

From: [REDACTED]
Sent: 22 October 2018 09:12

To: [REDACTED]

Subject: News update - NewEurope: EU-US relations Post GDPR



Future of privacy forum and Israel Tech Policy Institute

636 words
22 October 2018

New Europe

NEWEU

English

© 2018. New Europe.

Political and economic developments over the past few years have strained the transatlantic alliance. The Trump Administration and [EU](#) leaders continue to clash over issues that were once common core values, including the [NATO](#) alliance, immigration policy, cross Atlantic trade and climate change.

Only a year ago, it seemed as though the cohesion of the digital economy would unravel as Europe introduced the General Data Protection Regulation (GDPR) while the United States continued to cling to sector specific privacy regulation.

In addition, the demise of the EU-US Safe Harbor and legal pressure against the new Privacy Shield seemed to further destabilise the brittle global framework for data flows. But what a difference a year makes.

As 2018 draws to a close, a radical shift has occurred in the US stance towards privacy policy. Leading US companies have accepted and implemented the key requirements of GDPR on a global level. California, home of the tech industry and by far the largest US state, passed a strict privacy law adopting some key principles of GDPR, including a right to access and deletion. In some cases, the new law, the California Consumer Privacy Act, goes even further than European law in restricting corporate data practices.

These days, the [US government](#), leading companies and trade groups, including the powerful [US Chamber of Commerce](#), have embraced the call for federal privacy legislation. The Senate Commerce Committee held hearings about prospective federal privacy law, including testimony from Europe's lead regulator, [Andrea Jelinek](#), who Chairs the newly formed European Data Protection Board. Senator Richard Blumenthal even suggested that the US should proceed to adopt a local version of GDPR.

To be sure, it remains unlikely that the US will go that far. And the drive for federal legislation is partially motivated by companies seeking to soften California's new law with more flexible legislation. But the turnaround is dramatic, as only a year ago the majority of US companies were railing about GDPR and arguing that the US model of sector specific legislation, which regulates sensitive data and provides the FTC with overarching authority, was adequate.

Now, global technology companies have taken the lead on GDPR compliance. For example, the Data Transfer Project, a group led by [Twitter](#), [Facebook](#), [Google](#) and [Microsoft](#) launched the first major standard to advance data portability.

Similarly, academics and start up companies in the US and in Israel are playing an important role in developing

techniques that will live up to the GDPR's high standard of anonymous, privacy protective data processing. These include differential privacy, which permits querying databases without sacrificing the privacy of individual data subjects, and homomorphic encryption, which features computations performed on encrypted data.

Perhaps the most important issue for the future is AI and machine learning. How do we ensure that important decisions about health and finance, education and transportation, are fair and equitable where algorithmic decision making is opaque? How can engineers verify that autonomous vehicles are not only safe but also ethical?

Scholars all around the world are grappling with frameworks to ensure algorithmic due process and trust in AI. This week, at the 2018 International Conference of Data Protection and Privacy Commissioners in Brussels, the Public Voice, which brings together civil society organizations from the US, Europe and the rest of the world, will release a joint set of ethical principles for AI.

While the US legislative effort may yet falter, and is unlikely to match the comprehensiveness of GDPR, 2018 will be remembered as a year of convergence of privacy policy. At a time when many issues are pushing longtime allies apart, the common acceptance of the centrality of privacy and data protection to our digital future is a rare and important bond that brings global parties together.

SPRL Brussels News Agency



European Data Protection Board

Tel: 0032 2 2831907 – +32 474 38 39 88

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

 edpb.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPB therefore cannot guarantee the security of correspondence by email.