Cybersecurity & Data Privacy Updates

FG Law Blog

August 10, 2020

Donna Urban & Krishna Jani

There is a lot going on in the world right now—and the world of data privacy is no exception.

Here is a snapshot of what's on our radar:

1. Senators Jeff Merkley and Bernie Sanders introduced the National Biometric Information Privacy Act of 2020 on Tuesday, August 4, 2020.

This legislation would, among other things, prohibit private companies from collecting biometric data—including eye scans, voiceprints, faceprints, and fingerprints—without consumers' and employees' consent, or profiting from this data. This introduction comes amid growing concerns over the prevalence of biometric data collection among private companies, including the use of facial recognition technology.

This legislation limits the ability of companies to collect, buy, sell, lease, trade, or retain individuals' biometric information without specific written consent, and requires private companies to disclose to any inquiring individual the information the company has collected about that individual. Importantly, this bill would allow individuals *and* State Attorneys General to bring lawsuits against companies that fail to comply.

2. Several United States Senators have urged Congress to include the privacy protections contained in the Public Health Emergency Act into any new stimulus package.

On July 28, 2020, several U.S. senators drafted a letter addressed to senate leaders urging them to include the privacy protections contained in the Public Health Emergency Privacy Act in any forthcoming stimulus package.

The senators emphasized the need for commonsense privacy protections for COVID data because "public trust in COVID screening tools will be essential to ensuring meaningful participation in such efforts." Research shows that many Americans are hesitant to adopt COVID screening and tracing apps due to privacy concerns; therefore, the lack of health privacy protections could significantly undermine efforts to contain this virus and safely reopen—"particularly with many screening tools requiring a critical mass in order to provide meaningful benefits."

As the drafters point out, "health data is among the most sensitive data imaginable and even before this health emergency, there has been increasing bipartisan concern with gaps in our nation's privacy laws." The drafters believe these common-sense protections are critical in quelling the spread of COVID-19 while at the same time protecting sensitive health and geolocation information.

We will continue to track this legislation and provide updates as they become available.

***3. Schrems II* invalidated the EU-US Privacy Shield.**

On July 16, 2020, the Court of Justice of the European Union issued a decision in *Data Protection Commission v. Facebook Ireland, Schrems.* The decision, known as *Schrems II*, invalidated the European Commission's adequacy decision for the European Union-United States (EU-US) Privacy Shield framework, which is critical for more than 5,000 United States based companies that conduct trans-Atlantic trade in compliance with EU data protection rules.

The Court found the European Commission's adequacy determination for the Privacy Shield invalid for two primary reasons: (i) the US surveillance programs, which the commission addressed in its previously-issued Privacy Shield decision, are not limited to what is strictly necessary and proportional as required by EU law; and (ii) with regard to US surveillance, EU data subjects lack actionable judicial redress and, therefore, do not have a right to an effective remedy in the US, as required by the EU Charter.

The *Schrems II* decision requires both data importers and data exporters to be reasonably certain that they can comply with their obligations in the Standard Contractual Clauses. Where they cannot comply, importers and exporters should likely stop transferring data, forcing some companies into data localization. *Schrems II* addresses a long-running series of issues regarding the appropriate role of surveillance in our society and its inevitable clash with privacy.

This decision also influences data flows across nations. Some data privacy professionals believe that we are moving away from global data flows and moving towards more fragmented data flows. This shift could have a particularly significant impact on e-commerce. For more, see the Court of Justice of the European Union's Press Release on this decision.

The attorneys at Flaster Greenberg are following developments related to the COVID-19 Pandemic and formed a response team and to work with businesses to keep them up-to-date on developments that impact their business. If you have any questions on the information contained in this blog post, please feel free to reach out to Donna Urban, Krishna Jani, or any member of Flaster Greenberg's Telecommunications or Privacy & Data Security Groups.

COVID-19 RESOURCE PAGE

To serve as a central repository of information and contributions from Flaster Greenberg attorneys on legal developments during the COVID-19 crisis, we have launched a ***COVID-19 Resource page*** *on our website. Feel free to check back frequently for Flaster Greenberg's ongoing analyses of important legal updates that may affect you or your business.*