Quarterly Update: Cybersecurity and Data Privacy Developments

The cybersecurity and data privacy legal landscape continues its rapid evolution. Below is an outline of some of the most significant developments in the last quarter.

Federal Legislation:

In June, a bipartisan federal privacy bill, the American Data Privacy and Protection Act (ADDPA), was released for consideration. The law follows the general framework of various state privacy laws, as well as the European Union's General Data Protection Regulation (GDPR). Notably, unlike state privacy laws, ADDPA is intended to apply to most entities, including nonprofits and common carriers. Large data holders that meet certain thresholds, as well as service providers who use data on behalf of other covered entities, would face different or additional requirements.

Like other consumer privacy laws, the law grants numerous individual privacy rights, including rights to access, delete and correct data, as well as the right to data portability. ADDPA also broadly defines sensitive data and will require additional protections for such data. In addition, the law calls for transparency in processing, minimum data security requirements and a prohibition from using covered data in a way that discriminates on the basis of protected characteristics.

The ADDPA would be enforceable by the Federal Trade Commission (FTC) as well as by state attorneys general in civil actions. The bill does currently include a private right of action, but such right would not be effective for at least two years after the bill's passage. The most highly debated issue involves ADDPA's preemption of all state laws by default, except for state data breach statutes and other specific laws like Illinois' Biometric Information Privacy Act.

The bill is advancing to the House of Representatives after the House Committee on Energy and Commerce marked the document on July 20 and voted 53-2 to advance the bill to the full House for consideration. The committee made some significant changes to the initial bill, including changing the private right of action's effective date from four years to two years post-adoption, expanding the categories of sensitive information, enforcement tweaks and some definitional changes.

One of the major obstacles to the passage of the American Data Privacy and Protection Act is California. The California Privacy Protection Agency used an emergency meeting to make clear its opposition to the federal legislation and any federal framework that would preempt California's strict privacy law. In addition, the California Attorney General has led a coalition of nine other state attorneys general (including New York) calling for Congress to respect the roles of states to enforce and provide strong consumer privacy laws. The coalition is concerned with the broad preemption included in the federal bill and calls for the legislation to allow states to protect their residents' information by setting more stringent privacy standards. The states point to the Health Insurance Portability and Accountability Act (HIPAA), passed in 1996, which gives state attorneys general concurrent enforcement authority and only preempted state laws that were contrary to HIPAA.

State Privacy Laws – Who is Next?:

Utah and Connecticut were the next two states to pass comprehensive data privacy legislation, increasing the total number of states with consumer data privacy laws to five. Both the Utah Consumer Privacy Act (UCPA) and Connecticut Data Privacy Act (CDPA) are similar and track closely with the Virginia Consumer Data Protection Act as well the Colorado Privacy Act (CPA). Like VCDPA, UCPA and CDPA include exclusions for nonprofits, governmental entities and data concerning individuals acting in a commercial or employment context.

UCPA applies to any entity that (1) conducts business in Utah or produces a product or service that is targeted to Utah residents; (2) has annual revenue of at least $25 million; and (3) either (a) controls or processes personal data of 100,000 or more consumers per year or (b) makes more than 50% of its gross revenue from the sale of personal data and controls or processes personal data of at least 25,000 consumers. The CDPA will apply to organizations that conduct business in Connecticut or produce products or services targeted to Connecticut residents and during the preceding calendar year either: (1) controlled or processed the personal data of at least 100,000 consumers, excluding data controlled or processed solely for the purpose of completing payment transactions; or (2) controlled or processed the personal data of at least 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.

The laws, like their counterparts in Virginia and Colorado, include broad consumer privacy rights including the right to access, the right to correct, the right to delete and the right to data portability. UCPA and CDPA also include sensitive data categories and neither include a private right of action. CDPA has an explicit exclusion of data that is processed solely for payment transactions. This means, that if entities collect only personal data to the extent necessary to process debit or credit card transactions to complete a sale, they will not be subject to the law.

California will also face substantial modifications to its data privacy regime in the coming year. The California Privacy Rights Act (CPRA) will become effective on January 1, 2023, and will amend the California Consumer Privacy Act. Notable changes include the inclusion of employment/human resources data in CPRA, new consumer rights including the right to correct and to limit the use of sensitive information and updated rules for privacy policies and notices.

All five of the state privacy laws (California, Virginia, Colorado, Connecticut and Utah) have compliance deadlines for covered entities that are quickly approaching in 2023. Specifically, California and Virginia will require compliance by January 1, 2023. Colorado and Connecticut will become effective on July 1, 2023 and Utah by December 31, 2023.

Cyber Insurance Carrier Aggressively Denying Coverage:

Travelers Insurance has filed a lawsuit asking the U.S. District Court for the Central District of Illinois to rescind a cybersecurity insurance policy because the insured company misrepresented its use of multifactor authentication (MFA), which was a condition of receiving coverage. Travelers learned that the insured did not have MFA in place after investigating a data breach experienced by the insured in May 2022. If the court finds for Travelers, this could have significant implications for the ability of organizations to receive and be covered by cybersecurity insurance.

Data Breach Costs Rise to $4.4 Million:

IBM, in conjunction with the Ponemon Institute, researched 550 data breaches that occurred thus far this year. The study found that the average cost of a data breach rose to $4.4 million. This is a 2.6% increase from last year, and an almost 13% increase since 2020. Stolen or compromised credentials, phishing and cloud misconfiguration were the three most common types of attack that led to a breach. Further,

organizations that deployed a zero trust[1] approach saved an average of $1 million dollars in breach costs compared to those who did not.

The increased costs associated with a breach, as well as the above-mentioned Travelers' lawsuit, are an important reminder to all businesses that having and maintaining cybersecurity insurance is critical in today's digital world. Business should review their cybersecurity insurance policies to ensure that they can comply with and accurately attest to the required safeguards for coverage, which often include MFA and required policies concerning vendor due diligence and risk assessments.

Trans-Atlantic Data Privacy Framework:

In March, President Biden and the European Commission president announced that the United States and EU reached a new transatlantic data flow agreement. The history of data flow between the EU and U.S. has been unstable, with the EU invalidating data flow frameworks twice since 2015. The two outstanding obstacles to data transfer since the invalidation of the EU-U.S. Privacy Shield in 2020 include a workable redress mechanism for EU citizens and uncertainly about whether the U.S. can meet the EU Court of Justice Initiative's standards for necessity and proportionality in relation to data processing. U.S. officials are continuing to work on an executive order that would implement the Trans-Atlantic Data Privacy Framework, which should be finalized shortly.

Data Privacy and Cybersecurity Training:

New York has become the first state to mandate continuing legal education in privacy, cybersecurity and data protection for attorneys. Effective July 1, 2023, all New York practitioners must complete at least 1 credit hour of privacy, cybersecurity and data protection training per each two-year cycle. This training can be focused on general continuing legal education or ethics relating to cybersecurity and data protection.

Other Global News:

Canada is now working toward passage of broad privacy legislation. The Canadian bill would govern the private sector and, if passed, would both amend and repeal portions of the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's current privacy law.

The Chinese Legislature has become more active concerning China's Personal Information Privacy Act (PIPL), including several new regulations passed over the last couple of months. In addition, the Chinese privacy regulator recently passed down a $1.2 billion fine against a Chinese ride-hailing company, alleging data security violations including illegal collection of screenshot information, facial recognition data and demographic and location information. The penalty also includes a personal fine of $147,000 to two individuals, the CEO as well as the president of the company.

For more information regarding any of the information included in this memo and compliance efforts businesses should be taking, contact Amber Lawyer, CIPP/E, Shannon Knapp, CIPP/US, Jessica Copeland or any attorney in the cybersecurity and data privacy practice.

1 Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and requires verification and authentication of everything trying to connect or log into the system before granting access.

BOND SCHOENECK & KING ATTORNEYS