the agency has received.

FTC Chairwoman Edith Ramirez recently jumped in to defend the agency’s enforcement efforts on Safe Harbor, telling the Trans Atlantic Consumer Dialogue forum in Brussels last week that the agency’s “track record in consumer privacy enforcement is unrivaled among data protection authorities around the world.” The agency has been “vigorously enforcing” a range of laws governing consumer information, she said.

Both Brill and Ramirez also hinted that there are more enforcement efforts on the way, without providing details.