Legislative Update 243

June 1, 2024

Highlights this issue:

- On May 16, the U.S. Supreme Court issued a decision in Consumer Financial Protection Bureau et al. v. Community Financial Services Association of American, Ltd., et al. stating that the CFPB's funding method, which operates outside the congressional appropriations process and is funded through the Federal Reserve, is constitutional. The Court ruled 7-2 to reject an argument by the Community Financial Services Association, which represents short term lenders, that the CFPB's annual budget process violated the U.S.
- On May 15, the Bipartisan Senate Artificial Intelligence Working Group released its policy roadmap for AI policy along with a one-page document outlining the policy roadmap's priorities. The working group is led by Senate Majority Leader Chuck Schumer (D-NY), Sens. Mike Rounds (R-SD), Martin Heinrich (D-NM), and Todd Young (R-IN) and seeks to recognize the challenges and risks associated with AI technologies.
- On May 23, a House Committee on Energy and Commerce subcommittee advanced a working draft of the American Privacy Rights Act (APRA). The proposal, which has not been officially introduced, includes many of the provisions from a bill passed by the House committee in 2022, the American Data Privacy and Protection Act, and would establish a federal privacy law intended to preempt similar state laws and provide enforcement through a private right of action.
- On May 10, the California Privacy Protection Agency (CPPA) held their May board meeting where it reviewed a possible rulemaking to expand the definition of "data broker" for registration requirements. Under current law, a company is required to register as a data broker if it collects and sells information regarding consumers it does not have a direct relationship with.

FEDERAL UPDATE

Supreme court rules on CFPB case, finds funding is constitutional

On May 16, the U.S. Supreme Court issued a decision in Consumer Financial Protection Bureau et al. v. Community Financial Services Association of American, Ltd., et al. stating that the CFPB's funding method, which operates outside the congressional appropriations process and is funded through the Federal Reserve, is constitutional. The Court ruled 7-2 to reject an argument by the Community Financial Services Association, which represents short term lenders, that the CFPB's annual budget process violated the U.S. Constitution's Appropriations Clause. In the decision, Supreme Court Justice

Clarence Thomas, writing for the majority, stated that funding does not need to go through the congressional appropriations process and explained that the statute, which allows the CFPB to draw money from the combined earnings of the Federal Reserve System to perform its duties, satisfies the Appropriations Clause.

The CFPB, along with other federal agencies, still faces continued litigation pressure around regulatory authority. In January 2024, the Supreme Court heard two cases considering whether to overturn Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc. (Chevron). In Chevron, the Supreme Court established a two-part test to determine the level of deference a court will give to an agency's interpretation of a statute that delegates authority to an agency. If Chevron is overturned, federal agencies may be limited in terms of the ability to interpret regulatory authority– such as filling gaps or defining terms in the statute.

Senate bipartisan AI working group releases AI policy roadmap

On May 15, the Bipartisan Senate Artificial Intelligence Working Group released its policy roadmap for AI policy along with a one-page document outlining the policy roadmap's priorities. The working group is led by Senate Majority Leader Chuck Schumer (D-NY), Sens. Mike Rounds (R-SD), Martin Heinrich (D-NM), and Todd Young (R-IN) and seeks to recognize the challenges and risks associated with AI technologies. The policy roadmap includes the following priorities: create a strong comprehensive federal data privacy framework, increase funding for AI innovation, and utilize existing laws for AI enforcement. The roadmap also discusses prioritizing the development of standards for AI testing and addressing risks posed by "deepfakes" and foreign adversaries. While there have been several bills on AI introduced in the Congress, there is little consensus on the correct regulatory framework.

House Energy and Commerce Subcommittee advances American Privacy Rights Act

On May 23, a House Committee on Energy and Commerce subcommittee advanced a working draft of the American Privacy Rights Act (APRA). The proposal, which has not been officially introduced, includes many of the provisions from a bill passed by the House committee in 2022, the American Data Privacy and Protection Act, and would establish a federal privacy law intended to preempt similar state laws and provide enforcement through a private right of action. Notably, the proposal would divert from state privacy frameworks by establishing strict data minimization standards that only allow the processing of data for permitted purposes outlined in the legislation, which does not include processing of third-party data used in advertising. The bill would also establish a data broker registry at the Federal Trade Commission with a central "Do Not Collect" mechanism and a separate "Delete" option, allowing consumers to request that all data brokers stop collecting personal information as well as delete their personal information. As drafted, the bill contains exceptions for data under GLBA, HIPAA, FCRA, and data used to prevent fraud. The US Chamber of Commerce, along with other trade associations, submitted a letter to the committee outlining significant concerns with the legislation. The bill now progresses to the full Energy and Commerce

committee. A similar proposal in the Senate has not been scheduled for consideration.

CFPB releases RFI on mortgage closing costs

On May 30, the CFPB released a Request for Information ("RFI") regarding fees imposed in residential mortgage transactions. The CFPB wants to understand why closing costs are increasing, who is benefiting, and how costs for borrowers and lenders could be lowered. The RFI specifically cites the cost of credit reports as a contributor to rising prices. The RFI was preceded by a speech by CFPB Director Rohit Chopra at the Mortgage Bankers Association conference on May 20. In his speech, Chopra discussed the high closing costs associated with homebuying, including needing to pay for credit reports. The director claimed that closing costs, driven in part by the cost of credit reports, has outpaced inflation and that lenders who pass on those screening costs may risk violating legal limitations on charging borrowers' legitimate fees. One potential option floated by the Director was fee caps for credit reports, as well as limiting the charging of consumers multiple times for a single transaction.

CFPB issues interpretive rule recognizing BNPL lenders as credit card providers

On May 22, the Consumer Financial Protection Bureau announced that it issued an interpretive rule reaffirming that Buy Now, Pay Later (BNPL) lenders are credit card providers. Under this rule, BNPL lenders must extend the same legal protections and rights to consumers as traditional credit cards. In the announcement, CFPB Director Rohit Chopra emphasized the importance of protecting consumers under existing laws and regulations regardless of if they use a credit card or BNPL. According to the announcement, the interpretive rule will clarify how BNPL lenders qualify as credit card providers under the Truth in Lending Act. The interpretive rule will also require BNPL lenders to investigate disputes, refund returned products or cancelled services, and provide billing statements. The announcement highlighted several initiatives by the CFPB regarding the "rapidly" growing BNPL market, including a report into BNPL on issues such as debt accumulation, regulatory loopholes, and data collection practices as well as a market report, entitled "Buy Now, Pay Later: Market trends and consumer impacts." The announcement stated that comments from the public on the interpretive rule will be accepted until August 1, 2024.

STATE UPDATES

California Privacy Agency considers expansion of data broker definition; holds stakeholder sessions on upcoming privacy rulemaking

On May 10, the California Privacy Protection Agency (CPPA) held their May board meeting where it reviewed a possible rulemaking to expand the definition of "data broker" for registration requirements. Under current law, a company is required to register as a data broker if it collects and sells information regarding consumers it does not have a direct relationship with. The draft regulations would address what it means for a company to have a "direct relationship." The proposal states that a business will still meet the definition of data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.

This month, the Agency also conducted three statewide stakeholder session related to their upcoming rulemaking on automated decision-making technology (ADMT), risk assessments, and cybersecurity audits. The sessions are intended to help the public learn about and provide preliminary feedback on the Agency's proposed regulations before the Agency moves to the formal rulemaking process. One of the sessions was provided virtually and is available to watch online. Each session included a brief presentation by CPPA staff on the proposed rules and an overview of the rulemaking process when the formal comment period opens, likely later this year.

Colorado approves new protections for children's data, expands definition of "sensitive data" in privacy law

On May 15, the Colorado General Assembly sent SB 41 to Governor Polis. If signed, this bill would amend the Colorado Privacy Act to require new duties for companies that offer any online service, product, or feature to a minor under the age of 18. Businesses would need to take reasonable care to avoid heightened risk of harm to minors, including obligations to protect against foreseeable risk of unfair or deceptive treatment; financial, physical, or reputational injury; a security breach of the personal data; or an intrusion upon the solitude or seclusion of the minor. The bill would require the minor's consent, or the parent's verifiable consent for a child under 13 years of age, to process the minors' data for targeted advertising, sales, and profiling and would restrict controllers' collection of precise geolocation data from minors. If signed, the bill has an effective date of October 1, 2025. Additionally, the Governor signed HB 1058 to expand the definition of "sensitive data" under the Colorado Privacy Act, which requires consent to collect. The bill would add "biological data" and "neural data" to the definition of "sensitive data." Experian continues to work with our trade associations, including the Association of National Advertisers, to advocate for alignment among state privacy laws.

Minnesota and Vermont approve privacy laws, while Massachusetts bill advances

Minnesota

On May 24, Minnesota Governor Tim Walz signed an omnibus commerce package that included comprehensive privacy legislation, HF 4757. The privacy bill - also known as the Minnesota Consumer Data Privacy Act - takes effect on July 31, 2025, and grants consumers the right to access, correct, delete, and port their data, while allowing for consumers to opt out of the sale, targeted advertising, or profiling with data about them. The legislation largely follows a framework found in other state privacy laws. The Attorney General has exclusive enforcement authority and no rulemaking obligations. The Act also includes assessment and opt-in consent requirements for "sensitive data," including "specific geolocation data."

Vermont

On May 13, the Vermont legislature passed H. 121, a bill regarding consumer privacy and data brokers, and sent the bill to the Governor. The bill's framework follows other state laws but includes significant expansions. If enacted, the Vermont privacy law would be the first state to some level of enforcement by permitting a consumer's right to a private right of action ("PRA"). Under the bill, a consumer harmed by a data broker or large data holder's violations would have the right to sue and recover damages. The PRA would be limited to the collection of sensitive data, processing data in a manner that discriminates against an individual, and the confidentiality of consumer health data. The PRA does not go into effect until 2027 and would need to be revisited by the legislature before sunsetting in 2029. The legislation would also include new obligations for consumer data breaches by data brokers. Registered data brokers would be required to provide consumer notice for any breaches of "brokered personal information," unless there is no risk of harm in which case notice is provided to the Attorney General. If signed into law, the bill would go into effect July 1, 2025. The data breach provision would go into effect July 1, 2024.

Massachusetts

On May 9, a Massachusetts Senate Committee on advanced comprehensive privacy legislation, SB 2770. The bill would take a substantial deviation from other state privacy laws and generally follows previously introduced federal privacy legislation. The bill would limit the collection and processing of personal information unless there is a specific permissible purpose outlined in the legislation. The permitted purposes include, among others, providing or maintaining a product or service requested by the consumer, fraud prevention, and fulfilling a warranty. The bill does not provide a permissible purpose for advertising. The bill would also limit the collection of location information and prohibit the sharing of location information with third parties. The legislation would provide enforcement through a private right of action. The bill has significant opposition from the business community and is pending in the Senate Committee on Ways and Means.

California legislature advances privacy and artificial intelligence bills
Privacy
On May 22, the California Assembly passed AB 3048, a bill that would require businesses to include a setting on browsers and devices that enables a consumer to send an automatic opt-out preference signal. The bill also authorizes the CPPA to adopt regulations as necessary to implement and administer those provisions, including updating the definitions of "browser" and "device" to address changes in technology, data collection, obstacles to implementation, or privacy concerns. The bill is now eligible to be heard in the Senate.

On May 21, the California Assembly passed AB 1849. If enacted, AB 1949 would prohibit a business from collecting, using, or disclosing personal information related to a consumer less than 18 years of age unless the consumer or the consumer's parent or guardian affirmatively authorizes the collection, use, or disclosure of the personal information. The bill would also extend existing CCPA consent requirements related to sale and sharing of personal information related to U-16s to U-18s. In addition, the bill would require the California Privacy Protection Agency to adopt regulations to establish technical specifications for an opt-out preference signal that allows the consumer's parent or guardian, to specify that the consumer is less than 13 years of age, and address age verification and when a business must treat a consumer as being less than 13 or 18 years of age for purposes of the CCPA.

Artificial Intelligence (AI)
California considered 32 pieces of legislation on AI this year, with five bills AB 2013, AB 2930, AB 3211, SB 1047, and SB 942 advancing out of at least one legislative chamber. Experian is working directly and along with our trade associations, including CalChamber, CalRetailers, ANA, and CDIA, to educate lawmakers about the impact of the proposals. None of the proposals have become law thus far.

AB 2013
AB 2013 would require documentation on websites of developers regarding datasets used in the development of AI systems. Documentation would include a high-level summary of the datasets used in the development of the system or service, including, the data's sources or owners, size of the dataset, categories of data included, and descriptions of any cleaning or processing. The only exception included in the rule is if the AI system is used to help ensure security and integrity.
AI is broadly defined in the bill as an "engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments." The definition of developer is similarly broad, including any entity that "produces an artificial intelligence system or service, or substantially modifies an artificial intelligence system or service for use by a third party for free or for a fee."

AB 2930
AB 2903 would require deployers and developers to perform impact assessments on automated decision-making tools (ADMT), provide the results of that assessment to the Civil Rights Department, and not use any decision tool which is found to be discriminatory. The bill defines an ADMT as any automated tool that makes a significant factor in a consequential decision, including “a financial service provided by a mortgage company, mortgage broker, or creditor.”
Impact assessments would include a description of the automated decision tool’s outputs, a summary of the categories of information collected from natural persons, and each category of personal and sensitive information identified. The bill also includes legal recourse for use of a model that was found to be discriminatory with up to $25,000 per violation of algorithmic discrimination and a right to cure within 45 days. A consumer would also have the right to receive a notice prior to the use of an ADMT and the ability to opt-out of its use.

AB 3211
AB 3211 would make it mandatory to label all artificially generated content. Additionally, all “real” content – such as video and audio recordings – must be labeled as such, and large online platforms must be required to prominently display these labels. Providers and generators of AI content must embed watermarks on all outputs, and digital cameras must offer users the option to embed their content with watermarks marking their content as “real.”

The provisions in the bill extend to chatbots and conversational systems, which must disclose to users that they are AI generated and gain their consent before beginning a conversation. The penalty for a violation of the bill’s provisions is the greater of $1,000,000 or 5% of the violator’s annual global revenue.

SB 1047
SB 1047 establishes the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, requiring a developer of a nonderivative covered model that is not the subject of a limited duty exemption to submit an annual certification to the Frontier Model Division. The only exception is if the non-derivative model falls under a limited duty exemption. “Limited duty exemption” means that a developer can reasonably exclude the possibility that the covered model has a hazardous capability when accounting for a reasonable margin for safety and the possibility of post training modifications.

SB 942
SB 942 establishes the California AI Transparency Act which requires a covered provider to create an AI detection tool by which a person can query the covered provider as to the extent to which text, image, video, audio, or multimedia content was created, in whole or in part, by a generative AI system. The act would also require a covered provider to include a visible disclosure in AI-generated content, that identifies the content as generated by AI. “Covered provider” is defined as a business that provides a generative AI system that has, on average over the preceding 12 months, over 1,000,000

monthly visitors or users and is publicly accessible within the geographic boundaries of the state.

Colorado enacts artificial intelligence law while Connecticut bill fails
On May 17, Colorado Governor Jared Polis signed SB 205. The legislation creates an AI bill of rights that will require developers and deployers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination and to make certain disclosures on or after February 1, 2026. The law can only be enforced by the Attorney General, and it contains exemptions if the developer or deployer is already subject to other legal obligations. While Governor Polis signed the bill, he also expressed reservations and called on the legislature to work with stakeholders to amend the law if the U.S. Congress does not enact a national law before the state law takes effect in two years. Several trade associations, including AFSA and ANA, sent a joint letter to Governor Polis asking him to facilitate a stakeholder process so that unaddressed issues can be resolved before the law takes effect.

Connecticut had an almost identical bill (SB 2) that failed after the Governor threatened to veto the legislation. The legislature is expected to work on the bill prior to reconsidering it in 2025.

Minnesota enacts medical debt law while bills advance in Illinois and California
Minnesota
On May 21, Minnesota Governor Tim Walz signed an omnibus commerce package that includes a ban on furnishing and reporting medical debts, SF 4097. The bill prohibits collecting parties from furnishing medical debt to a consumer reporting agency ("CRA") and prohibits CRAs from making a consumer report containing information that the CRA knows or should know concerns medical debt. CDIA opposed the legislation based on FCRA preemption.

Illinois
On May 16, the Illinois General Assembly passed SB 2933, a bill to ban the reporting of medical debt. The bill would amend the consumer protection statute to make it an unlawful practice for a consumer reporting agency to furnish a report containing adverse information that the CRA knows or should know relates to medical debt. Also, a CRA could not maintain in the file any information relating to medical debt incurred by a consumer. While CDIA opposed this legislation because it is preempted by Federal law, the legislature passed it after amending the definition of medical debt to exempt most credit cards and other extensions of credit.

California
On May 21, the California Senate passed a ban prohibiting medical debt on credit reports. The bill is supported by the Attorney General and the CFPB has taken the unusual step of submitting a letter to the committee in support of the bill. The bill will next be heard by the Assembly.

New Jersey Governor considers public records legislation
On May 13, the New Jersey legislature passed S. 2930, sending the bill to Governor Phil Murphy.
The bill would amend the Open Public Records Act (OPRA) to address the complaints of local governments and state agencies that had to respond to abusive public records requests and often pay the attorney fees of activists and malcontents for technical errors. As introduced in March, the bill would have disrupted access to records that are important to public safety and commerce in the state by prohibiting the resale of information from public records. It would have also defined data brokers and prohibited them from buying or selling public records. Experian was able to engage with the legislators in New Jersey through CDIA and the Coalition for Sensible Public Record Access to ensure that businesses would be able to have access to information in the records for critical uses.

The bill still faces stiff opposition from various advocacy organizations and public records attorneys, The Governor has 45 days to sign or veto the bill or it automatically becomes law.

Minnesota enacts judicial privacy law
On May 24, judicial data privacy legislation became law when Minnesota Governor Tim Walz signed the omnibus judiciary bill, HF 5216. The judicial data privacy provision has an effective date of August 1, 2024. Under the judicial data privacy provisions, no business shall knowingly publicly post, display, publish, sell, or otherwise make available on the Internet the personal information of any judicial official within 30 days of receiving a written notice from the protected individual. The law's exemptions include FCRA, consumer reporting agencies, DPPA, fraud, GLBA data and financial institutions, HIPAA covered entities and business associates, UCC records, and publicly available information.

CDIA worked with the proponents and the legislators to secure the necessary amendments to provide clear requirements and important exemptions.