FAST COMPANY

The new trans-Atlantic data agreement puts E.U. priorities first

U.S. inaction on privacy has let E.U. priorities take precedent with the new Trans-Atlantic Data Privacy Framework.

BY ROB PEGORARO

March 30, 2022

For the third time in seven years, Washington and Brussels have shaken hands on a deal to keep customer data flowing—and to keep a certain American social network afloat—across the Atlantic.

The new Trans-Atlantic Data Privacy Framework's provisions for E.U. individuals to seek redress against overreaching U.S. intelligence collection may or may not survive court scrutiny in Europe. But this much about the arrangement seems clear: Once again, U.S. inaction on privacy has let E.U. priorities take precedent. Americans still stand to gain privacy upgrades—for example, lower odds of having their data swept up unintentionally in an intelligence agency's search of overseas communications—but any handwritten thank-you cards will need to be sent with international postage.

The U.S. and the E.U. inked the deal, announced Friday by the White House and the European Commission, to solve a problem that's been festering for U.S. firms—Facebook foremost—since Edward Snowden revealed the National Security Agency's post-9/11 bulk collection of communications data.

Those disclosures of sweeping online surveillance programs led Austrian privacy activist Maximillian Schrems to file a complaint with regulators alleging that international "Safe Harbor" data-transfer policies left his Facebook data exposed to the NSA without adequate recourse. After multiple appeals, the Court of Justice of the European Union agreed, scuttling Safe Harbor in an October 2015 ruling.

The U.S. and the E.U. tried again with a 2016 arrangement called Privacy Shield—but Schrems sued and won again, with the CJEU ruling in July of 2020 that this newer deal still yielded insufficient protection for Europeans' data.

That "Schrems II" sequel suit has now yielded the framework announced Friday. A White House outline breaks down the major provisions:

- U.S. intelligence agencies may only collect signals intelligence when "legitimate national security objectives" require it, may not "disproportionately" hurt privacy and civil rights in the process, and must upgrade its oversight of these stronger standards.
- If E.U. individuals find their data has been collected, a new Data Protection Review Court comprised of people outside the U.S. government can hear their appeal and direct remedial action.
- Companies will remain under Privacy Shield rules, which require them to certify their compliance to the Department of Commerce and face enforcement action from the Federal Trade Commission if they fall short.

The immediate effect here should be to fill the regulatory void that led to Meta warning in a Feb. 3 SEC filing that without a replacement data-transfer agreement, it would have to yank Facebook and Instagram from Europe.

"It feels to me like privacy professionals have been holding their breath for a year and a half," says Caitlin Fennessy, vice president and chief knowledge officer at the International Association of Privacy Professionals, a privacy nonprofit.

Last October, the International Association of Privacy Professionals found that 10% of members responding to its survey said their firms had stopped data transfers, parked E.U. user data on European servers, or pulled services from the E.U. because of the Schrems II suit.

But the announced framework is not a full set of rules—and the E.U. court might still find the finished product doesn't offer enough safety for E.U. citizens against the curiosity of the U.S. intelligence community.

Schrems, who must now be Facebook's least favorite European user, said in a statement Friday that he or like-minded activists "will likely challenge" the framework in court; Monday, E.U. competition commissioner Margrethe Vestager told Reuters that she also saw yet another court test coming.

The framework's data-protection court for Europeans looks to be its biggest and trickiest change.

"The idea that a country would offer such a mechanism for people outside their country to seek redress is significant," says Amie Stepanovich, vice president of U.S. policy at the Future of Privacy Forum. "However, challenging U.S. government surveillance activity has proven difficult even by U.S. citizens even in our established courts."

Julian Sanchez, a senior fellow at the Cato Institute, wrote in an email that if this new court is sufficiently empowered to pass E.U. court scrutiny, it would invite a politically-awkward reaction along the lines of "Hey, wait a minute, E.U. citizens now have a more practically effective means of getting FISA [Foreign Intelligence Surveillance Act] grievances addressed than Americans do."

In the meantime, Americans should still gain some privacy thanks to this framework curbing NSA data collection in Europe—which often scoops up data about Americans. “As a practical matter, anything that reduces broad collection on Europeans is going to reduce the volume of ‘incidentally collected’ messages to and from Americans that winds up in an NSA database,” Sanchez wrote.

As under Privacy Shield, U.S. customers may also benefit from the FTC’s ability to punish companies that fall short of professed privacy commitments.

“When the Federal Trade Commission brings a privacy case against a U.S. company, they often use Privacy Shield commitments as a hook,” Fennessy says. For example, that regulator has used that hook in recent cases against CafePress, NTT Global Data Centers Americas Inc., and Flo Health.

Meanwhile, even as negotiators on opposite sides of the Atlantic have crafted three different privacy agreements in seven years, elected representatives in Washington have yet to pass any comprehensive privacy legislation in the same time.

Here and in such other cases as the privacy rules of the EU’s General Data Protection Regulation, this results in a policy outsourcing by the U.S. Greg Nojeim, senior counsel at the Center for Democracy & Technology and codirector of that nonprofit’s Security and Surveillance Project, says, “Many companies will simply apply the changes they adopted under pressure abroad to all of their users.”

That’s not necessarily bad, but it is weird, and privacy advocates still hope that developments overseas and states here passing their own privacy laws will coax Congress to act.

“I do think it’s coming,” says Stepanovich. “I don’t think that this is something that is going to be several years.”

That would be a welcome development. But this isn’t the first privacy-policy story I’ve written to feature such an optimistic quote about the future of privacy policy.