Skadden

Major Developments Continue To Reshape the Global Privacy Landscape

Contributing Partners

Ken D. Kumayama / Palo Alto

Stuart D. Levi / New York

Counsel

Eve-Christie Vermynck / London

This article is from Skadden's ***2021 Insights***.

One Manhattan West
New York, NY 10001
212.735.3000

The global privacy landscape has shifted dramatically over the past few years, with 2020 marking a watershed in many respects. The year commenced with the California Privacy Protection Act going into effect and ended with voters passing the California Privacy Rights Act, which will supplement the earlier law and bring the state another step closer to the requirements imposed by the European General Data Protection Regulation (GDPR). Elsewhere, Brazil's Lei Geral de Proteção de Dados Pessoais, modeled after the GDPR, went into effect last year as well, marking another example of robust privacy requirements that global companies need to take into account and that will add to a company's privacy compliance costs. But perhaps the greatest privacy reverberations arose once again in Europe, as a new ruling from the Court of Justice of the European Union (CJEU) created global shockwaves regarding the flow of personal data out of the European Economic Area (EEA).

We examine below some of the key privacy trends from 2020 and the outlook for 2021.

What Happens Next for Data Transfers Outside the EEA?

The CJEU decision in *Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems* (*Schrems II*) struck down the EU-U.S. Privacy Shield as a valid data transfer mechanism from the EEA to the U.S. after only four years in existence. The EU-U.S. Privacy Shield had been crafted to replace the long-standing "Safe Harbor" agreement the CJEU invalidated in *Schrems I* due to the limitations on the protection of personal data under U.S. law and the disproportionate access and use of EEA personal data by U.S. authorities, with no effective redress mechanism for data subjects. In the July 2020 ruling, the CJEU also imposed enhanced due diligence obligations on parties seeking to rely on the long-standing European Commission Standard Contractual Clauses (SCCs), one of the mechanisms under Article 46 of the GDPR by which personal data can be transferred lawfully outside the European Economic Area, creating uncertainty for those utilizing this common data transfer mechanism.

In October 2020, the CJEU handed down another key decision that will shape the narrative relating to the regulation of data transfers outside the EEA. In *La Quadrature du Net and Others v. Commission*, the CJEU found certain EU member states' national security laws to be incompatible with EEA law. Touching upon the same concern at the heart of the *Schrems II* judgment, in *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* the CJEU ruled as unlawful member state legislation that allowed electronic communications service providers to indiscriminately store personal data for use or collection by intelligence services.

With these developments in mind, what data transfer developments can we expect in 2021?

- **The Normalization of Transfer Impact Assessments.** In November 2020, the European Data Protection Board (EDPB) released two recommendations addressing the due diligence obligations and supplementary measures imposed by the CJEU in the *Schrems II* decision for organizations transferring data outside the EEA. In line with the recommendations, organizations now must perform case-by-case transfer impact assessments (TIAs) that determine whether the data-importing country provides "essentially equivalent" protection of personal data as that guaranteed under EU law. Where an essentially equivalent level of protection cannot be guaranteed, supplementary technical, contractual and/or organizational measures must be implemented. This creates a new workstream for organizations wherever personal data is transferred outside the EEA on the terms of the SCCs, and TIA templates and policies are likely to become commonplace. What remains to be seen is the form these will ultimately take and how long until any sort of standard approach is developed.
- **Increased Localization Options.** We expect cloud-based service providers that historically transferred EEA personal data to the U.S., or even accessed such data remotely from the U.S. to provide services, to increasingly offer regionalized data hosting and support services within the EEA. For vendors, this may prove a preferable solution to negotiating bespoke supplementary measures with a large number of customers. For customers, the localization of personal data within the EEA eliminates the risk of a court or supervisory authority finding any relevant TIA or supplementary measures inadequate.
- **Implementing New SCCs.** On November 12, 2020, the European Commission (EC) released draft SCCs for transfers of personal data to third countries outside the EEA, which were updated to account for the GDPR and *Schrems II* and to address the need for SCCs governing processor-to-processor and processor-to-controller relationships. Once adopted by the EC, which is expected in early 2021, the updated SCCs will replace the existing ones with a one-year grace period for implementation by organizations. Keeping up-to-date data maps of both intragroup and third-party data flows will facilitate this transition to the new sets of SCCs.
- **Brexit.** Following the Trade and Cooperation Agreement reached between the EU and U.K. on December 24, 2020, data transfers from the EEA to the U.K. will not be considered transfers to a third country for a period of six months and can therefore continue as before, until either (1) the end of the six-month period or (2) the EC reaches a decision on the U.K.'s adequacy. Given the political nature of the adequacy decision, it is difficult to predict with accuracy when the EC will make its decision. With respect to data transfers from the U.K. to the EEA, the U.K. has provisionally recognized the EU as adequate, meaning that data transfers from the U.K. to the EEA can continue as before.

Cookies and Profiling: The Next Enforcement Priorities for European Supervisory Authorities in 2021?

In recent years, various European supervisory authorities have issued guidance on the consent required from users to place cookies or similar technology on user devices, though there was scant enforcement action in this area. That changed in 2020 with a series of cookie-related actions by the French supervisory authority, the Commission Nationale de l'Informatique et des Libertés. Such enforcement activity extends beyond just the French supervisory authority and appears likely to continue in 2021 and should be considered along with the upcoming Digital Services Act, which was published by the EC in December 2020. Among other changes to expand the regulation of large online platforms, the Digital Services Act is expected to increase transparency and user control with respect to profiling. Organizations should take this opportunity to review their practices around cookies and profiling and align them with regulatory standards.

Increased Cost and Complexity for Businesses Under California Data Privacy Laws

In the November 2020 U.S. elections, California voters opted to supplement the privacy rights afforded to them under the 2018 California Consumer Privacy Act (CCPA) with the passage of the California Privacy Rights Act (CPRA). Importantly, the application of both laws is based on whether the data subject is a California resident, not whether an organization has offices in the state. That said, if other states follow California's lead with their own individual privacy laws, demand for a U.S. federal privacy law — which until recently seemed like a remote idea — could gain traction.

The CPRA adds new rights and strengthens certain existing protections for California residents, in many ways affording rights more similar to those of EEA residents under the GDPR, including:

- greater control over the sharing of personal information;
- stricter data minimization requirements;
- enhanced protections for sensitive personal information;
- the right to correct inaccuracies in personal information; and
- greater transparency regarding, and the right to opt out of, the use of automated decision-making technology.

While these changes do not come into force until January 1, 2023, businesses need to take them into account as part of their long-term data monetization and usage strategies.

The CPRA also included several changes that will take place sooner, including increasing resources to enforce California's privacy laws and creating a new California Privacy Protection Agency (CalPPA) with primary responsibility for enforcing the CCPA and CPRA going forward. CalPPA will have authority to coordinate with data protection authorities in California and other jurisdictions, which given the many similarities

between rights under the CPRA and GDPR may include regulators in the EU. The California Office of the Attorney General will transfer its regulatory authority to CalPPA upon the earlier of (1) July 1, 2021, or (2) six months after CalPPA provides notice to the attorney general that it is prepared to exercise CCPA regulatory authority. This development answers the question that many had been wondering as to whether the attorney general had the resources to enforce the new privacy laws.

Organizations should expect continuing and, depending on their use of data, potentially increased costs to comply with the CCPA, especially as the California attorney general rolls out new or modified CCPA regulations. In 2020 alone, there were four rounds of adopted or proposed regulations, many dealing with the manner in which companies disclose how they sell consumer data. Longer-term compliance also will remain challenging, as the regulations for the CPRA have yet to be written and the law may be subject to further change before being finalized. Organizations must maintain their current compliance programs while remaining nimble enough to address future requirements.