What's on the Horizon? 2022 State, Federal and International Data Privacy Action

The momentum for state legislation concerning consumer data privacy is at an all-time high. Data privacy regulation continues to evolve dramatically to keep up with developments in technology and the surge of online activity. Since the California Consumer Privacy Act (CCPA) was enacted in 2018, an increasing number of state legislatures have followed suit by proposing similar legislation aimed at protecting consumers in their states.

At least 38 states introduced more than 160 consumer privacy-related bills in 2021, compared to 30 states in 2020. A more comprehensive approach to privacy regulation was a common trend and was introduced in at least 25 states. Heading into 2022, there are now three states with comprehensive consumer data privacy legislation. Virginia and Colorado followed California's lead by enacting Virginia's Consumer Data Privacy Act (VCDPA) on March 2, 2021, and the Colorado Privacy Act (CPA) on July 8, 2021, respectively. The CCPA, VCDPA, and CPA share similar provisions that expand consumer rights to access, correct, delete and obtain a copy of personal data provided to or collected by a company. They also provide the option to opt out of the processing of personal data for purposes of targeted advertising, sale or profiling of the personal data. Each state varies in certain provisions such as exemptions, opt out rights and other aspects. Virginia's and Colorado's new data privacy laws reflect the growing trend among states to enhance consumer privacy protections.

2022 will likely see continued upward trend in data privacy regulation enacted here in the U.S. and abroad. The COVID-19 pandemic continues to increase business and non-business online activity forcing many legislatures to consider the need for stricter and more comprehensive data privacy regulations.

At least 15 state legislatures are poised to consider comprehensive consumer privacy legislation in 2022 with lawmakers in Arizona, Connecticut, Florida, Minnesota, Mississippi and Washington confirming they will be introducing bills. Additionally, Maryland has pre-filed a privacy bill and eight other states have bills that will carry over from the 2021 session.

At the federal level, efforts to pass privacy legislation have been ongoing for years. Dozens of proposals for a comprehensive federal law that governs data privacy in the U.S. have worked their way through the halls of Congress to no avail. Numerous legislators from across the aisles have worked together on legislation addressing all facets of privacy, including individual rights and business obligations, special protections for sensitive information, access to records by law enforcement and emerging technologies such as facial recognition and artificial intelligence. Congress, industry, civil society and the White House have all taken steps toward the creation of a U.S. federal privacy law. It is still very much in question what this law will look like or if and when it will even happen, however, it is looking more likely that a federal law could be enacted.

Although the U.S. has yet to implement national legislation, there has been movement at the federal level to recognize the importance of privacy and data protection. Since 2017, the U.S. General Services Administration (GSA) has implemented data privacy related training in its annual requirements for federal contractors. The training covers GSA's policies on protecting Personally Identifiable Information (PII). The GSA requires all employees and contractors to complete privacy and security awareness training upon employment and each year thereafter. The Federal Trade Commission (FTC) has exercised its broad enforcement power and authority to regulate on behalf of consumer protections by pursuing privacy and data security cases in myriad areas, including against social media companies, mobile app developers, data brokers, ad tech industry participants, retailers and other companies. Moving forward, the FTC is focusing its efforts on improving the agency's effectiveness at

protecting Americans' privacy. The FTC has even put forth proposals to increase its budget, resources and personnel in an effort to perform as the country's de-facto privacy regulator.

Outside the U.S., for example, there has been an increase in ambiguity surrounding international data transfers by entities subject to the GDPR. On Nov. 19, 2021, the European Data Protection Board (EDPB) published draft guidelines on the interplay between the GDPR's territorial scope and its international transfer provisions. The guidelines aim to assist organizations subject to the GDPR in identifying whether a data processing activity constitutes an international data transfer under the GDPR, as the GDPR does not define the term. The new guidance includes a three-part definition of what constitutes an international data transfer as the EDPB interprets it under the law. The facets of the definition include identifying whether the processing activity falls under the GDPR, an exporter-to-importer transmission and the geographical location of the importer. The guidelines provide some clarity on international data transfers, however, the EDPB has raised questions by requiring transfer mechanisms for onward transfers of personal data that originate in the European Economic Area (EEA) but take place outside the EEA, for example by a U.S. company to its U.S. processors. Even where there is no "transfer" under the draft guidelines, the EDPB effectively requires an assessment of the risk of government access to European personal data, including any need to implement additional measures. The guidelines are currently under a longer-than-usual consultation period until Jan. 31, 2022.

The Austrian Data Protection Authority (DPA) recently issued a decision that the use of Google Analytics violates the GDPR. The DPA rules that in providing the Google Analytics service, the company collects and transfers personal data to the U.S. while failing to protect it from U.S. government surveillance. The DPA determined that configuration abilities for customers, such as truncating IP addresses, are insufficient to prevent re-identification, potentially by Google or the U.S. government. The decision also determined that supplementary measures implemented by Google, including government access transparency reports and encryption of data, were insufficient. The DPA's decision could have far reaching implications if other EU regulators take the same view, considering the similar issues would then arise with many other services provided by entities outside of the EU, especially those in the U.S.

The need for data privacy continues to be recognized across the globe, and the progression toward greater privacy and data-related laws is only gaining speed. For more information or guidance concerning any of the topics above, please contact Fred Price or any one of our attorneys in the Cybersecurity and Data Privacy practice.

Thank you to Associate Trainee Gianelle Duby for her help drafting this information memorandum.

BOND SCHOENECK & KING ATTORNEYS