Published on *The National Law Review* https://natlawreview.com

The BR Privacy & Security Download: April 2025

Article By:

Sharon R. Klein

Philip N. Yannella

Alex C. Nisenbaum

Harrison Brown

Jennifer J. Daniels

Jeffrey N. Rosenthal

STATE & LOCAL LAWS & REGULATIONS

Virginia Governor Vetoes AI Bill: Virginia Governor Glenn Youngkin vetoed the Virginia High-Risk Artificial Intelligence Developer and Deployer Act (the "Act"). The Act was similar to the Colorado AI Act and would have required developers to use reasonable care to prevent algorithmic discrimination and to provide detailed documentation on an AI system's purpose, limitations, and risk mitigation measures. Deployers of AI systems would have been required to implement risk management policies, conduct impact assessments before deploying high-risk AI systems, disclose AI system use to consumers, and provide opportunities for correction and appeal. The governor stated that the Act's "rigid framework fails to account for the rapidly evolving and fast-moving nature of the AI industry and puts an especially onerous burden on smaller firms and startups that lack large legal compliance departments" and that the Act "would harm the creation of new jobs, the attraction of new business investment, and the availability of innovative technology" in the state. The governor also noted that existing state laws "protect consumers and place responsibilities on companies relating to discriminatory practices, privacy, data use, libel, and more" and that an executive order issued by the governor in 2024 established safeguards and oversight for AI use.

CPPA Advances Regulations for Data Broker Deletion Mechanism: The California Privacy Protection Agency ("CPPA") advanced proposed California Delete Act regulations through the establishment of the Delete Request and Opt-Out Platform ("DROP"). These regulations would create an accessible mechanism for consumers to request the deletion of all their non-exempt personal information held by registered data brokers via a single request to the CPPA. The proposed rules also clarify the definition of a "direct relationship" with a consumer, specifying that simply collecting personal information directly from a consumer does not constitute a direct relationship

unless the consumer intends to interact with the business. This revision could bring more businesses, such as third-party cookie providers, under the definition of data brokers. Consumers will likely be able to access DROP by January 1, 2026, and data brokers will be required to access it by August 1, 2026.

Virginia Enacts Reproductive Privacy Law: Virginia enacted amendments to the Virginia Consumer Data Protection Act to prohibit the collection, disclosure, sale, or dissemination of consumers' reproductive or sexual health data without consent. "Reproductive or sexual health information" is defined under the law as "information relating to the past, present, or future reproductive or sexual health of an individual," including: (1) efforts to research or obtain reproductive or sexual health information services or supplies, including location information that may indicate an attempt to acquire such services or supplies; (2) reproductive or sexual health conditions, status, diseases, or diagnoses, including pregnancy, menstruation, ovulation, ability to conceive a pregnancy, whether an individual is sexually active, and whether an individual is engaging in unprotected sex; (3) reproductive and sexual health-related surgeries and procedures, including termination of a pregnancy; (4) use or purchase of contraceptives, birth control, or other medication related to reproductive health, including abortifacients; (5) bodily functions, vital signs, measurements, or symptoms related to menstruation or pregnancy, including basal temperature, cramps, bodily discharge, or hormone levels; (6) any information about diagnoses or diagnostic testing, treatment, or medications, or the use of any product or service relating to the matters described in 1 through 5; and (7) any information described in 1 through 6 that is derived or extrapolated from non-health-related information such as proxy, derivative, inferred, emergent, or algorithmic data. "Reproductive or sexual health information" does not include protected health information as defined by HIPAA.

Oregon Attorney General Releases Enforcement Report on Oregon's Consumer Privacy Act: The Oregon Attorney General released a six-month report on the enforcement of Oregon's comprehensive privacy law, the Consumer Privacy Act ("OCPA"), which took effect on July 1, 2024. The report provides that, as of the beginning of 2025, the Privacy Unit within the Civil Enforcement Division at Oregon's Department of Justice ("Privacy Unit") received 110 complaints. Most of these complaints were about online data brokers. In the last six months, the Privacy Unit initiated and closed 21 matters after sending cure notices (the OCPA provides for a 30-day cure period, which sunsets on January 1, 2026) and broader information requests. Some of the most common deficiencies identified were the lack of requisite disclosures or confusing privacy notices (*e.g.*, not listing the OCPA rights or not naming Oregon in "your state rights" section), and lacking or burdensome rights mechanisms (*e.g.*, the lack of a webpage link for consumers to submit opt-out requests).

Utah Becomes First State to Enact Legislation Requiring App Stores to Verify Users' Ages:Utah has enacted the App Store Accountability Act, which mandates that major app store providers must verify the age of every user in the state. For users under 18, the law requires verifiable parental consent before any app can be downloaded, including free apps, or any in-app purchases can be made. App stores must also confirm a user's age category (adult, older teen (16-17), younger teen (13-15), or child (under 13)). When a minor creates an account, it must be linked to a parent's account. App store providers are responsible for building systems to verify ages, obtain parental consent, and share this data with app developers. They must also provide sufficient disclosure to parents about app ratings and content and notify them of significant changes to apps their children use, requiring renewed consent. Violations of the law will be considered deceptive trade practices, and the act creates a private right of action for harmed minors or their parents. The core requirements for age verification and parental consent are set to take effect on May 6, 2026.

Michigan Legislative Committee Advances Judicial Privacy Bill: The Michigan Senate Committee on Civil Rights, Judiciary, and Public Safety provided a favorable recommendation for a judicial privacy bill that would allow state and federal judges to request the deletion of their personal information from public listings. The Michigan bill would create a private right of action with mandatory recovery of legal fees for any entity that fails to respond to a valid deletion request. The purpose of the bill is to protect against a significant uptick in threats against judicial officers and their families. The bill is based on Jersey's Daniel's Law, which has sparked a wave of class action lawsuits against data brokers and online listing companies. If passed, businesses that receive a valid request from a member of the judiciary or their immediate family members under the proposed bill would have to remove from publication any covered information pertaining to the requestor.

Virginia Legislature Passes Consumer Data Protection Act Amendments Restricting Minors' Use of Social Media; Governor Declines to Sign: The Virginia Legislature unanimously passed a bill to amend the Virginia Consumer Data Protection Act to limit minors' use of social media to one hour per day. Specifically, the bill would require that any social media platform operator to (1) use commercially reasonable methods, such as a neutral age screen mechanism, to determine whether a user is a minor younger than 16 years of age and (2) limit any such minor's use of such social media platform to one hour per day, per service or application, and allow a parent to give verifiable parental consent to increase or decrease the daily time limit. Virginia Governor Glenn Youngkin declined to sign the bill as passed, recommending several changes to strengthen the bill. These recommendations include raising the age of covered users from 16 to 18 and requiring social media platform operators to disable infinite scroll features and auto-playing videos unless the operator has obtained verifiable parental consent.

FEDERAL LAWS & REGULATIONS

Lawmakers Reintroduce COPPA 2.0 to Strengthen Children and Teens' Online Privacy:U.S. Senators Bill Cassidy (R-LA) and Edward Markey (D-MA) have reintroduced the Children and Teens' Online Privacy Protection Act ("COPPA 2.0"), aiming to update online data privacy rules to better protect children and teenagers. The bill seeks to address the youth mental health crisis by stopping data practices that contribute to it. COPPA 2.0 proposes several key measures, including a ban on targeted advertising to children and teens and the creation of an "Eraser Button," allowing users to delete personal information. It also establishes data minimization rules to limit the excessive collection of young people's data and revises the "actual knowledge" standard to prevent platforms from ignoring children on their sites. Furthermore, the legislation would require internet companies to obtain consent before collecting personal information from users aged 13 to 16. Previous versions of COPPA 2.0 have advanced in Congress, passing the Senate and a House committee in the past.

White House Seeks Stakeholder Input for Trump Administration's AI Action Plan:The White House Office of Science and Technology Policy issued a Request for Information to gather public input on the administration's AI Action Plan. This AI Action Plan intends to define priority policy actions to enhance America's position as an AI powerhouse and prevent unnecessary regulations from hindering private sector innovation. The focus is on promoting U.S. competitiveness in AI, limiting regulatory burdens, and developing safeguards that support responsible AI advancement. Stakeholders, including academia, industry groups, and private sector organizations, were encouraged to share their policy ideas on topics such as model development, cybersecurity, data privacy, regulation, national security, innovation, and international collaboration. The submitted comments will be used to inform future regulatory proposals.

Congresswoman Issues RFI for Input on U.S. Privacy Act Reform: Congresswoman Lori Trahan

(D-MA) announced her effort to reform the Privacy Act of 1974, aiming to protect Americans' data from government abuse. The proposed reforms seek to address outdated provisions in the act and enhance privacy protections for individuals in the digital age. Trahan emphasized the importance of updating the act to reflect modern technological advancements and the increasing amount of personal data collected by government agencies. The initiative includes measures to ensure greater transparency, accountability, and oversight of data collection practices. Trahan highlights the urgency of the issue as a result of access by the Department of Government Efficiency staff to personal data held by several agencies and calls for legislative action to protect citizens' privacy rights and prevent government overreach.

U.S. LITIGATION

Court Blocks Enforcement of California Age-Appropriate Design Code: Industry group NetChoice scored yet another victory over the California Age-Appropriate Design Code Act, obtaining a second preliminary injunction temporarily blocking its enforcement. The act was passed unanimously by the California legislature in 2022 and—if enforced—would place extensive new requirements on websites and online services that are "likely to be accessed by children" under the age of 18. NetChoice won its first preliminary injunction in September 2023 on the grounds that the act would likely violate the First Amendment. In August 2024, the Ninth Circuit partially upheld this injunction, finding that NetChoice was likely to succeed in demonstrating that the act's data protection impact assessment provisions violated the First Amendment. However, the Ninth Circuit remanded the case for determination of the constitutionality of the remaining provisions as well as whether any unconstitutional provisions could be severed from the remainder of the act. On remand, Judge Beth Labson Freeman again granted NetChoice's motion for preliminary injunction finding that the act regulates protected speech, triggering a strict scrutiny review. Judge Freeman concluded that although California has a compelling interest in protecting the privacy and well-being of children, this interest alone is not sufficient to satisfy a strict scrutiny standard. This ruling is likely to strengthen NetChoice's opposition of similar acts, such as the Maryland Age-Appropriate Design Code Act.

Court Rejects Allegheny Health Network's Attempt to Force Arbitration over Meta Pixel Tracking:The U.S. District Court for the Western District of Pennsylvania ruled that Allegheny Health Network ("AHN") cannot compel arbitration in a class action lawsuit filed by a patient under a pseudonym. The patient alleged that AHN unlawfully collected and disclosed his confidential health information to Meta Platforms. AHN initially sought to compel arbitration based on an arbitration provision within their website's Terms of Service. However, the court denied this motion, finding that the patient did not have actual or constructive notice of the arbitration agreement. The court found that the link to the AHN's Terms of Service, a "browsewrap" agreement, was not sufficiently conspicuous, as it was located at the bottom of the homepage among numerous other links and in a less visible footer on its "Find a Doctor" page. Additionally, the court found AHN failed to prove the patient had seen the specific Terms of Service containing the arbitration provision that was added to the website.

Supreme Court Declines Review of Sandhills Medical Data Breach Suit:The U.S. Supreme Court has declined to review a Fourth Circuit decision that ruled Sandhills Medical Foundation Inc. ("Sandhills Medical"), a federally funded health center, cannot use federal immunity to shield itself from a data breach lawsuit. The lawsuit was brought by Joann Ford following a data breach at Sandhills Medical. Sandhills Medical argued it was entitled to federal immunity under 42 U.S.C. § 233(a), which protects federally funded health centers from lawsuits related to the performance of medical, surgical, dental, or related functions. The Fourth Circuit, however, interpreted "related functions" narrowly, stating it did not cover data protection. Sandhills Medical, in its petition to the

Supreme Court, contended that this ruling created a circuit split with the Ninth and Second Circuits, which have taken a broader view of the immunity. Sandhills Medical warned that the Fourth Circuit's "unnaturally cramped" reading of the statute needed correction. Despite these arguments, the Supreme Court denied Sandhills Medical's petition, meaning the health center will now face the lawsuit in South Carolina District Court.

Utah Attorney General Seeks Reinstatement of Utah Minor Protection in Social Media Act: Utah has requested a federal appeals court to reinstate a law that imposes restrictions on social media platforms. The Utah Minor Protection in Social Media Act (the "Act"), passed in 2024, was previously blocked by a lower court. The act aims to protect minors from harmful content and requires social media companies to verify the age of users and obtain parental consent for minors. Utah's Attorney General argues that the law is necessary to safeguard children from online dangers and prevent exploitation. Previously, tech industry group NetChoice successfully sued to block the law, arguing it infringes on First Amendment rights and imposes undue burdens on businesses.

Court Holds Sharing of IP Address Insufficient to Prove Harm in CIPA Case: Judge Edgardo Ramos of the Southern District of New York granted defendant Insider, Inc.'s ("Insider") motion to dismiss claims that its use of Audiencerate's website analytics tools constituted an unlawful 'pen register' in violation of California's Invasion of Privacy Act ("CIPA"). Plaintiffs argued that Insider invaded their privacy when it installed a tracker on their browsers, sending their IP addresses to a third party, Audiencerate, without their consent. However, Judge Ramos found that this collection and disclosure of IP addresses was insufficient to establish harm for purposes of Article III standing. He found that unlike a Facebook ID, which can be used to track or identify specific individuals, an IP address cannot be used to identify an individual and can only provide geographic information "as granular as a zip code." Therefore, disclosure of an IP address would not be highly offensive to a reasonable person. Judge Ramos further emphasized that this "conclusion is consistent with the general understanding that in the Fourth Amendment context a person has no reasonable expectation of privacy in an IP address." Despite this ruling, CIPA class actions and demands are likely to remain a constant threat to business with California-facing websites.

Periodical Publisher Unable to Dismiss VPPA Class Action: Judge Lewis J. Liman of the Southern District of New York denied defendant Springer Nature America's ("Nature") motion to dismiss claims that its use of Meta Pixel violated the Video Privacy Protection Act ("VPPA"). The VPPA prohibits videotape service providers from knowingly disclosing personally identifiable information about their renters, purchasers, or subscribers. Despite being drafted to address information collected through physical video stores, the VPPA has become a potent tool in the hands of the plaintiffs' bar to challenge websites containing video content. Although Nature is primarily a research journal publication, Judge Lewis found that it could qualify as a videotape service provider as defined under the VPPA in part because of the video content on its website and its subscription-based business model. Relying on the recent Second Circuit decision in *Salazar v. National Basketball Association*, Judge Liman also found that the plaintiff had alleged a concrete injury sufficient to confer standing because the disclosure of information about videos viewed was adequately similar to the public disclosure of private facts. This ruling should remind companies whose websites contain significant video content to carefully review their cookie usage and consent management capabilities.

U.S. ENFORCEMENT

CPPA Requires Data Broker to Shut Down: As part of its public investigative sweep of data broker registration compliance, the CPPA reached a settlement agreement with Background Alert, Inc.

("Background Alert") for failing to register and pay an annual fee as required by California's Delete Act. The Delete Act requires data brokers to register and pay an annual fee that funds the California Data Broker Registry. As part of the settlement, Background Alert must shut down its operations for three years for failing to register between February 1 and October 8, 2024. If Background Alert violates any term of the settlement, including the requirement to shut down its operations, it must pay a $50,000 fine to the CPPA.

New York Attorney General Settles with App Developer for Failure to Protect Students' Privacy: The New York Attorney General settled with Saturn Technologies, the developer of the Saturn app, for failing to protect students' privacy. Saturn allows high school students to create a personal calendar, interact with other users, share social media accounts, and know where other users are located based on their calendars. The New York Attorney General's investigation found that unlike what Saturn Technologies represented, the company failed to verify users' school email and age to ensure only high school students from the same high school interacted. The investigation also found that Saturn Technologies used copies of users' contact books even when the user changed their phone settings to deny Saturn's access to their contact book. Under the settlement, Saturn Technologies must pay $650,000 in penalties and change its verification process, provide enhanced privacy options for students under 18, and prompt users under 18 to review their privacy settings every six months.

New York Attorney General Sues Insurance Companies for Back-to-Back Data Breaches: The New York Attorney General sued insurance companies National General and Allstate Insurance Company for back-to-back data breaches, which exposed the driver's license numbers of more than 165,000 New Yorkers. In 2020, attackers took advantage of a flaw on two of National General's auto insurance quoting websites, which displayed consumers' full driver's license numbers in plain text. The complaint alleges that National General failed to detect the breach for two months and failed to notify consumers and the appropriate state agencies. The complaint also alleges that National General continued to leave driver's license numbers exposed on a different quoting website for independent insurance agents, resulting in another data breach in 2021. This action is the New York Attorney General's latest effort to hold auto insurance companies accountable for failing to protect consumers' personal information against an industry-wide campaign by attackers targeting online auto insurance quoting applications.

California Attorney General Announces Investigative Sweep of Location Data Industry: The California Attorney General announced an ongoing investigative sweep into the location data industry. The California Attorney General sent letters to advertising networks, mobile app providers, and data brokers that appear to be in violation of the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"). The enforcement sweep is intended to ensure that businesses comply with their obligations under the CCPA with respect to consumers' rights to opt out of the sale and sharing of personal information and limit the use of sensitive personal information, which includes precise geolocation data. The letters sent by the California Attorney General notify recipients of potential violations of the CCPA and request additional information regarding how the recipients offer and effectuate such CCPA rights. Location data has become an enforcement priority for the California Attorney General given the federal landscape affecting California's immigrant communities and reproductive and gender-affirming healthcare.

CPPA Settles with Auto Manufacturer for CCPA Violations: The CPPA settled with American Honda Motor Co. ("Honda") for its alleged CCPA violations. The CPPA alleged that Honda (1) required consumers to verify themselves and provide excessive personal information to exercise their rights to opt out and limit; (2) used an online privacy management tool that failed to offer consumers

their CCPA rights in a symmetrical way; (3) made it difficult for consumers to authorize agents to exercise their CCPA rights on their behalf; and (4) shared personal information with ad tech companies without contracts containing CCPA-required language. As part of the settlement, Honda must pay $632,500, implement new and simpler methods for submitting CCPA requests, and consult a user experience designer to evaluate its methods, train its employees, and ensure the requisite contracts are in place with third parties with whom it shares personal information. This action is a part of the CPPA's investigative sweep of connected vehicle manufacturers and related technologies.

OCR Settles with Healthcare Provider for HIPAA Violations: The U.S. Department of Health and Human Services Office for Civil Rights ("OCR") settled with Oregon Health & Science University ("OHSU") over potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule's right of access provisions. The HIPAA Privacy Rule requires covered entities to provide individuals or their personal representatives access to their protected health information within thirty days of a request (with the possibility of a 30-day extension) for a reasonable, cost-based fee. OCR initiated an investigation against OHSU for a second complaint OCR received in January 2021 from the individual's personal representative. OCR resolved the first complaint in September 2020, when OCR notified OHSU of its potential noncompliance with the Privacy Rule for only providing part of the requested records. However, OHSU did not provide all of the requested records until August 2021. As part of the settlement, OHSU must pay $200,000 in penalties.

Democratic FTC Commissioners Fired by Trump Administration: The Trump administration fired the Federal Trade Commission's ("FTC") Democratic Commissioners Alvaro Bedoya and Rebecca Kelly Slaughter. Their removal leaves the FTC with no minority party representation among the agency's five commissioner bench. Slaughter was originally nominated by Trump in 2018 and was serving her second term. Bedoya was in his first term as commissioner. Bedoya and Slaughter indicated in public statements that they would take legal action to challenge the firings. Among potential privacy impacts of the firings is how the lack of minority party representation may affect the enforcement of the EU-U.S. Data Privacy Framework ("DPF"), which is used by many businesses to legally transfer personal data from the EU to the United States. The DPF is intended to be an independent data transfer mechanism, and the removal may heighten concerns about the independence of agencies tasked with enforcing the DPF. The move at the FTC follows the prior removal of democrats from the U.S. Privacy and Civil Liberties Oversight Board, which is charged with providing oversight of the redress mechanism for non-U.S. citizens under the DPF.

CFPB Drops Suit Against TransUnion: The Consumer Financial Protection Bureau ("CFPB") voluntarily dismissed with prejudice its lawsuit against TransUnion in which it alleged that TransUnion engaged in deceptive marketing practices in violation of a 2017 consent order. The CFPB provided no explanation for its decision and each party agreed to bear its own litigation costs and attorneys' fees.

INTERNATIONAL LAWS & REGULATIONS

CJEU Rules Data Subject Is Entitled to Explanation of Automated Decision Making: The Court of Justice of the European Union ("CJEU") ruled that a controller must describe the procedure and principles applied in any automated decision-making technology in a way that the data subject can understand what personal data was used, and how it was used, in the automated decision making. The ruling stemmed from an Austrian case where a mobile telephone operator refused to allow a customer to conclude a contract on the ground that her credit standing was insufficient. The operator relied on an assessment of the customer's credit standing carried out by automated means by Dun & Bradstreet Austria. The court also stated that the mere communication of an algorithm does not

constitute a sufficiently concise and intelligible explanation. In order to meet the requirements of transparency and intelligibility, it may be appropriate to inform the data subject of the extent to which a variation in the personal data would have led to a different result. Companies will have to be creative in assessing what information is required to ensure the explainability of automated decision-making to data subjects.

European Parliament Publishes Report on Potential Conflicts Between GDPR and EU AI Act: The European Parliament published a report on the interplay of the EU AI Act with the EU General Data Protection Regulation ("GDPR"). One of the AI Act's main objectives is to mitigate discrimination and bias in the development, deployment, and use of "high-risk AI systems." To achieve this, the EU AI Act allows "special categories of personal data" to be processed, based on a set of conditions (*e.g.*, privacy-preserving measures) designed to identify and to avoid discrimination that might occur when using such new technology. The report concludes that the GDPR, which imposes limits on the processing of special categories of personal data, might prove restrictive in the circumstances under which the GDPR allows the processing of special categories of personal data. The paper recommends that GDPR reforms of further guidelines on how the GDPR works with the EU AI Act would help address any conflicts.

Norwegian and Swedish Data Protection Authorities Release FAQs on Personal Data Transfers to United States: The Norwegian and Swedish data protection authorities issued FAQs on Personal Data Transfers to the United States in response to the dismissal of several members of the U.S. Privacy and Civil Liberties Oversight Board ("PCLOB"). The PCLOB is responsible for providing oversight of the redress mechanism for non-U.S. citizens under the U.S.-EU Data Protection Framework ("DPF"), which is one legal mechanism available to transfer EU personal data to the U.S. under the GDPR. Datatilsynet, the Norwegian data protection authority, stated that it understands that the intent is to appoint new PCLOB members in the future and that, even without a quorum, the PCLOB can perform some tasks related to the DPF. Accordingly, Datatilsynet stated that issues would only arise in the adequacy decision underpinning the DPF as a result of the removal of the PCLOB members if the appointment of new members takes a long time. The Swedish data protection authority, Integritetsskydds myndigheten ("IMY") also cited confusion of the European business community following the dismissal of several members of the PCLOB. The IMY stated that the Court of Justice of the European Union has the authority to annul the DPF adequacy decision but has not taken such action. As a result, the DPF is still a valid mechanism for data transfer according to the IMY. Both data protection authorities indicated they would continue to monitor the situation in the U.S. to determine if anything occurred that affected the DPF and its underlying adequacy decision.

OECD Releases Common Reporting Framework for AI Incidents: The OECD Organization for Economic Co-operation and Development ("OECD") released a paper titled "Towards a Common Reporting Framework for AI Incidents." The paper outlines the need for a standardized approach to reporting AI-related incidents. It emphasizes the importance of transparency and accountability in AI systems to ensure public trust and safety. The report proposes a framework that includes guidelines for identifying, documenting, and reporting incidents involving AI technologies. The paper specifically identifies 88 potential criteria for a common AI incident reporting framework across 8 dimensions. The 8 dimensions are (1) incident metadata, such as date of occurrence, title, and description of the incident; (2) harm details focusing on severity, type, and impact; (3) people and planet, describing impacted stakeholders and associated AI principles; (4) economic context describing the economic sectors where the AI was deployed; (5) data and input, which includes a description of the inputs selected to train the AI system; (6) AI model providing information related to the model type; (7) task and output, describing the AI system tasks, automation level, and outputs; and (8) other information

about the incident to catch any complementary information reported with respect to an incident.

China Issues Draft Measures for Financial Institutions to Report Cybersecurity Incidents and for Data Compliance Audits: The People's Bank of China ("PBOC") released draft administrative measures for reporting cybersecurity incidents in the financial sector ("Draft Measures"). The Draft Measures provide guidelines for identifying, reporting, and managing cybersecurity incidents by financial institutions regulated by the PBOC. Reporting requirements and timing vary according to type of entity and classification of incidents. Incidents would be classified as one of four categories – especially significant, significant, large, and average. Separately, the Cyberspace Administration of China ("CAC") issued administrative measures on data protection audit requirements ("Data Protection Audit Measures"). The Data Protection Audit Measures provide (1) the conditions under which an audit of a data handler's compliance with relevant personal information protection legal requirements would be required; (2) selection of third-party compliance auditors; (3) frequency of compliance audits; and (4) obligations of data handlers and third-party auditors in conducting compliance audits. The Data Protection Audit Measures include guidelines setting forth the specific factors that data handlers must evaluate in an audit, including the legal basis for processing personal information, whether the data handler has complied with notice obligations, how personal information is transferred outside of China, and the technical security measures employed by the data handler to protect personal information, among other factors.

European Commission Releases Third Draft of General-Purpose AI Code of Practice: The European Commission announced the publication of the third draft of the EU General-Purpose AI Code ("Code"). The first two sections of the draft Code detail transparency and copyright obligations for all providers of general-purpose AI models, with notable exemptions from the transparency obligations for providers of certain open-source models in line with the AI Act. The third section of the Code is only relevant for a small number of providers of most advanced general-purpose AI models that could pose systemic risks, in accordance with the classification criteria in Article 51 of the AI Act. In the third section, the Code outlines measures for systemic risk assessment and mitigation, including model evaluations, incident reporting, and cybersecurity obligations. A final version of the General-Purpose AI Code of Practice is due to be presented and published to the European Commission in May.

Additional Authors: Daniel R. Saeedi, Rachel L. Schaller, Gabrielle N. Ganze, Ana Tagvoryan, P. Gavin Eastgate, Timothy W. Dickens, Jason C. Hirsch, Adam J. Landy, Amanda M. Noonan and Karen H. Shin.

National Law Review, Volume XV, Number 93