Legal Matters®

Business
fall 2023

What businesses need to know about state consumer privacy legislation

A growing number of states are enacting consumer data privacy laws. In June, Texas, Florida and Oregon became the latest states to pass these laws designed to give consumers more choice over how companies access and manage their personal data.

California, Colorado, Connecticut, Utah and Virginia were among the first to pass legislation. So far, seven more states have followed in 2023, including Montana, Indiana, Iowa and Tennessee.

General scope: Consumer data privacy laws are regulations that govern how businesses collect, use and share personal information about consumers. These laws aim to protect consumers' privacy rights, such as the right to access, delete and bar resale of their personal information.

Most states are following the same core model legislation, but some variations exist. Oregon's legislation, for example, is unique in that consumers are entitled to obtain a list of any third parties to whom their information was disclosed.

Applicability: In general, businesses that collect personal information from consumers in a particular state must comply with that state's law. For example, a Massachusetts business that collects personal information from California consumers must comply with the California Consumer Privacy Act.

Most state laws have limited applicability to large businesses that process a significant amount of personal data as well as those in the business of selling personal data. However, analysts suggest that the recently passed Texas law is much more broad and could affect any business that collects, stores or otherwise handles personal data for any Texas resident — unless that business meets the SBA definition of a "small business."

GLBA exemption: So far, each state law includes some kind of exemption for financial institutions and related businesses (e.g., tax preparers, title companies, mortgage brokers, etc.) already subject to the Gramm-Leach-Bliley Act (GLBA). The GLBA exemption is intended to avoid conflicting and/or duplicative compliance requirements.

continued on page 3

MAHDAVI BACON HALFHILL & YOUNG, PLLC

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@mbhylaw.com | www.mbhylaw.com

SAFE Banking Act has limited bipartisan support

Recreational marijuana use is legal in 23 states and medical use is legal in 38. Nevertheless, marijuana remains a Schedule 1 controlled substance under federal law.

Because of this federal designation, businesses in the marijuana industry will often struggle to secure standard banking services, such as bank accounts, loans or the ability to accept credit cards. That means many of these businesses operate on a cash basis. That creates a lucrative target for thieves and a general public safety issue.

The Secure and Fair Enforcement Banking Act of 2023 (the SAFE Banking Act) is an effort to address this issue and make it easier for banks to engage with state-sanctioned marijuana businesses (SSMBs).

If enacted, the SAFE Banking Act would allow financial institutions to provide financial products and services to SSMBs as well as to the third-party providers that serve them. The act, however, would not require financial institutions to do business with these companies.

Theft deterrent

Advocates say the bill would help reduce theft at cash-heavy dispensaries. Proponents point to a 2015 analysis by the Wharton School of Business Public Policy Initiative, which found that half of all unbanked cannabis dispensaries had been robbed, with the average thief walking away with anywhere from $20,000 to $50,000 in a single theft.

"It makes absolutely no sense that legal businesses are being forced to operate entirely in cash, and it's dangerous — and sometimes even fatal — for employees behind the register," Washington Sen. Patty Murray said in a statement to The Associated Press last year.

Long-time coming

The SAFE Banking Act was first introduced in 2013, soon after Washington and Colorado became the first states to legalize the regulated sale of marijuana. While the House has passed a version of the bill several times, it never made it past the Senate. However, Senate Majority Leader Chuck Schumer has said that cannabis banking legislation is a priority this year.

Current conflict

Introduced by bipartisan sponsors, the legislation is supported by many business groups, state attorneys general, and the American Bankers Association. However, the legislation has hit bipartisan resistance over Section 10 of the bill, which deals with how regulators deter banks from engaging with bad actors.

The concern is that Section 10 requires a bank to notify customers when the federal government suspects they may be engaging in illegal activity. That could either deter regulators from taking effective action or warn criminals to "take the money and run," Rhode Island Sen. Jack Reed, a Democrat, said during a committee hearing.

Select consumer groups, including the Consumer Federation of America and the National Consumer Law Center, have issued concerns that Section 10 could inhibit efforts to stop payment fraud or other unlawful banking activity such as money laundering, hacks and scams.

IT test triggered $2.3 billion in unauthorized payments

An electronic payment processor was hit with a $25 million fine from the Consumer Financial Protection Bureau (CFPB) after an IT mistake accidentally withdrew $2.3 billion in unauthorized mortgage payments from more than 500,000 home-owner accounts.

The incident happened in April 2021, when ACI Worldwide was conducting tests of its payment platform. Instead of testing with dummy data, ACI used actual consumer information, including account numbers, routing numbers and mortgage amounts. During the test, ACI sent several large files into the ACH network, initiating approximately $2.3 billion in withdrawals from homeowners' accounts, the CFPB alleged in its announcement.

That subjected thousands of account holders to overdraft and insufficient fund fees. The CFPB says that the morning after ACI's test, "impacted account holders began noticing inaccuracies in their account balances." At one bank, "more than 60,000 accounts experienced more than $330 million in combined unlawful debits by that morning."

The CFPB found that ACI's actions violated federal consumer financial protection laws by illegally initiating withdrawals from borrower bank accounts and improperly handling sensitive consumer data.

The CFBP cited ACI's "inappropriate use of consumer data in its testing process. Specifically, the company failed to establish and enforce reasonable information security practices that would have prevented files created for testing purposes from ever being able to enter the ACH network."

Last year, the CFPB issued an enforcement circular describing how shoddy data handling practices can constitute violations of the Consumer Financial Protection Act.

The $25 million penalty will be deposited into the CFPB's victim relief fund. ACI also faces several class action lawsuits on behalf of affected consumers.

Former Uber exec sentenced, fined for covering up 2016 data breach

Joseph Sullivan, former chief security officer for Uber, was sentenced to three years of probation and 200 hours of community service and ordered to pay a $50,000 fine for covering up a 2016 data breach at the ride share company. While federal penalties for data breaches are not new, it's believed to be the first time an executive has been held criminally liable for a breach.

Sullivan joined Uber soon after the Federal Trade Commission began investigating a 2014 data breach at the company. Sullivan participated in Uber's response to that investigation, including giving sworn testimony to the FTC in March 2016.

Ten days after testifying, Sullivan received an email from a hacker who claimed to have found a vulnerability in the system. The hackers had downloaded personal information associated with 57 million Uber users and drivers. According to a statement from the U.S. Attorney General's Office, Sullivan then "executed a scheme to prevent any knowledge of the breach from reaching the FTC."

Uber paid the hackers $100,000 under the stipulation that they sign nondisclosure agreements and agree not to reveal the hack to anyone. The payments were purportedly made under Uber's "bug bounty" program, a way of paying legitimate researchers to find and report security vulnerabilities in a company's network.

The U.S. AG's Office alleged that the nondisclosure contracts falsely represented the nature of the breach and that Sullivan withheld information from most Uber lawyers. As a result, Uber entered into a preliminary settlement with the FTC without disclosing the 2016 breach.

In the fall of 2017, when new Uber management began investigating the 2016 breach, Sullivan allegedly lied to the company's CEO as well as outside counsel. However, leadership ultimately discovered the true nature of the breach and disclosed it publicly and to the FTC that year.

Judge signals harsher consequences in future

Charges against Sullivan focused on his failure to disclose and his efforts to hide the 2016 breach. Prosecutors recommended a 15-month sentence. According to the Wall Street Journal, Judge William Orrick said he was showing Sullivan leniency partly because this was the first case of its kind. However, Orrick warned that future offenders "should expect to spend time in custody."

Lessons for responding to a security breach

Information security professionals and other company leaders should stay up to date on risk mitigation and disclosure requirements. Know the legal reporting requirements for various breach scenarios. These may include reporting the breach to government agencies, affected individuals or both.

Work with legal counsel when responding to security incidents. An experienced attorney can help ensure that your legal obligations are met while helping to protect any privileged work product.

What businesses need to know about state consumer privacy legislation

continued from page 1

Technology: New tools are emerging to help companies comply with the regulations. For example, data privacy management software can track and manage your customers' personal data, as well as handle customer requests to access, delete or opt out of data sales.

Next steps: Businesses need to stay abreast of the changing data privacy landscape to determine which laws apply to them. That can be a complex process, so your organization may want to consult with a business attorney.

As more and more states pass these laws, it is likely that the federal government will eventually take action to create a comprehensive federal data privacy law. For now, however, businesses have a patchwork of legislation to manage.

MAHDAVI
BACON
HALFHILL &
YOUNG, PLLC
ATTORNEYS AT LAW

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@mbhylaw.com | www.mbhylaw.com

Environmental Protection Agency continues focus on PFAS

In June, the U.S. Environmental Protection Agency issued a final rule updating the Toxics Release Inventory or — TRI — chemical list to include nine additional PFAS (per- and polyfluoroalkyl substances) subject to reporting requirements.

Earlier this year, the EPA also proposed a rule to establish a National Primary Drinking Water Regulation for six types of PFAS, which would set maximum contaminant levels for drinking water supplies, subjecting water utilities to monitoring, reporting and treatment obligations.

The EPA is further expected to finalize a rule designating two PFAS (PFOA and PFOS) as "hazardous substances" under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA). That would give the agency the authority to mandate remediation actions or order companies to pay for the cost of remediation.

State laws

In addition to looming federal regulations, a number of states have already enacted their own PFAS restrictions. PFAS laws have been enacted in 24 states, banning their use in a wide array of consumer products, from carpeting to outdoor apparel and non-stick cookware. Twelve states have bans on PFAS in food packaging and four have restrictions on its use in personal care products.

About PFAS

PFAS are or have historically been used in various industrial and commercial applications, including firefighting foams, water-resistant fabrics, stain-resistant coatings, food packaging, and numerous other consumer products. Additionally, they have been utilized in certain industrial processes due to their unique properties, such as resistance to heat, water and oil.

Recently, PFAS have been dubbed "forever chemicals" because they don't break down in the environment or the human body. Studies have linked them to cancer, infertility and other diseases.

Next steps

The proposed regulations could have a significant impact on companies that use or have used PFAS. Companies that are currently using PFAS may need to find alternative compounds or processes. However, companies that have used PFAS in the past may face legal claims due to environmental contamination, personal injury or misrepresentation.

Companies should work to understand how PFAS are used in their products today, as well as the company's past production processes. An experienced attorney can help you gauge your legal risk. If your company is subject to a remediation mandate or injury claim, an attorney can help you understand your rights and obligations and represent the company in negotiations with the government or other parties.