withersworldwide

Privacy, the pandemic, and the immediate need for legislative and regulatory support

21 OCTOBER 2020

M. Ridgway Barker
PARTNER | US

CATEGORY:
ARTICLE

CLIENT TYPES:
COVID-19

CORONAVIRUS

M. Ridgway Barker co-authored this article with Joseph Bambara CIPP/US.

The focus of almost everything in 2020 has been the COVID-19 pandemic. Predictably, privacy has been impacted by the pandemic. Governing agencies have been required to consider privacy in adjusting practices to account for who has symptoms, who has traveled where, who has come into contact with whom, and what community members have tested positive or been exposed. See our article (https://www.withersworldwide.com/en-gb/insight/identity-verification-and-privacy-in-the-time-of-pandemic). As a result, governments and we: the citizens have had to deal with inevitable trade-offs between the exclusive focus on privacy versus exclusive focus on public health and safety. While privacy is not a guaranteed right in any jurisdiction, it is important to acknowledge that no democratic country has taken the position suggesting that individual privacy is irrelevant even during a pandemic emergency.

The pandemic was not the only disruption to the privacy system in 2020. On July 16, the Court of Justice of the European Union (" CJEU") invalidated the Privacy Shield ("PS") framework agreed between the European Commission and the U.S. Department of Commerce which facilitated data flows to the United States. The CJEU upheld the validity of using standard contractual clauses ("SCC") to transfer personal data to countries not yet deemed "adequate" by the EU, such as the United States. The CJEU then imposed considerable new obligations on organizations looking to transfer data and for data protection authorities to consider when approving such transfers.

These new obligations stem from relentless campaigns by privacy advocate Max Schrems and associates against Facebook ("FB") among others for privacy violations. Schrems is the founder of NOYB ('none of your business") see, (https://noyb.eu/en). See, also, the European Center for Digital Rights, (https://edri.org/). Back in 2011, Schrems while studying law at Santa Clara University in California learned how to access his FB records. He received a disk containing over 1,200 pages of data and he was overwhelmed by his privacy violated. This began a series of complaints filed by Schrems (aka Schrems I and II) about violations of European privacy laws and the alleged transfer of personal data to the US National Security Agency (NSA) as part of the NSA's PRISM program.

With respect to invalidating the PS framework, the Schrems complaints led the CJEU to minimally review but nonetheless decide U.S. surveillance safeguards and remedies to be inadequate or as the CJEU put it less than "essentially equivalent" to those of the EU. The decision will affect trillions of dollars of trans-Atlantic trade. For many companies, the issues of national security data access that appear to have concerned the CJEU in Schrems II are unlikely to arise because the data they handle is of no interest to the U.S. intelligence community. In any event, companies are reviewing /amending their processing to demonstrate that, under the Schrems II decision, see, *Facebook Ireland Ltd. v. Maximillian Schrems*, they can transfer personal data to the United States and other non "adequate" countries without such data being accessible to national security surveillance by the data importing country. Data exporters relying on the SCCs will need to be able to demonstrate that they have carefully assessed the risks associated with the transfer of personal data via the SCCs. Such a "transfer impact assessment" should provide solid legal arguments for the continued use of the SCCs. Without it, companies run the risk of having their data transfers challenged by the supervisory authorities.

The United States in response to privacy advocates, provided the 2018 Clarifying Lawful Overseas Use of Data Act (" CLOUD") which amends the Stored Communications Act (SCA) of 1986. Principally, it provides that U.S. communications service providers (" CSD") must provide stored data for a customer or subscriber on any server they own and operate when requested by warrant. That said, it provides protective mechanisms for the companies or the courts to reject or challenge these if they believe the request violates the privacy rights of the foreign country the data is stored in. CLOUD became effective in July 2020. The CLOUD Act requires foreign governments who want to engage to demonstrate their respect for the rule of law and for international human rights, privacy, free speech rights, data minimization, the principles of non-discrimination, accountability, transparency, independent oversight, and numerous other detailed safeguards. Courts must consider the nature of the legal conflict at stake, the materiality of the alleged violation of the foreign law, the respective interests of the two countries in the matter at hand, the contacts of the service provider and the individual in question with the United States, and the importance of the individual's information to the

criminal or national security interest at issue. The nature of this analysis required by the CLOUD Act is well reasoned. It serves as a model of safeguards, checks and balances, independent oversight, and international comity for government access to electronic communications.

In any event, privacy developments in the United States have not been all about government access to information. In this past year and a half, U.S. regulators and litigators have aggressively moved forward on alleged violations of privacy and data security requirements. This trend began in July of 2019 when the U.S. Federal Trade Commission obtained a $5 billion settlement following an investigation of the Cambridge Analytica affair. The FTC and state attorneys general have collected hundreds of millions of dollars in financial recoveries concerning data breaches as well as alleged violations of the U.S. Children's Online Privacy Protection Act.

Even the U.S. Securities and Exchange Commission (" SEC") is focused on digital practices and risks. The SEC is now actively enforcing the accuracy and reliability of privacy and cybersecurity disclosures by public companies. Companies could face regulatory action if they materially understate their digital risks or avoid discussing significant incidents they have already experienced or if they publicly overstate their data security or privacy practices.

As a result, many companies especially tech and affiliate marketing companies are expanding their discussion of how U.S. and international privacy laws are affecting or could affect their global regulatory risk profile or the economic viability of their current and future business models.

But perhaps the most important U.S. privacy development is the new California Consumer Privacy Act (" CCPA") which took effect July 1, 2020. See, again our article on the CCPA, (https://www.withersworldwide.com/en-gb/insight/identity-verification-and-privacy-in-the-time-of-pandemic) which requires privacy disclosures, grants privacy rights and imposes privacy restrictions comparable to the GDPR. The CCPA also suggests the prospect of statutory damages to incentivize lawyers to file litigation over data breaches affecting the personal information of California residents. Here again, it is incumbent that companies implement and maintain "reasonable security." California did not stop there. An even more restrictive California Privacy Rights Act ("CPRA") will be on the ballot for the November election. We will discuss this Act in a forthcoming article. That said, other states have begun to follow in California's footsteps in creating similar consumer privacy laws. Enterprises would be wise to adopt "best of breed" compliance and digital identity verification solutions that offer data security, transparency, and retention policies that comply with CCPA and any new legislation. With expanded rights come expanded enterprise responsibilities, and enterprises must retain trust to protect both their business and their consumers. The combination of well-designed legislation and technology can solve most any new challenge to our privacy and prosperity.

Our Withers attorneys can assist and educate clients from a legal and technical standpoint to incorporate these emerging privacy, security and technology trends safely and efficiently. Please contact your Withers attorney or the author of this piece with any questions.

To read more about how we can help please click here.
"":https://www.withersworldwide.com/innovation-during-the-coronavirus-covid-19-crisis

Authors

M. Ridgway Barker

PARTNER | GREENWICH

Corporate

+1 203 302 4084

mr.barker@withersworldwide.com