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

The BR Privacy & Security Download: June 2024

Article By:

Sharon R. Klein

Philip N. Yannella

Alex C. Nisenbaum

Harrison Brown

Jennifer J. Daniels

Jeffrey N. Rosenthal

Welcome to this month's issue of *The BR Privacy & Security Download*, the digital newsletter of Blank Rome's Privacy, Security & Data Protection practice.

STATE & LOCAL LAWS & REGULATION

Colorado Enacts AI Act

Colorado has become the first State to enact comprehensive AI legislation, SB 24-205 (the "Colorado AI Act"). Unlike Colorado's comprehensive privacy law, the Colorado AI Act applies to all "developers" and "deployers" of "high-risk artificial intelligence systems" that do business in Colorado without any other applicability thresholds. It also applies to the use of high-risk artificial intelligence systems affecting all Colorado residents ("consumers"), including employees. The Colorado AI Act follows several principles of the EU AI Act, including transparency, preventing "algorithmic discrimination," and imposing differing obligations for developers and deployers. Violations of the Colorado AI Act constitute an unfair trade practice under state law. However, the Colorado AI Act does not provide for a private right of action, and the Colorado Attorney General has exclusive enforcement authority. The Colorado Attorney General also has the authority to promulgate rules as necessary for implementing and enforcing the Colorado AI Act. The Colorado AI Act will take effect on February 1, 2026. For an in-depth review of the Colorado AI Act and its requirements, please see Blank Rome's Client Alert.

Illinois Legislature Passes BIPA Amendment Overturning Accrual Liability

The Illinois Legislature approved Senate Bill 2979 ("S.B. 2979") to amend the Biometric Information

Privacy Act (“BIPA”). SB 2979 would limit the extent of potential civil penalties awarded under BIPA by clarifying that multiple collections of a person’s biometric identifier or biometric information using the same method of collection is considered a single violation of BIPA. Once signed, S.B. 2979 will overturn the Illinois Supreme Court’s interpretation of accrual of damages under BIPA in *Cothron v. White Castle Sys., Inc.*, which held that separate BIPA claims accrued with each scan or transmission. SB 2979 further provides that BIPA’s “written release” requirement may be met by an electronic signature.

Maryland Passes Comprehensive Data Privacy Legislation

Maryland joined the list of states that have adopted comprehensive privacy laws with the passage of the Maryland Online Data Privacy Act of 2024 (“MODPA”). MODPA applies to persons that conduct business in Maryland or provide products or services that are targeted to Maryland residents and, during the preceding calendar year, either controlled or processed the personal data of at least: (1) 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) 10,000 consumers and derived more than 20 percent of its gross revenue from the sale of personal data. MODPA does not contain exemptions for nonprofits or institutions of higher education. Protected Health Information (“PHI”) under the Health Insurance Portability and Accountability Act (“HIPAA”) is exempted, but there is no exemption for entities subject to HIPAA. MODPA provides for consumer data rights and requires controllers to provide an appropriate notice describing data processing activities. MODPA also requires data protection assessments in certain circumstances, restricts the processing and sale of the personal data of minors, prohibits the sale of sensitive data, and requires heightened data minimization requirements for sensitive personal data. MODPA will be enforced by the Maryland Attorney General. MODPA takes effect on October 1, 2025, but requirements relating to personal data processing will apply starting on April 1, 2026. For more information, please see Blank Rome’s client alert addressing the full implications of MODPA.

Minnesota Passes Comprehensive Data Privacy Law

Minnesota became the 19th state to pass a comprehensive privacy bill by passing the Minnesota Consumer Data Privacy Act (“MCDPA”). The MCDPA significantly complicates the state privacy law patchwork by adding a number of significant obligations not required under existing US state privacy laws, including the requirement to maintain data inventories and designate a Chief Privacy Officer or other individual designated to handle consumer data protection. The MCDPA also provides for new consumer rights, allowing consumers to challenge and obtain additional information about the profiling of their personal information. The law is scheduled to become effective July 31, 2025, and will be enforced by the Minnesota Attorney General.

Vermont Legislature Passes Comprehensive Data Privacy Law

The Vermont Legislature passed H.121, the Vermont Data Privacy Act (“VDPA”). If signed by the governor of Vermont, the VDPA would apply to businesses that process the personal data of at least 25,000 consumers (lowering to 12,500 consumers by July 1, 2026, and 6,250 consumers by July 1, 2027) or process the personal data of at least 12,500 (lowering to 6,250 consumers by July 1, 2026, and lowering to 3,125 by July 1, 2027) and derive more than 25 percent of gross revenue from the sale of personal data. The law also contains other notable obligations on businesses operating in Vermont, including bans on selling sensitive data and consent requirements for processing sensitive data. The VDPA also creates a private right of action for consumers harmed by a data broker or larger data holders’ processing of sensitive data without consent, processing of sensitive data of a

known child in a manner that does not comply with the Children's Online Privacy Protection Act, the sale of sensitive data, and violation of confidential obligations relating to consumer health data.

Colorado Privacy Act Amended to Add Heightened Protections for Children's Data

Colorado has enacted S.B. 24-041 (the "Bill"), which amends the Colorado Privacy Act ("CPA") to add enhanced protections when processing the data of minors (i.e., any Colorado consumer under the age of 18). The Bill has a broader scope than the CPA and has no revenue or processing threshold requirements. The Bill requires controllers that offer any online service, product, or feature to a Colorado consumer whom the controller actually knows or willfully disregards is a minor ("Covered Controllers") to use reasonable care to avoid and prepare data protection assessments where there is, a heightened risk of harm to minors. The Bill also requires consent when Covered Controllers: (1) process minors' personal data for the purpose of targeted advertising, sale, or profiling; (2) use any feature to significantly increase, sustain, or extend a minor's use of the Covered Controller's online service; or (3) collect minors' precise geolocation, except in certain instances. The Bill will be effective October 1, 2025.

Maryland Passes Age Appropriate Design Law

The Maryland General Assembly passed Senate Bill 571, also known as the Maryland Kids Code. The Maryland Kids Code follows in the footsteps of the embattled California Age Appropriate Design Code Act, requiring companies that maintain websites or offer online services "reasonably likely to be accessed by children" to conduct risk assessments and implement default privacy settings designed to protect the personal information of children. The Code defines children as consumers under the age of eighteen (18), significantly older than the "under thirteen" (13) standard under federal law. This "reasonably likely" standard paired with the broad definition of "child" means that this law would likely have significant impacts on a broad range of general-purpose websites not typically subject to children's privacy laws, significantly restricting the types of trackers permissible on these websites. The Maryland Kids Code is certain to face constitutional challenges from a broad range of industry groups, including those that won a preliminary injunction of the California Age Appropriate Design Code Act.

California and Other States' Attorneys General Write to Congress Opposing Preemption in Proposed Federal Comprehensive Privacy Bill

The California Attorney General along with 14 other states' attorneys general have written a letter to Congress urging Congress to remove preemption language in the current draft of the American Privacy Rights Act ("APRA"), a proposed federal comprehensive privacy bill. In the letter, the attorneys general highlight the importance of current and future state privacy protections and ask that any federal privacy framework leave room for states to legislate responsively to changes in technology and data collection practices. The attorneys general argue that the states are better equipped to adjust to the challenges presented by technological innovation. The attorneys general state that the federal comprehensive privacy law should act as a "baseline" and allow states to provide additional protections.

Oregon Attorney General Releases FAQs on Privacy Law

The Oregon Attorney General released on its website FAQs for businesses and consumers on Oregon's comprehensive privacy law, the Oregon Consumer Privacy Act ("OCPA"). The FAQs for businesses focus on compliance obligations (*e.g.*, whether

consent is required to process personal data, how long controllers have to respond to rights requests, and what the penalties are for noncompliance), while the FAQs for consumers focus on the rights afforded to them under the OCPA. The OCPA takes effect on July 1, 2024.

NYDFS Releases Cybersecurity Program Template

The New York Department of Financial Services ("NYDFS") published a Template Cybersecurity Program to help individual licensees and individually owned affiliates comply with the New York Cybersecurity Regulations part 500. The Template is intended to assist individual licensees and affiliates that: have fewer than 20 employees and independent contractors; that have less than $7,500,000 in gross annual revenue in each of the last three fiscal years; or that have less than $15,000,000 in year-end total assets, including assets of all affiliates. The template contains a broad range of instructions for developing a comprehensive program, including instructions for conducting risk assessments, monitoring third-party service providers, and managing access privileges for covered information. Although the Template is only designed for compliance with New York law, it may also serve as a useful starting point for companies seeking to develop or understand industry-standard cybersecurity programs.

FEDERAL LAWS & REGULATION

SEC Publishes Guidance on Cyber Incident Disclosures

The U.S. Securities and Exchange Commission ("SEC") Director of the Division of Corporation Finance, Erik Gerding, published guidance reminding companies of their obligations under the SEC's 2023 cybersecurity rules. Under the cybersecurity rules, public companies are required to disclose material cybersecurity incidents under Item 1.05 of Form 8-K. Companies may alternatively report cybersecurity incidents that they have either determined not to be material or about which they have not made a materiality determination through Form 8-K Item 8.01. When an incident that was originally reported through Item 8.01 is later determined to be material, it must be reported again through a separate form 8-K within four business days of such determination. Gerding also re-emphasized that materiality determinations should consider qualitative factors beyond mere impact on financial condition or operations, such as the impact of the incident on the company's reputation, customer or vendor relationships, and competitiveness. Companies should also consider risks associated with litigation and regulatory investigation.

Senators Call on FTC to Investigate Automakers; FTC Issues Warning to Automakers

Senators Ron Wyden and Edward Markey issued a letter to the Federal Trade Commission ("FTC") Commissioner Lina Khan requesting that the FTC investigate major automakers' sharing of geolocation data in response to law enforcement requests. The letter follows an inquiry by Senator Wyden's office, which asked the association representing automakers how their members respond to law enforcement requests for location information collected from vehicles. The letter alleges that several auto manufacturers do not require a warrant or court order to provide geolocation information to law enforcement as required by their pledge under the Consumer Privacy Protection Principles of the Alliance of Automobile Manufacturers and the Association of Global Automakers. Two weeks later, the FTC released a post to its Technology Blog reminding car manufacturers, and all businesses, that the FTC will take action to protect consumers against unfair and deceptive practices with respect to the collection, use, and sharing of data, particularly sensitive personal data such as geolocation and biometric data.

Federal Trade Commission ("FTC") Releases Guidance on Breach Reporting under Safeguards Rule

The FTC has released guidance on reporting security breaches under the Gramm-Leach Bliley Act's Safeguards Rule ("Safeguards Rule"). The guidance highlights that under the Safeguards Rule, financial institutions must notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach involving the information of at least 500 consumers. The Safeguards Rule defines a security breach that triggers notification obligations as "an acquisition of unencrypted customer information without the authorization of the individual to which the information pertains." The guidance notes that unauthorized acquisition is presumed to include unauthorized access to unencrypted customer information unless there is reliable evidence that there has not been, or could not reasonably have been, unauthorized acquisition of such information. The guidance also provides the link to an online form that should be used to provide notice of a security breach to the FTC.

NIST Releases Generative AI Profile for Artificial Intelligence Risk Management Framework

NIST released a draft publication based on the AI Risk Management Framework ("AI RMF") to help manage the risk of Generative AI. The draft AI RMF Generative AI Profile can help organizations identify unique risks posed by generative AI and proposes actions for generative AI risk management that best aligns with their goals and priorities. The AI Profile guidance document centers on a list of 12 risks and actions that developers can take to manage them.

NIST Releases Final Version of Revised Guidelines for Sensitive Information

NIST finalized a third revision to NIST Special Publication 800-171 ("SP 800-171"). SP 800-171 was initially issued in 2015 and provides security guidelines for protecting the confidentiality of federally controlled unclassified information being stored or processed outside the government. The revisions intend to bring SP 800-171 in line with NIST's "source catalog" of security and privacy controls and give organizations who do business with the government clearer guidance for protecting sensitive data they handle. The revisions also allow the use of organization-defined parameters, which are intended to give agencies and non-federal organizations more flexibility to implement certain security requirements. NIST stated that it plans to also revise NIST Special Publication 800-172, which provides a more stringent set of security requirements for important or sensitive controlled unclassified information.

SEC Adopts Amendments to Regulation S-P

The SEC announced the adoption of amendments to Regulation S-P to modernize and enhance the rules governing the treatment of consumers' nonpublic information by certain financial institutions. The amendments to Regulation S-P update the rules' requirements for broker-dealers, investment companies, registered investment advisers, and transfer agents (collectively, "covered institutions") to address the expanded use of technology and corresponding risks that have emerged since Regulation S-P was adopted in 2000. The amendments will require covered institutions to develop, implement, and maintain written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The amendments will become effective 60 days after publication in the Federal Register.

CISA Issues Secure by Design Pledge

The American Cybersecurity and Infrastructure Security Agency ("CISA") has implemented a Voluntary Pledge designed to improve the security of enterprise software products and services. Participating companies pledge to make a good-faith effort to work towards the program's seven goals, including Multi-Factor Authentication, reduction of default passwords, reducing vulnerabilities, security patching, and the implementation of policies for disclosing vulnerabilities. The pledge is not legally binding and participating companies are encouraged to provide reports on their progress as well as the challenges they face in reaching the program's goals.

U.S. LITIGATION

Blackbaud Avoids Plaintiffs' Class Certification in Data Breach Case

The U.S. District Court for the District of South Carolina has denied a motion to certify several proposed classes consisting of approximately 1.5 billion individuals in the case against Blackbaud, Inc. ("Blackbaud") for a ransomware attack the company suffered in February 2020. The district court held that that the plaintiffs had failed to show ascertainability, which requires that a court be able to readily identify class members and that there be an administratively feasible way for the court to determine whether a particular individual is a class member. The plaintiffs argued that members of their proposed classes and subclasses could be ascertained in several ways, including through restoring Blackbaud's customer database files and conducting a search using information provided by that putative class member. However, the court held that this method was unreliable and unhelpful to the court. Blank Rome represented Blackbaud in its recent settlements with the attorneys general of 49 states and the District of Columbia.

Hospital Unable to Shake Federal Wiretapping Claims Relating Meta Pixel

A U.S. District Court rejected the University of Chicago Medical Center's ("UCMC") motion to dismiss repleaded claims for violations of the Electronic Communications Privacy Act ("ECPA") in *Hartley v. University of Chicago Medical Center et al.*, a putative class action filed against UCMC and Meta Platforms, Inc. ("Meta") in the Northern District of Illinois. The second amended complaint alleges that UCMC, which operates a non-profit hospital network and website, unlawfully "sells" UCMC patients' communications and individually identifiable health information ("IIHI") collected through UCMC's patient portal by disclosing such information to Meta and using Meta's collection tools on UCMC's website for targeted advertising purposes without patients' knowledge or consent. The Court found it "plausible" that UCMC could have acquired patients' IIHI "with the purpose of disclosing it to Meta for their mutual financial benefits," thereby allowing the plaintiff to seek monetary damages against UCMC for the greater of actual damages or unlawfully gained profits.

Court Approves $62 Million Dollar Location Tracking Settlement

A California U.S. District Court granted final approval to Google's $62 million settlement to resolve allegations that it illegally collected and stored smartphone users' private location information. The case involved six related proposed class actions, which were consolidated in 2018. In total, Judge Davila certified a class of 247.7 million consumers who used one or more mobile devices and whose information was stored by Google while their location history was disabled. The deal awards $18 million to the lawyers representing the consolidated class and $42 million to various advocacy groups through a cypres fund. The fund will help support these groups to provide education, advocacy, and security against similar privacy violations in the future. The deal also requires Google to disclose

details of its location-information storage, allowing users to have more control over their data.

U.S. ENFORCEMENT

SEC Announces Enforcement Action for Failure to Timely Notify of Cyber Attack

The SEC announced that the Intercontinental Exchange, Inc. ("ICE") —parent to the New York Stock Exchange—agreed to pay a $10 million penalty to settle charges that it caused its nine wholly-owned subsidiaries to fail to timely notify the SEC of a cyber intrusion as required by Regulation Systems Compliance and Integrity ("Regulation SCI"). In April 2021, ICE learned of a potential system intrusion due to a vulnerability in their VPN. Upon investigation, ICE determined that a threat actor had successfully deployed malicious code to access ICE's corporate network. However, ICE failed to notify the legal and compliance officials at ICE's subsidiaries of the intrusion for several days in direct violation of its own internal incident response procedures. As a result, its subsidiaries were not able to fully assess the intrusion to fulfill their independent regulatory disclosure obligations, which required them to immediately notify the SEC within twenty-four hours of the incident.

Telecommunications Company Appeals FCC Fine for Selling Customer Location Data

AT&T is appealing a $57 million fine from the Federal Communications Commission ("FCC") for failing to protect consumer location data. The FCC fine was part of a nationwide sanction against top wireless carriers in April 2024. In addition to AT&T, Verizon was fined nearly $47 million, Sprint was fined $12 million, and T-Mobile was ordered to pay $80 million. The FCC's decision was part of a years-long investigation into whether wireless carrier companies sold location data to third parties. According to the FCC, these companies failed to implement reasonable measures protecting against unauthorized location data access from third parties in violation of Section 222 of the Communications Act. In its appeal, AT&T alleges that the FCC's order is arbitrary, capricious, and contrary to the law. AT&T further argues that the location data at issue is not "customer proprietary network information" as it's defined in the Communications Act. While AT&T is the first carrier to appeal the FCC's order, Verizon and T-Mobile have both stated that they would appeal the order as well.

INTERNATIONAL LAWS & REGULATION

GDPR Complaint Filed over AI Hallucination

NOYB – European Center for Digital Rights ("NOYB") filed a complaint against Open AI LLC ("Open AI"), alleging that Open AI's operation of its popular AI chatbot, ChatGPT, violates the European Union General Data Protection Regulation ("GDPR"). Among other things, parties subject to the GDPR must ensure that personal data processed and displayed is accurate, and the individuals who are the subjects of such information may request access to their personal data and related processing, as well as rectification or erasure of incorrect personal data. NOYB alleges that Open AI is incapable of preventing ChatGPT's systems from displaying specific pieces of personal data (including false information), did not adequately respond to an individual's request to access specific information about data processed by ChatGPT, and failed to respond to the individual's request to rectify or delete false personal data generated and displayed by ChatGPT. The complaint requests an investigation by the Austrian Data protection Authority into ChatGPT's "hallucinations" of false information generated about real individuals and Open AI's capabilities and data practices.

Dutch Data Protection Authority Issues Guidance Stating That Scraping Personal Data from

the Internet Almost Never Compliant with GDPR

The Dutch Data Protection Authority, the Autoriteit Personnsgevens (“AP”), issued guidance stating that automated collection and storage of personal data from the internet, a process called scraping, will almost always be a violation of the GDPR. The guidance states that the fact that personal data is publicly available on the Internet does not mean that consent has been provided to process that data by scraping. Consent can only be given if a request is made in advance of the processing, which is generally not possible with scaping. The guidance goes on to explain that, in practice, processing through scraping would generally be possible only on the basis of legitimate interest. The AP stated that the basis is subject to strict conditions and that it would almost never be possible to meet those conditions when scraping. The guidance did illustrate “exceptional” cases in which scraping may be allowed, including when an organization scrapes the websites of news media in order to get news about its own company or in the case of the strictly domestic use of private individuals.

European Council Announces Data Transfer Framework with Japan

The European Council (“Council”) announced it had concluded an agreement that included protocols for cross-border data flows between the EU and Japan. The Council stated that the protocols will ensure removal of unjustified data localization requirements and enable companies to handle data efficiently without cumbersome administrative or storage requirements and provide them with a predictable legal framework.

National Law Review, Volume XIV, Number 158