Legislative Update 249

December 1, 2024

Highlights this issue:

- On November 14, the Federal Trade Commission's (FTC) announced the new Negative Option Rule will take effect on January 14, 2025. This rule requires sellers to make it as easy for consumers to cancel subscriptions as it is to sign up for them.
- On November 12, the CFPB released a report on the state of federal and state privacy safeguards for consumer financial data. The report is intended to highlight, from the CFPB's perspective, areas where federal financial laws do not provide blanket preemption and where states may take additional steps to protect consumers.
- On November 21, the CFPB announced a final rule to oversee large nonbank companies offering digital payment apps. This rule grants the CFPB examination and supervision authority to ensure that companies handling over 50 million transactions annually comply with federal laws.
- On November 8, the California Privacy Protection Agency's (CPPA) Board of Directors voted to advance a package of draft regulations related to automated decision-making technology, cybersecurity audits, risk assessments, and updates to existing regulations. This action initiates the formal rulemaking process to obtain public comment. The proposals are moving forward despite concern about scope and cost.

FEDERAL UPDATE

FTC announces effective date for negative option rule; CFPB looks at enforcement

On November 14, the Federal Trade Commission's (FTC) announced the new Negative Option Rule will take effect on January 14, 2025. This rule requires sellers to make it as easy for consumers to cancel subscriptions as it is to sign up for them. It applies to almost all negative option programs across various media and aims to simplify the cancellation process for unwanted subscriptions and memberships. The rule sets requirements for sellers, such as disclosing all necessary information to consumers, obtaining informed consent before charging them, and allowing easy cancellation of products or services. Some financial firms already let consumers block certain recurring payments, but the rule emphasizes the need for direct cancellation with the company charging the payments. Two separate challenges were filed to block the rule's

implementation – one by the Michigan Press Association and the NFIB in the Sixth Circuit Court of Appeals, and a second filed by multiple trade associations, including the IAB, the Electronic Security Association and The Internet & Television Association in the Fifth Circuit. The petitions ask the courts to vacate the rule and set it aside, claiming that the FTC violated the Administrative Procedures Act and went beyond its authority in issuing the rule. Both lawsuits are pending.

CFPB releases report on state data privacy laws and their impact on consumer financial data

On November 12, the CFPB released a report on the state of federal and state privacy safeguards for consumer financial data. The report is intended to highlight, from the CFPB's perspective, areas where federal financial laws do not provide blanket preemption and where states may take additional steps to protect consumers.

The report expresses concern about industries increasingly building business models premised on the monetization of consumer data, leaving consumers without adequate privacy safeguards due to state law exemptions. The report points out that state privacy laws often exempt financial data regulated by federal laws like the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA), meaning data held by financial institutions may lack enhanced privacy protections, including the right to delete or correct information. The CFPB urges state policymakers to examine these gaps in data privacy laws.

CFPB issues final rule on oversight of digital payment apps

On November 21, the CFPB announced a final rule to oversee large nonbank companies offering digital payment apps. This rule grants the CFPB examination and supervision authority to ensure that companies handling over 50 million transactions annually comply with federal laws. Many large tech companies offering payment apps were previously not under CFPB supervision. In the announcement, CFPB Director Rohit Chopra emphasized the necessity of digital payment apps and the importance of protecting consumer privacy, combating fraud, and preventing illegal account closures. The rule enables proactive examinations to ensure compliance. The CFPB has previously warned "Big Tech" firms about their consumer protection obligations, highlighted the lack of federal deposit insurance for funds in popular apps, and researched regulations in the "tap-to-pay" market.

STATE UPDATES

CPPA proposes rules on automated decision making, risk assessments, and cybersecurity

On November 8, the California Privacy Protection Agency's (CPPA) Board of Directors voted to advance a package of draft regulations related to automated decision-making technology, cybersecurity audits, risk assessments, and updates to existing regulations. This action initiates the formal rulemaking process to obtain public comment. The proposals are moving forward despite concern about scope and cost.

Board Member Alastair Mactaggart was the lone opposition, raising objections that the scope of the automated decision-making technology (ADMT) and risk assessment proposals go beyond what was intended by the law. Key issues raised by Mactaggart and business groups include the broad definition of ADMT, which would encompass behavioral advertising, subjecting it to opt-out requirements. Additionally, business groups warned that the broad definitions would necessitate burdensome risk assessments for technology use and that the proposal would cover artificial intelligence products that the agency does not have authority to regulate.

The board also considered a revised regulatory impact assessment, which covers the economic cost and benefits of rulemaking. The assessment indicated that the direct cost to California businesses subject to the regulations would be $3.5 billion. Despite concerns about the high cost, the Board believed that any further revisions should be made after public comments are received.

Public comments on the proposed regulations are due by January 14, when the CPPA will also hold a public hearing to consider oral statements. Experian, along with the federal and state trade associations, will review the proposed regulations for potential comments.

CPPA finalizes expanded data broker rule, prepares for deletion mechanism

On November 8, the California Privacy Protection Agency's Board of Directors approved new regulations expanding the definition of a data broker. The Board unanimously approved the regulations to clarify what is considered a "direct relationship" in the definition of a data broker. Under the regulations, a business would be considered a data broker if it collects a consumer's personal information not directly from the consumer and sells the information to another party. The regulations also update registration requirements, mandating that data brokers disclose the approximate percentage of their general data broker activities.

The CPPA Board also received an update about the implementation of the data broker deletion mechanism. Under the 2023 law, the agency must establish a process for a consumer to make a single deletion request with registered data brokers. Staff indicated that building the system, which must be established by January 1, 2026, would cost approximately $4.4 million. Using some existing funds, staff encouraged the board to

increase the annual data broker registration fee from $400 to $6,600 to cover the build. The Board is likely to consider the increase in a December meeting. Staff also indicated plans in 2025 to contract with a vendor to build the mechanism and draft regulations establishing the policy requirements.

Michigan considers reproductive data privacy bill

As Michigan nears the end of its legislature session, a pair of reproductive data privacy bills have been deemed priorities by the Governor's office. HB6077 and SB 1082 would establish consumer protections for reproductive health data not covered under HIPAA. As drafted, the bills require that entities collecting or processing this data must provide their privacy policy to individuals, obtain clear consent, and only use the data for specific purposes such as providing requested services, completing transactions, complying with legal obligations, or protecting public health and safety. Entities must also offer a clear way for individuals to access and delete their health data via a link on their homepage. The measures do not apply to entities covered by HIPAA. The legislation would place enforcement with the Attorney General.

Michigan committee approves judicial privacy bill

After passing the Michigan House earlier this year, on November 13, a Senate Committee on Civil Rights approved HB5724. The bill allows a judge to request that a public body or person not publicly post or display the personal identifying information of a judge or a judge's immediate family member. A judge may submit a written request, on a form prescribed by the state court administrative office, to a public body or person to remove a public posting or display of personal identifying information of the judge or the judge's immediate family member. A person that has received such a request must not publicly post, display, or transfer the specified personal identifying information of a judge or a judge's immediate family member, as applicable. The bill provides exceptions for data subject to financial laws, including the FCRA and GLBA, as well as the federal DPPA and HIPAA. The bill is now eligible to be considered by the full Senate.