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

The BR Privacy & Security Download: October 2023

Article By:

Sharon R. Klein

Alex C. Nisenbaum

Jennifer J. Daniels

Jeffrey N. Rosenthal

Harrison Brown

Karen H. Shin

STATE & LOCAL LAWS & REGULATIONS

California Passes New Data Broker Law

The California legislature passed the Delete Act, imposing new requirements on data brokers. California law currently requires data brokers to register with the California Attorney General and provide certain information about how consumers may exercise certain rights and find out more information on the data broker's data collection practices. The California Privacy Rights Act ("CPRA") further requires businesses, including data brokers, to delete information collected directly from a consumer in response to a consumer request, but not information collected from other sources. The Delete Act would expand data broker obligations by requiring data brokers to register with the California Privacy Protection Agency ("CPPA"), delete all personal information related to a consumer who has made a delete request, continue to delete any new information received about that consumer every 45 days, report specific information on data collection and

consumer request metrics, and undergo independent compliance audits every three years. The Delete Act charges the CPPA with creating an accessible deletion mechanism by January 1, 2026, that allows consumers to request every data broker to delete personal information through a single verifiable request. The Delete Act's registration and reporting requirements would take effect in 2024. CPPA portal submission and audit requirements would take effect in 2026 and 2028, respectively. Entities subject to the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the California Insurance Code are exempted from the new law.

California Governor Signs Executive Order on Artificial Intelligence

California Governor Gavin Newsom has signed an executive order to develop a process for evaluation and deployment of artificial intelligence ("AI") technology within the state government. The executive order directs state agencies and departments to perform a joint risk analysis of potential threats to and vulnerabilities of California's critical energy infrastructure from generative AI and to develop a report examining the most significant and beneficial uses of generative AI. The executive order also requires state agencies and departments to issue general guidelines for public sector procurement, uses, and required training for generative AI; provide training for state government workers; evaluate the impact of generative AI on the state government workforce; develop guidelines to analyze the impact that adopting generative AI tools may have on vulnerable communities; and partner with educational institutions and legislative partners to consider and evaluate the impacts of generative AI on California and provide policy recommendations.

Delaware Passes Comprehensive Privacy Law

Delaware has become the twelfth state to pass a comprehensive privacy law. The Delaware Personal Data Privacy Act ("DPDPA") notably has a much lower applicability threshold than those of the other state laws and, like Colorado's and Oregon's laws, does not wholly exempt non-profits. The DPDPA also does not provide entity-level exemptions for covered entities or business associates governed by the

Health Insurance Portability and Accountability Act ("HIPAA"). However, similar to the other state comprehensive laws, the DPDPA provides Delaware consumers the rights to know, access, delete, and correct personal data and opt out of the processing of personal data for purposes of targeted advertising, sale, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. The DPDPA further requires opt-in consent for the processing of sensitive data. The DPDPA is effective on January 1, 2025, and provides a 60-day cure period that sunsets on December 31, 2025.

Federal Judge Blocks the California Age-Appropriate Design Code

The U.S. District Court for the Northern District of California granted a request for preliminary injunction, halting enforcement of the California Age-Appropriate Design Code ("CA AADC"). The CA AADC, modeled after the U.K. Age-Appropriate Design Code, prohibits companies providing online services, products, or features likely to be accessed by children under the age of 18 from collecting a child's personal information unless there is a compelling reason that such collection is in the child's best interest. In *NetChoice v. Bonta*, the court held that NetChoice, LLC, a trade group that includes Google Inc., Amazon.com Inc., Meta Platforms Inc., and TikTok, would likely succeed on its claim that the CA AADC violates the First Amendment, failing both strict and intermediate scrutiny. The preliminary injunction blocks the CA AADC from taking effect until the case is resolved, meaning the CA AADC may not take effect as planned on July 1, 2024.

Massachusetts Gaming Commission Approves Sports Wagering Privacy Regulations

The Massachusetts Gaming Commission (the "Commission") approved Sports Wagering Data Privacy Regulations ("Regulations"). The Regulations apply to sports wagering operators' use of "confidential information," which is defined under the Regulations as any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular patron, individual, or household, including amounts wagered and events related to the wager, unique patron ID,

username, and authentication credentials. The Regulations provide wagering patrons with certain rights regarding their confidential information, including the right to request a description of how their confidential information is being used, to access a copy of their confidential information, to restrict processing, and to request deletion. The Regulations also impose a number of requirements on sports wagering operators, including requirements to develop, implement, and maintain comprehensive administrative, technical, and physical data privacy and security policies appropriate to the size and scope of the business, notify the Commission of a data breach "immediately," and restrict data use and retention and data sharing, among other things. The Regulations took effect on September 1, 2023.

FEDERAL LAWS & REGULATIONS

Consumer Financial Protection Bureau Releases Outline of Planned Rulemaking

The Consumer Financial Protection Bureau ("CFPB") released an outline of the CFPB's planned rulemaking under the Fair Credit Reporting Act ("FCRA"). The outline indicates that the CFPB is considering proposals that would result in a dramatic expansion of the FCRA, including regulation of data brokers as consumer reporting agencies if they collect and sell consumer data such as payment histories, income, and criminal records. The CFPB stated that the proposal would limit the sale of certain data broker data for advertising or marketing and prohibit the sale of data except to companies to whom the consumer applied for credit, insurance, employment, housing, or some other service, or with the consumer's consent. The CFPB's rulemaking process is expected to extend into 2025.

NIST Announces Planned Updates to HIPAA Security Rule Resource Guide

The National Institute of Standards and Technology ("NIST") announced that changes will be made to the draft NIST Special Publication (SP) 800-66 Revision 2 on Implementing the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule: A

Cybersecurity Resource Guide ("SP 800-66 Revision 2"), which was released for public comment in July 2022. These changes include (1) separately providing Appendix E and F online; and (2) clarifying the differences between the terms "risk analysis" and "risk assessment," with "risk analysis" referring to the term as used in the HIPAA Security Rule (i.e., an accurate and thorough assessment of the threats and vulnerabilities to electronic protected health information ("ePHI")), and "risk assessment" referring to the process by which a regulated entity can determine the level of risk to ePHI. Additionally, more specific resources for small, regulated entities will be provided as a separate effort from the final publication of SP 800-66 Revision 2.

ONC and HHS OCR Release Updated HIPAA Security Risk Assessment Tool

The National Coordinator for Health Information Technology ("ONC") and the U.S. Department of Health and Human Services' ("HHS") Office for Civil Rights ("OCR") released version 3.4 of the Security Risk Assessment ("SRA") Tool under the HIPAA Security Rule. The SRA Tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and is intended for medium and small providers. The latest version of the SRA Tool includes a number of new features, including a remediation report to track and record responses to vulnerabilities, a glossary and tooltips (in which you can hover over terms to receive more information), updated references to the latest edition of the Health Industry Cybersecurity Practices, and bug fixes and usability improvements.

HHS and FTC Publishes Updated Version of Consumer Health Data Privacy and Security Guide

The Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") published an updated version of their joint publication titled "Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule." This publication provides a guide to businesses on how to comply with multiple data privacy laws, including the HIPAA Privacy, Security, and Breach Notification Rules, the FTC Act, and the

FTC's Health Breach Notification Rule. The publication offers general guidance on issues, including what entities the laws and regulations cover, the measures these entities can adopt to maintain the privacy and security of consumers' health information, and the steps entities must take in the event of a breach.

Senate Committee Requested Information to Improve Health Data Privacy Laws

The U.S. Senate Committee on Health, Education, Labor, and Pensions issued a Request for Information ("RFI") to improve privacy and security protections for health data, particularly sensitive information, and to modernize the Health Insurance Portability and Accountability Act ("HIPAA") to also safeguard health data collected by new technologies, such as wearable devices and wellness apps, which are not currently protected under HIPAA. The RFI comment period closed on September 28, 2023, and included questions categorized by the following categories: general privacy considerations, health information under HIPAA, collection and sharing of health data, biometric data, genetic information, location data, financial information, artificial intelligence, state and international privacy frameworks, and enforcement. The RFI follows growing federal and state efforts to raise awareness about, and to safeguard security over, the collection, use, and disclosure of sensitive health data.

U.S. LITIGATION

New Generative AI Consumer Data Privacy Class Action Filed

OpenAI, the creator of popular generative artificial intelligence ("AI") technologies and the popular chatbot ChatGPT, and OpenAI's main investor, Microsoft Corporation ("Microsoft"), face a new proposed class action in a federal court in San Francisco, for allegedly violating federal and state privacy laws, including the federal Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the California Invasion of Privacy Act. The two unnamed plaintiffs, both of whom are software engineers and users of ChatGPT, claim that the defendants' AI products have scraped and stolen the personal information (*e.g.*,

financial information, health data, chat communications, keystrokes, etc.) of millions of consumers, including children, and used that stolen data to further develop products that the plaintiffs fear could "someday result in [their] professional obsolescence." The case is *A.T., et al. v. OpenAI LP, et al.* in the U.S. District Court for the Northern District of California, No. 3:23-cv-04557.

U.S. ENFORCEMENT

U.S. Department of Justice Settles Claims with Federal Contractor Relating to Cybersecurity Control Failure

The U.S. Department of Justice ("DOJ") announced that Verizon Business Network Services LLC ("Verizon") has settled False Claims Act allegations that it failed to completely satisfy certain cybersecurity controls in connection with an information security service provided to federal agencies. Verizon will pay $4,091,317 to resolve the allegations. Verizon provides its Managed Trusted Internet Protocol Service ("MTIPS") to federal agencies. The MTIPS is designed to provide federal agencies with secure connections to the public internet and other external networks. Verizon discovered that the MTIPS solution did not completely satisfy contractual requirements for three required cybersecurity controls for Trusted Internet Connections from 2017 to 2021. After learning of the issues, Verizon provided the government with a written self-disclosure, initiated an independent investigation and compliance review of the issues, and provided the government with multiple detailed supplemental written disclosures. The DOJ acknowledged that Verizon took several significant remedial steps and cooperated with the DOJ investigation, entitling it to credit under DOJ guidelines for taking disclosure, cooperation, and remediation into account in False Claims Act cases.

HHS Office for Civil Rights Settles Potential Violations of HIPAA with Public Health Plan

On September 11th, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") announced a settlement of potential violations of the Health Insurance Portability and Accountability

Act (“HIPAA”) with LA Care, which is the largest publicly operated health plan in the nation. The OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Security Rule”). The settlement concluded that there were multiple potential violations of the HIPAA Security Rule, including (1) a failure to conduct an accurate and thorough risk analysis; (2) a failure to implement security measures to reduce risks of electronically protected health information; and (3) a failure to implement sufficient procedures to regularly review records of information system activity. Under the settlement agreement, LA Care agreed to pay $1,300,000 and implement a corrective action plan, which identifies steps LA Care will take to resolve HIPAA Security Rule violations.

NYC-based College Agrees with NY AG to Invest $3.5 Million in Data Security Enhancements

Marymount Manhattan College (“MMC”) reached a settlement with the New York attorney general over claims that MMC’s failure to maintain adequate safeguards opened it up to a 2021 cyberattack that exposed personal data of nearly 100,000 students, faculty, and alumni. In November 2021, MMC’s security systems were breached by a hacker who gained access to Social Security numbers, medical information, and other data. The hacker subsequently encrypted the data and demanded a ransom in exchange for the return of the data. MMC paid the ransom, but the data was ultimately deleted. After an investigation, the attorney general found that MMC failed to take several steps to protect personal information, including using multifactor authentication for accounts. As part of the settlement, MMC agreed to invest $3.5 million over the next six years to better protect the personal information of students and staff.

FTC Finalizes $75,000 Settlement Order with 1Health.io

The Federal Trade Commission (“FTC”) finalized its order with 1Health.io, Inc., also d/b/a Vitagene, Inc. (collectively, “1Health.io”) to settle the June 2023 action against 1Health.io over allegations that the genetic testing company failed to secure sensitive genetic and health data collected from consumers, deceived consumers about the

company's privacy and security practices, and improperly changed its privacy policy retroactively without providing consumers with adequate notice and without obtaining their consent. Among other things, the order imposes a $75,000 fine that will be used to issue refunds to impacted consumers and requires 1Health.io to establish and maintain an information security program to address the security failures identified by the FTC's investigation.

Health System Agrees to Pay $49 Million Settlement for Illegal Disposal of Waste and Protected Patient Information

Kaiser Foundation Health Plan, Inc. and Kaiser Foundation Hospitals (collectively "Kaiser") agreed to pay $49 million as part of a settlement with California prosecutors after an undercover investigation revealed that 16 different Kaiser facilities improperly disposed of hazardous waste, medical waste, and over 10,000 paper records containing the information, including patients' protected health information, of over 7,700 patients. The waste management issues at Kaiser involved the improper disposal of fully intact paper records in unsecured trash cans, which put patients at risk of identity theft. The $49 million payment includes $37,513,000 in civil penalties and an additional $1.75 million in civil penalties if Kaiser does not spend $3.5 million at its California facilities to implement certain measures to ensure compliance with the law within five years of the entry of the final judgment.

California AG Announces $93 Million Settlement with Google over Location Data Claims

Google, LLC ("Google") has agreed to pay $93 million as part of a settlement to resolve allegations that the company deceived users about its location-privacy practices, including the collection, storage, and use of users' location data, even if those users turned "Location History" off in their settings, for consumer profiling and advertising purposes without those consumers' informed consent. In addition to the $93 million payment to the California Attorney General's Office, Google must also implement various notice and disclosure practices to protect the privacy interests of California users. The proposed settlement terms remain subject to court approval.

FTC Settles with Two Companies over Alleged FCRA Violations

The Federal Trade Commission announced a settlement with TruthFinder and Instant Checkmate over allegations that the companies had deceived consumers about whether consumers had criminal records and violated the FCRA by failing to ensure the accuracy of their consumer reports, among other things. The FTC alleged that the companies provided misleading information about consumers by stating in marketing emails that subjects of background reports had criminal records when the record was merely a traffic ticket while touting the accuracy of the information they provided. The FTC further alleged that the companies deceived consumers by providing "remove" and "flag as inaccurate" buttons that did not work as advertised. Under the proposed FTC order, the companies are required to pay a $5.8 million penalty and establish and implement a comprehensive monitoring program related to FCRA compliance, among other things.

Cybersecurity and Infrastructure Security Agency Releases K-12 Education Technology Secure by Design Pledge

The Cybersecurity and Infrastructure Security Agency ("CISA") announced a voluntary pledge for K-12 Education Technology software manufacturers to commit to the use of secure by design principles. The pledge focuses on three principles: (1) take ownership of security outcomes; (2) embrace radical transparency and accountability; and (3) lead from the top by making secure technology a key priority for company leadership. Each principle has a set of security goals, such as providing single sign-on capabilities and security audit logs to customers at no additional charge, publishing a secure-by-design software development roadmap, including an outline of how the manufacturer plans to nudge all users, including students, towards MFA, with the understanding that students may not possess a mobile device traditionally used for MFA, publishing a vulnerability disclosure policy, and publicly naming a top business leader other than the Chief Technology Officer or Chief Information Security Officer as an individual who is responsible for managing the process of integrating security as a core function of the business. As of September 30, 2023, eight companies had signed onto the pledge.

First Legal Challenge to EU-U.S. Data Protection Framework Begins

A French Member of the European Parliament, Philippe Latombe, filed two lawsuits with the European Union Court of Justice challenging the validity of the EU-U.S. Data Privacy Framework ("DPF") and seeking to annul the European Union's approval of the DPF. The DPF provides a framework for the transfer of personal data of data subjects in the European Union to companies in the United States that self-certify to adhere to the DPF. Latombe alleges that the DPF violates the European Union's Charter of Fundamental Rights due to insufficient guarantees of respect for private and family life with regard to bulk collection of personal data and the General Data Protection Regulation. NOYB, a digital rights organization founded by Max Schrems, which successfully challenged the two predecessor frameworks to the DPF, is also widely expected to file a challenge to the DPF after October 10, when U.S. companies will be able to use the DPF for the cross-border exchange of data.

UK Finalizes UK-U.S. Data Bridge

The United Kingdom Secretary of State for Science, Innovation, and Technology laid regulations in the UK Parliament. The action gives effect to the UK-U.S. Data Bridge, which will allow organizations in the UK to transfer personal data to U.S. organizations that have certified the UK extension to the EU-U.S. Data Privacy Framework. The UK-U.S. Data Bridge will become effective and may be used for transfers of personal data from the UK to the U.S. starting on October 12, 2023.

United Kingdom's Online Safety Bill to Become Law

In the United Kingdom, the Online Safety Bill ("OSB") passed its final Parliamentary debate and is ready to become law. The OSB places new duties on social media companies to protect children on the internet, including (1) removing illegal content quickly or preventing it from appearing; (2) preventing children from accessing age-inappropriate content; (3) enforcing age limits and checks; (4) ensuring risks and

dangers posed to children are more transparent; and (5) providing parents and children with clear and accessible ways to report problems online. Under the bill, social media platforms will face significant fines up to £18 million or 10 percent of their global annual revenue, whichever is larger, if they do not act rapidly to prevent and remove illegal content and stop children from seeing harmful material. In addition, the bill includes new laws that will tackle online fraud and violence against women and girls.

Tianmei Ann Huang, Amanda M. Noonan, and Jason C. Hirsch also contributed to this article.

National Law Review, Volume XIII, Number 278