FAST LTA

?!

Factcheck

EU data in US hands

An analysis of the status of transatlantic data protection efforts

Since: April 2025

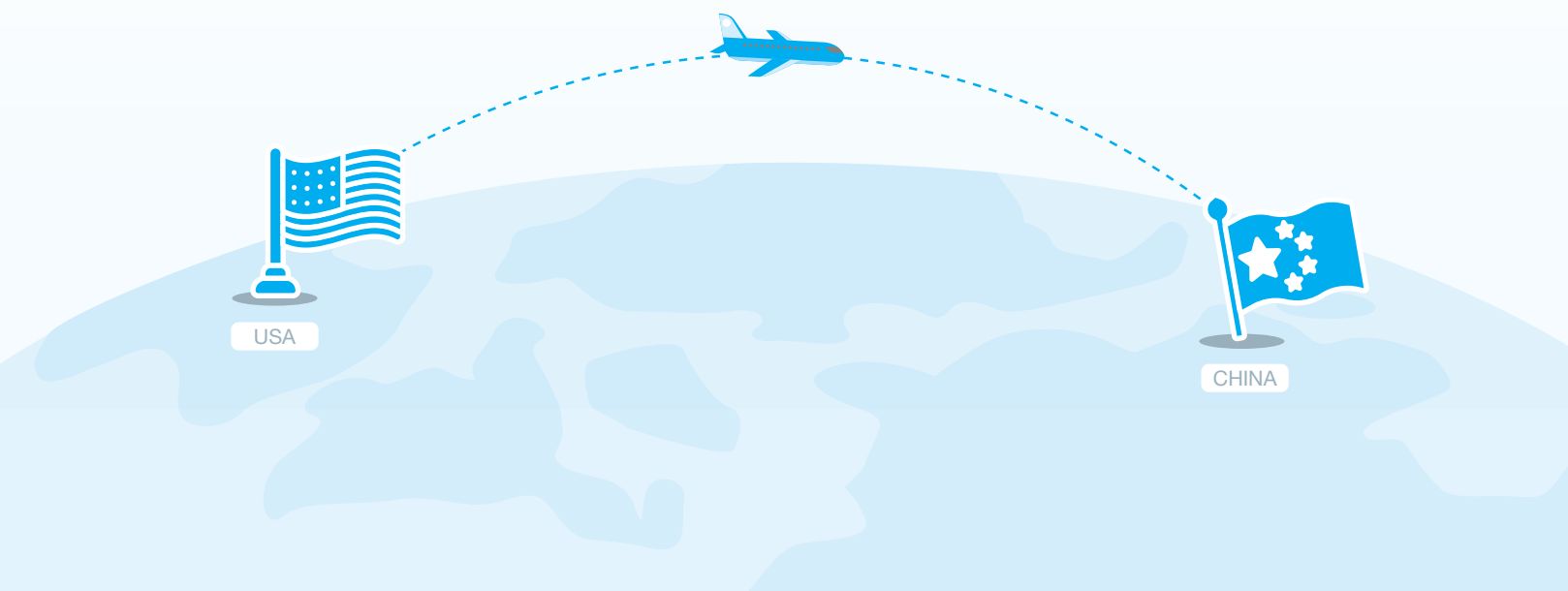
In order not to stand out, he had apologized to his supervisor in May 2013 on medical grounds. He had been diagnosed with epilepsy the year before, and necessary treatment provided the perfect excuse. But instead of going to the doctor, he packed his most important belongings and flew from Hawaii to Hong Kong - one way - there was no turning back.

He had spent months gathering evidence and his decision to go public had been carefully considered. He did not say a word to anyone, not to his family, not to his girlfriend, because that would have made them complicit. He left only a bill saying he was away on business.

> *„I had arranged everything so that my family could cut ties with me and judge me if things went badly. And that was fine with me; I was willing to accept that.“*

In Hong Kong, he spent three weeks in hiding in a hotel room, which he was only allowed to leave three times during that time. The fear of being detected by the CIA was too great. In his luggage were four laptops containing explosive documents that would transform him overnight into a symbolic figure. A true patriot, a defender of the Constitution, of the Fourth Amendment, which was supposed to protect people‘s basic personal rights from state interference - an enemy of the state.

It was June 6, 2013, when Edward Snowden changed the world. In his Hong Kong hotel room, the then 29-year-old Snowden handed over top-secret documents to journalists Glenn Greenwald and Laura Poitras. What followed was the largest disclosure of secret service activities in history. The consequences were immediate and far-reaching. As Snowden fled first to Hong Kong and later to Moscow, where he still lives in exile today, a process began in Europe that would fundamentally change the digital economy.



The beginning of the end of digital peace

The documents revealed shocking details: under the innocuous-sounding name “PRISM,” the NSA has been systematically accessing the data of Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL and Apple since 2007, giving it almost unlimited access to the private communications, photos, videos and files of millions of people worldwide.

European citizens, businesses and even governments were also affected. The “Upstream” program tapped directly into the undersea cables through which most international data traffic flows.

An Austrian student shakes up the system

Despite the revelations, the process to fundamentally change the digital economy was not a political one. The European Commission demanded only guarantees that the rights of European citizens would not be violated. Only later in the year, when further intelligence activities came to light regarding the Chancellor‘s (Merkel) interception of a smartphone that had nothing to do with PRISM, did much excitement arise.

A young Austrian law student had to step into the breach. Max Schrems was preparing his master‘s thesis. For this, he had made a request to Facebook for his personal data and received a 1,222-page report - including information that had long since been “deleted.”

After Snowden‘s revelations, it was clear that it could no longer just be about Facebook‘s shoddy handling of European data protection standards. Instead, Schrems asked himself the question: if U.S. companies like Facebook were required to share their data with the NSA, how could the Safe Harbour Agreement between the EU and the U.S. guarantee the protection of European data?

The fall of the digital wall

What began as an individual student‘s complaint grew into a legal earthquake. On Oct. 6, 2015, the European Court of Justice (ECJ) issued a ruling that shook the digital economy: Safe Harbor, the agreement that had regulated data transfers between the EU and the US for 15 years, was declared invalid.”

US surveillance programs go beyond what is strictly necessary and proportionate,” the ECJ said. More than 4,000 companies that relied on Safe Harbour suddenly had no legal basis for their transatlantic data transfers.

This would not last long, and in the months following the ruling, the meeting rooms of the European Commission and the U.S. Department of Commerce buzzed with activity. The successor agreement was officially adopted on July 12, 2016.

The Obama administration had made commitments: a new ombudsperson would provide EU citizens with remedies against U.S. surveillance. The NSA promised to limit its powers. But Max Schrems remained skeptical: “They essentially just renamed the old system.”

Trump I (2017–2021), Schrems II (2020)

The Privacy Act, a U.S. federal law regulating the handling of personal data by U.S. federal authorities, has existed since 1974. Although it has always been limited to U.S. citizens and permanent residents, some authorities had administratively extended protection to non-U.S. citizens.

With Executive Order 13768, Trump clarified the situation and explicitly excluded data protection for non-U.S. citizens. Although the Privacy Act was not part of the Privacy Shield, Trump‘s action showed the importance he places on data protection for non-U.S. citizens.

Even more serious than the presidential decree was the fact that the ombudsperson promised in the Privacy Act was not even appointed, missing a crucial part of the agreement for years.

Law student Max Schrems, by now a sought-after data protection expert, founded the crowdfunded organization “NYOB - European Center for Digital Rights” in the first year of Trump‘s presidency. The organization, whose acronym stands for “None of Your Business,” campaigns for the protection of privacy and digital rights in Europe.

Against the backdrop of Trump‘s actions, Facebook again found itself in Schrems‘ crosshairs, filing a new lawsuit, this time against Facebook‘s standard contractual clauses. The case became known as “Schrems II” and led to the following bombshell on July 16, 2020: the ECJ also declared the Privacy Shield invalid “because standard data protection clauses cannot bind third-country authorities because of their contractual nature.” The ECJ also summarized the consequences in its ruling: “The controller is obliged to suspend or terminate the transfer if the recipient is unable to comply with the standard data protection clauses.”

The impact was immense. Companies like Facebook threatened to pull out of Europe. Amazon and Microsoft began setting up European data centers. But the fundamental problem remained: as long

as U.S. laws such as FISA 702 and the Clarifying Lawful Overseas Use of Data (CLOUD) Act gave U.S. authorities far-reaching access to data, any agreement had to be based on feet of clay. After all, the CLOUD Act even gives U.S. authorities access to data stored in European data centers operated by U.S. providers - a fact that makes the efforts of U.S. tech giants to set up European data centers largely absurd.

The Data Privacy Framework - New hope?

When Joe Biden and Ursula von der Leyen announced the new Data Privacy Framework (DPF) in March 2022, the economy breathed a sigh of relief. After two years of legal uncertainty, a solution seemed finally in sight. However, the controversial Section 702 of the Foreign Intelligence Surveillance Act (FISA 702), which gives US authorities far-reaching surveillance powers, remained untouched. Instead, new surveillance mechanisms were introduced. In particular, the new Privacy and Civil Liberties Oversight Board (PCLOB) is now tasked with ensuring that privacy is adequately protected. Biden also signed Executive Order 14086, which was intended to address European Court of Justice concerns and limit U.S. intelligence agencies‘ access to European data.

Indeed, the order introduced new restrictions:

- Intelligence surveillance may not be used to suppress or discriminate against criticism.
- Economic espionage is expressly prohibited.
- Mass surveillance is limited to six specific targets.

However, the order contains loopholes. The president can, for example, add new surveillance targets at any time if “new national security requirements” make this necessary. Worse still, what is supposed to be sold as a limitation of the intelligence services actually expands their capabilities through additional surveillance objectives. The intelligence services are now, for instance, the guardians of the Paris Climate Agreement and can collect data to defend against threats from “climate and ecological changes.” Eavesdropping on the chancellor’s smartphone may have been a scandal in 2013, but would now be justified by the goal of “understanding and evaluating foreign political organizations.”

It was therefore all the more astonishing that the European Commission declared the level of data protection in the U.S. “adequate” under the new Data Privacy Framework on July 10, 2023.

“The supposedly ‘new’ transatlantic data protection framework is largely a copy of the failed Privacy Shield,” said Schrems, justifying his intention to file another lawsuit immediately after the DPF was approved by the EU Commission. However, it is possible that the agreement may not even reach the

court in Luxembourg.

Trump II

Since January 20, 2025, a different wind has been blowing from Washington—an icy wind. Travis LeBlanc felt it during the first week under Trump II. A bachelor's degree from Princeton, a master's from Harvard, a doctorate from Yale—as an expert in cybersecurity, data protection, and emerging technologies, he seems tailor-made for a position on the PCLOB. But in Trump's eyes, he has one flaw: he is a Democrat. And so, shortly after the inauguration, he received a dismissal letter, along with the two other Democrats on the board.

All that remains is Beth Williams, a Trump loyalist who played a key role during his first term in selecting and confirming 230 federal judges. According to her own statements, she is focusing on preparing for work in the future. What exactly that entails and when that future will arrive is uncertain. What is certain, however, is that due to the dismissals, the PCLOB is currently unable to operate, as at least three members are needed for a quorum. In its adequacy decision, the European Commission mentioned the PCLOB 31 times as a safeguard for data protection. After the dismissals, the question remains how "adequate" the level of data protection in the transatlantic relationship still is.

The wave of dismissals at U.S. authorities triggered by Trump—which mainly affects Democrats and Trump opponents—may well be just the beginning. In October 2023, during a speech at the annual conference of the Republican Jewish Coalition, he announced that he would revoke all executive orders issued by Joe Biden. This would also affect Executive Order 14086, the second central component of the DPF.

Conclusion

When Edward Snowden published the first documents about PRISM in 2013, no one could have imagined the avalanche he would set in motion. Today, twelve years later, we are once again at a turning point.

The DPF not only seems to be built on sand; its foundations also show significant cracks. A fundamental reorganization is hardly conceivable under the current U.S. administration. Instead, Europe and the U.S. appear to be drifting further apart, as evidenced by the speeches at the Munich Security Conference. “We must fear that our common value base is no longer so common,” MSC Chairman Christoph Heusgen summarized the situation.

This is also reflected in a survey by the European Council on Foreign Relations: In Germany, France, Italy, and Spain, less than 20 percent of respondents still view the U.S. as an ally with shared values.

Europe faces the challenge of redefining its digital sovereignty. German and European companies must prepare for a worst-case scenario. The situation is even more critical than with the previous agreements Safe Harbour and Privacy Shield.

FAST LTA

FAST LTA
Rüdesheimer Str. 11
80686 München
info@fast-lta.de
www.fast-lta.de

Design,
Entwicklung
und Support
in **Deutschland**