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

The BR Privacy & Security Download: January 2025

Article By:

Sharon R. Klein

Philip N. Yannella

Alex C. Nisenbaum

Harrison Brown

Jennifer J. Daniels

Jeffrey N. Rosenthal

Must Read! The U.S. Department of Health and Human Services Office for Civil Rights recently proposed an amendment to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule to strengthen cyber security protections for electronic protected health information. Read the full alert to learn more about the first significant update to HIPAA's Security Rule in over a decade. **Read More >>**

STATE & LOCAL LAWS & REGULATIONS

Five New State Comprehensive Privacy Laws Effective in January with Three More to Follow in 2025: With the start of the new year, five new state comprehensive privacy laws have become effective. The comprehensive privacy laws of Delaware, Iowa, Nebraska, and New Hampshire became effective on January 1, 2025, and New Jersey's law will come into effect on January 15, 2025. Tennessee, Minnesota, and Maryland will follow suit and take effect on July 1, 2025, July 31, 2025, and October 1, 2025, respectively. Companies should review their privacy compliance programs to identify potential compliance gaps with differences in the increasing patchwork of state laws.

Colorado Issues Proposed Draft Amendments to CPA Rules: The Colorado Attorney General announced the adoption of amendments to the Colorado Privacy Act ("CPA") rules. The rules will become effective on January 30, 2025. The rules provide enhanced protections for the processing of biometric data as well as the processing of the online activities of minors. Specifically, companies must develop and implement a written biometric data policy, implement appropriate security measures regarding biometric data, provide notice of the collection and processing of biometric data,

obtain employee consent for the processing of biometric data, and provide a right of access to such data. In the context of minors, the amendment requires that entities obtain consent prior to using any system design feature designed to significantly increase the use of an online service of a known minor and to update the Data Protection Assessments to address processing that presents heightened risks to minors. Entities already subject to the CPA should carefully review whether they may have heightened obligations for the processing of employee biometric data, a category of data previously exempt from the scope of the CPA.

CPPA Announces Increased Fines and Penalties Under CCPA: The California Privacy Protection Agency ("CPPA"), the enforcement authority of the California Consumer Privacy Act ("CCPA"), has adjusted the fines and monetary thresholds of the CCPA. Under the CCPA, in January of every odd-numbered year, the CPPA must make this adjustment to account for changes in the Consumer Price Index. The CPPA has increased the monetary thresholds of the CCPA from $25,000,000 to $26,625,000. The CPPA also increased the range of monetary damages from between $100 to $750 per consumer per incident or actual damages (whichever is greater) to $107 to $799. The range of civil penalties and administrative fine amounts further increased from $2,500 for each violation of the CCPA or $7,500 for each intentional violation and violations involving the personal information of children under 16 to $2,663 and $7,988, respectively. The new amounts went into effect on January 1, 2025.

Connecticut State Senator Previews Proposed Legislation to Update State's Comprehensive Privacy Law: Connecticut State Senator James Maroney (D) has announced that he is drafting a proposed update to the Connecticut Privacy Act that would expand its scope, provide enhanced data subject rights, include artificial intelligence ("AI") provisions, and potentially eliminate certain exemptions currently available under the Act. Senator Maroney expects that the proposed bill could receive a hearing by late January or early February. Although Maroney has not published a draft, he indicated that the draft would likely (1) reduce the compliance threshold from the processing of the personal data of 100,000 consumers to 35,000 consumers; (2) include AI anti-discrimination measures, potentially in line with recent anti-discrimination requirements in California and Colorado; (3) expand the definition of sensitive data to include religious beliefs and ethnic origin, in line with other state laws; (4) expand the right to access personal data under the law to include a right to access a list of third parties to whom personal data was disclosed, mirroring similar rights in Delaware, Maryland, and Oregon; and (5) potentially eliminate or curtail categorical exemptions under the law, such as that for financial institutions subject to the Gramm-Leach-Bliley Act.

CPPA Endorses Browser Opt-Out Law: The CPPA's board voted to sponsor a legislative proposal that would make it easier for California residents to exercise their right to opt out of the sale of personal information and sharing of personal information for cross-context behavioral advertising purposes. Last year, Governor Newsome vetoed legislation with the same requirements. Just as last year's vetoed legislation, the legislative proposal sponsored by the CPPA requires browser vendors to include a feature that allows users to exercise their opt-out right through opt-out preference signals. Under the CCPA, businesses are required to honor opt-out preference signals as valid opt-out requests. Opt-out preference signals allow a consumer to exercise their opt-out right with all businesses they interact with online without having to make individualized requests with each business. If the proposal is adopted, California would be the first state to require browser vendors to offer consumers the option to enable these signals. Six other states (Colorado, Connecticut, Delaware, Montana, Oregon, and Texas) require businesses to honor browser privacy signals as an opt-out request.

FEDERAL LAWS & REGULATIONS

HHS Proposes Updates to HIPAA Security Rule: The U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") issued a Notice of Proposed Rulemaking ("NPRM") to amend the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule to strengthen cybersecurity protections for electronic protected health information ("ePHI"). The NPRM proposes the first significant updates to HIPAA's Security Rule in over a decade. The NPRM makes a number of updates to the administrative, physical, and technical safeguards specified by the Security Rule, removes the distinction between "required" and "addressable" implementation specifications, and makes all implementation specifications "required" with specific, limited exceptions.

Trump Selects Andrew Ferguson as New FTC Chair: President-elect Donald Trump has selected current Federal Trade Commission ("FTC") Commissioner Andrew Ferguson to replace Lina Khan as the new FTC Chair. Ferguson is one of two Republicans of the five FTC Commissioners and has been a Commissioner since April of 2024. Prior to becoming an FTC Commissioner, Ferguson served as Virginia's solicitor general. During his time as an FTC Commissioner, Ferguson dissented from several of Khan's rulemaking efforts, including a ban on non-compete clauses in employment contracts. Separately, Trump also selected Mark Meador to be an FTC Commissioner. Once Meador is confirmed to give the FTC a Republican majority, a Republican-led FTC under Ferguson may deprioritize rulemaking and enforcement efforts relating to privacy and AI. In a leaked memo first reported by Punchbowl News, Ferguson wrote to Trump that, under his leadership, the FTC would "stop abusing FTC enforcement authorities as a substitute for comprehensive privacy legislation" and "end the FTC's attempt to become an AI regulator."

FERC Updates and Consolidates Cybersecurity Requirements for Gas Pipelines : The U.S. Federal Energy Regulatory Commission ("FERC") has issued a final rule to update and consolidate cybersecurity requirements for interstate natural gas pipelines. Effective February 7, 2025, the rule adopts Version 4.0 of the Standards for Business Practices of Interstate Natural Gas Pipelines, as approved by the North American Energy Standards Board ("NAESB"). This update aims to enhance the efficiency, reliability, and cybersecurity of the natural gas industry. The new standards consolidate existing cybersecurity protocols into a single manual, streamlining processes and strengthening protections against cyber threats. This consolidation is expected to make it easier and faster to revise cybersecurity standards in response to evolving threats. The rule also aligns with broader U.S. government efforts to prioritize cybersecurity across critical infrastructure sectors. Compliance filings are required by February 3, 2025, and the standards must be fully adhered to by August 1, 2025.

House Taskforce on AI Delivers Report to Address AI Advancements: The House Bipartisan Task Force on Artificial Intelligence (the "Task Force") submitted its comprehensive report to Speaker Mike Johnson and Democratic Leader Hakeem Jeffries. The Task Force was created to ensure America's continued global leadership in AI innovation with appropriate safeguards. The report advocates for a sectoral regulatory structure and an incremental approach to AI policy, ensuring that humans remain central to decision-making processes. The report provides a blueprint for future Congressional action to address advancements in AI and articulates guiding principles for AI adoption, innovation, and governance in the United States. Key areas covered in the report include government use of AI, federal preemption of state AI law, data privacy, national security, research and development, civil rights and liberties, education and workforce development, intellectual property, and content authenticity. The report aims to serve as a roadmap for Congressional action, addressing the potential of AI while mitigating its risks.

CFPB Proposes Rule to Restrict Sale of Sensitive Data: The Consumer Financial Protection

Bureau (“CFPB”) proposed a rule that would require data brokers to comply with the Fair Credit Reporting Act (“FCRA”) when selling income and certain other consumer financial data. CFPB Director Rohit Chopra stated the new proposed rule seeks to limit “widespread evasion” of the FCRA by data brokers when selling sensitive personal and financial information of consumers. Under the proposed rule, data brokers could sell financial data only for permissible purposes under the FCRA, including checking on loan applications and fraud prevention. The proposed rule would also limit the sale of personally identifying information known as credit header data, which can include basic demographic details, including names, ages, addresses, and phone contacts.

FTC Issues Technology Blog on Mitigating Security Risks through Data Management, Software Development and Product Design: The Federal Trade Commission (“FTC”) published a blog post identifying measures that companies can take to limit the risks of data breaches. These measures relate to security in data management, security in software development, and security in product design for humans. The FTC emphasizes comprehensive governance measures for data management, including (1) enforcing mandated data retention schedules; (2) mandating data deletion in accordance with these schedules; (3) controlling third-party data sharing; and (4) encrypting sensitive data both in transit and at rest. In the context of security in software development, the FTC identified (1) building products using memory-safe programming languages; (2) rigorous testing, including penetration and vulnerability testing; and (3) securing external product access to prevent unauthorized remote intrusions as key security measures. Finally, in the context of security in product design for humans, the FTC identified (1) enforcing least privilege access controls; (2) requiring phishing-resistant multifactor authentication; and (3) designing products and services without the use of dark patterns to reduce the over-collection of data. The blog post contains specific links to recent FTC enforcement actions specifically addressing each of these issues, providing users with insight into how the FTC has addressed these issues in the past. Companies reviewing their security and privacy governance programs should ensure that they consider these key issues.

U.S. LITIGATION

Texas District Court Prevents HHS from Enforcing Reproductive Health Privacy Rule Against Doctor: The U.S. District Court for the Northern District of Texas ruled that a Texas doctor is likely to prevail on her claim that HHS exceeded its statutory authority when it adopted an amendment to the Health Insurance Portability and Accountability Act (“HIPAA”) Privacy Rule that protects reproductive health care information and enjoined HHS from enforcing the rule against her. The 2024 amendment to the HIPAA Privacy Rule prohibits covered entities from disclosing information that could lead to an investigation or criminal, civil, or administrative liability for seeking, obtaining, providing, or facilitating reproductive health care. The Court stated that the rule likely unlawfully interfered with the plaintiff’s state-law duty to report suspected child abuse in violation of Congress’s delegation to the agency to enact rules interpreting HIPAA without limiting any law providing for such reporting. The plaintiff argued that, under Texas law, she is obligated to report instances of child abuse within 48 hours, and that relevant requests from Texas regulatory authorities demand the full, unredacted patient chart, which for female patients includes information about menstrual periods, number of pregnancies, and other reproductive health information, among other reproductive health information.

Attorneys General Oppose Clearview AI Biometric Data Privacy Settlement: A proposed settlement in the Clearview AI Illinois Biometric Information Privacy Act (“BIPA”) litigation is facing opposition from 22 states and the District of Columbia. The Attorneys General of each state argue that the settlement, which received preliminary approval in June 2024, lacks meaningful injunctive relief and offers an unusual financial stake in Clearview AI to plaintiffs. The settlement would grant the class of consumers a 23 percent stake in Clearview AI, potentially worth $52 million, based on a

September 2023 valuation. Alternatively, the class could opt for 17 percent of the company's revenue through September 2027. The AGs contend the settlement doesn't adequately address consumer privacy concerns and the proposed 39 percent attorney fee award is excessive. Clearview AI has filed a motion to dismiss the states' opposition, arguing it was submitted after the deadline for objections. A judge will consider granting final approval for the settlement at a hearing scheduled on January 30, 2025.

Federal Court Upholds New Jersey's Daniel's Law, Dismissing Free Speech Challenges: A federal judge affirmed the constitutionality of New Jersey's Daniel's Law, dismissing First Amendment objections raised by data brokers. Enacted following the murder of Daniel Anderl, son of U.S. District Judge Esther Salas, the law permits covered individuals—including active, retired, and former judges, prosecutors, law enforcement officers, and their families—to request the removal of personal details, such as home addresses and unpublished phone numbers, from online platforms. Data brokerage firms that find themselves on the receiving end of such requests are mandated by the statute to comply within ten (10) business days, with penalties for non-compliance including actual damages or a $1,000 fine for each violation, as well as potential punitive damages for instances of willful disregard. Notably, in 2023, Daniel's Law was amended to allow claim assignments to third parties, resulting in over 140 lawsuits filed by a single consumer data protection company: Atlas Data Privacy Corporation. Atlas Data, a New Jersey firm specializing in data deletion, has emerged as a significant force in this litigation, utilizing Daniel's Law to challenge data brokers on behalf of around 19,000 individuals. The court, in upholding Daniel's Law, emphasized its critical role in safeguarding public officials while concurrently ensuring public oversight remains strong. Although data brokers contended that the law infringed on free speech and unfairly targeted their operations, the court dismissed these claims as lacking merit, instead placing significant emphasis on the statute's relatively focused scope and substantial state interest at play. Although unquestionably a significant victory for advocates of privacy rights, the judge permitted an immediate appeal by the data brokers.

GoodRx Settles Class Action Suit Over Alleged Data Sharing Violations: GoodRx has agreed to a $25 million settlement in a class-action lawsuit alleging the company violated privacy laws by sharing users' sensitive health data with advertisers like Meta Platforms, Google, and Criteo Corp. The settlement, if approved, would resolve a lawsuit filed in February 2023. The lawsuit followed an FTC action alleging that GoodRx shared information about users' prescriptions and health conditions with advertising companies. GoodRx settled the FTC matter for $1.5 million. The proposed class in the class-action lawsuit is estimated to be in the tens of millions and would give each class member an average recovery ranging from $3.31 to $11.03. The settlement also allows the plaintiffs to use information from GoodRx to pursue their claims against the other defendants, including Meta, Google, and Criteo.

23andMe Data Breach Suit Settlement Approved: A federal judge approved a settlement to resolve claims that alleged 23andMe Inc. failed to secure the sensitive personal data causing a data breach in 2023. According to 23andMe, a threat actor was able to access roughly 14,000 user accounts through credential stuffing, which further enabled access to the personal information that approximately 6.9 million users made available through 23andMe's DNA Relative and Family Tree profile features. Under the terms of the $30 million settlement, class members will receive cash compensation and three years of data monitoring services, including genetic services.

U.S. ENFORCEMENT

FTC Takes Action Against Company for Deceptive Claims Regarding Facial Recognition Software: The Federal Trade Commission ("FTC") announced that it has entered

into a settlement with IntelliVision Technologies Corp. (“IntelliVision”), which provides facial recognition software used in home security systems and smart home touch panels. The FTC alleged that IntelliVision’s claims that it had one of the highest accuracy rates on the market, that its software was free of gender or racial bias, and was trained on millions of faces was false or misleading. The FTC further alleged that IntelliVision did not have adequate evidence to support its claim that its anti-spoofing technology ensures the system cannot be tricked by a photo or video image. The proposed order against IntelliVision specifically prohibits IntelliVision from misrepresenting the effectiveness, accuracy, or lack of bias of its facial recognition technology and its technology to detect spoofing, and the comparative performance of the technology with respect to individuals of different genders, ethnicities, and skin tones.

FTC Settles Enforcement Actions with Data Brokers for Selling Sensitive Location Data: The FTC announced settlements with data brokers Gravy Analytics Inc. (“Gravy Analytics”) and Mobilewalla, Inc. (“Mobilewalla”) related to the tracking and sale of sensitive location data of consumers. According to the FTC, Gravy Analytics violated the FTC Act by unfairly selling sensitive consumer location data, by collecting and using consumers’ location data without obtaining verifiable user consent for commercial and government uses, and by selling data regarding sensitive characteristics such as health or medical decisions, political activities, and religious views derived from location data. Under the proposed settlement, Gravy Analytics will be prohibited from selling, disclosing, or using sensitive location data in any product or service, delete all historic location data and data products using such data, and must establish a sensitive data location compliance program. Separately, the FTC settled allegations against Mobilewalla stemming from allegations that Mobilewalla collected location data from real-time bidding exchanges and third-party aggregators, including data related to health clinic visits and visits to places of worship, without the knowledge of consumers, and subsequently sold such data. According to the FTC, when Mobilewalla bid to place an ad for its clients on a real-time advertising bidding exchange, it unfairly collected and retained the information in the bid request, even when it didn’t have a winning bid. Under the proposed settlement, Mobilewalla will be prohibited from selling sensitive location data and from collecting consumer data from online advertising auctions for purposes other than participating in those auctions.

Texas Attorney General Issues New Warnings Under State’s Comprehensive Privacy Law: The Texas Attorney General issued warnings to satellite radio broadcaster Sirius XM and three mobile app providers that they appear to be sharing sensitive data of consumers, including location data, without proper notification or obtaining consent. The letter warnings did not come with a press release or other public statement and were reported by Recorded Future News, who obtained the notices through a public records request. The letter to Sirius XM stated that the Attorney General’s office found a number of violations of the Texas Data Privacy and Security Act by the Sirius XM privacy notice, including failing to provide reasonably clear notice of the categories of sensitive data being processed and processing sensitive data without appropriate consent. Similar letters were sent to mobile app providers stating that the providers failed to obtain consumer consent for data sharing or including information on how consumers could exercise their rights under Texas law.

Texas Attorney General Launches Investigations Into 15 Companies for Children’s Privacy Practices: The Texas Attorney General’s office announced it had launched investigations into Character.AI and 14 other companies including Reddit, Instagram, and Discord. The Attorney General’s press release stated that the investigations related to the companies’ privacy and safety practices for minors pursuant to the Securing Children Online through Parental Empowerment (“SCOPE”) Act and the Texas Data Privacy and Security Act (“TDPSA”). Details of the Attorney General’s allegations were not provided in the announcement. The TDPSA requires companies to

provide notice and obtain consent to collect and use minors' personal data. The SCOPE Act prohibits digital service providers from sharing, disclosing, or selling a minor's personal identifying information without permission from the child's parent or legal guardian and provides parents with tools to manage privacy settings on their child's account.

HHS Imposes Penalty Against Medical Provider for Impermissible Access to PHI and Security Rule Violations: The U.S. Department of Health and Human Services Office of Civil Rights ("OCR") announced that it imposed a $1.19 million civil penalty against Gulf Coast Pain Consultants, LLC d/b/a Clearway Pain Solutions Institute ("GCPC") for violations of the HIPAA Security Rule arising from a data breach. GCPC's former contractor had impermissibly accessed GCPC's electronic medical record system to retrieve protected health information ("PHI") for use in potential fraudulent Medicare claims. OCR's investigation determined that the impermissible access occurred on three occasions, affecting approximately 34,310 individuals. The compromised PHI included patient names, addresses, phone numbers, email addresses, dates of birth, Social Security numbers, chart numbers, insurance information, and primary care information. OCR's investigations revealed multiple potential violations of the HIPAA Security Rule, including failures to conduct a compliant risk analysis and implement procedures to regularly review records of activity in information systems and terminate former workforce members' access to electronic PHI.

HHS Settles with Health Care Clearinghouse for HIPAA Security Rule Violations: OCR announced a settlement with Inmediata Health Group, LLC ("Inmediata"), a healthcare clearinghouse, for potential violations of the HIPAA Security Rule, following OCR's receipt of a 2018 complaint that PHI was accessible to search engines like Google, on the Internet. OCR's investigation determined that from May 2016 through January 2019, the PHI of 1,565,338 individuals was made publicly available online. The PHI disclosed included patient names, dates of birth, home addresses, Social Security numbers, claims information, diagnosis/conditions, and other treatment information. OCR's investigation also identified multiple potential HIPAA Security Rule violations including failures to conduct a compliant risk analysis and to monitor and review Inmediata's health information systems' activity. Under the settlement, Inmediata paid OCR $250,000. OCR determined that a corrective action plan was not necessary in this resolution as Inmediata had previously agreed to a settlement with 33 states that included corrective actions that addressed OCR's findings.

New York State Healthcare Provider Settles with Attorney General Regarding Allegations of Cybersecurity Failures: HealthAlliance, a division of Westchester Medical Center Health Network ("WMCHealth"), has agreed to pay a $1.4 million fine, with $850,000 suspended, due to a 2023 data breach affecting over 240,000 patients and employees in New York State. The breach at issue, which occurred between September and October 2023, was reportedly caused by a security flaw in Citrix NetScaler—a tool used by many organizations to optimize web application performance and availability by reducing server load—that went unpatched. Although HealthAlliance was made aware of the vulnerability, they were unsuccessful in patching it due to technical difficulties, ultimately resulting in the exposure of 196 gigabytes of data, including particularly sensitive information like Social Security numbers and medication records. As part of its agreement with New York State, HealthAlliance must enhance its cybersecurity practices by implementing a comprehensive information security program, developing a data inventory, and enforcing a patch management policy to address critical vulnerabilities within 72 hours. For more details, view the press release from the New York Attorney General's office.

HHS Settles with Children's Hospital for HIPAA Privacy and Security Violations: OCR announced a $548,265 civil monetary penalty against Children's Hospital Colorado

("CHC") for violations of the HIPAA Privacy and Security Rules arising from data breaches in 2017 and 2020. The 2017 data breach involved a phishing attack that compromised an email account containing 3,370 individuals' PHI and the 2020 data breach compromised three email accounts containing 10,840 individuals' PHI. OCR's investigation determined that the 2017 data breach occurred because multi-factor authentication was disabled on the affected email account. The 2020 data breach occurred, in part, when workforce members gave permission to unknown third parties to access their email accounts. OCR found violations of the HIPAA Privacy Rule for failure to train workforce members on the HIPAA Privacy Rule, and the HIPAA Security Rule requirement to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems.

INTERNATIONAL LAWS & REGULATIONS

Italy Imposes Landmark GDPR Fine on AI Provider for Data Violations: In the first reported EU penalty under the GDPR relating to generative AI, Italy's data protection authority, the Garante, fined OpenAI 15 million euros for breaching the European Union's General Data Protection Regulation ("GDPR"). The penalty was linked to three specific incidents involving OpenAI: (1) unauthorized use of personal data for ChatGPT training without user consent, (2) inadequate age verification risking exposure of minors to inappropriate content, and (3) failure to report a March 2023 data breach that exposed users' contact and payment information. The investigation into OpenAI, which began after the Garante was made aware of the March 2023 breach, initially resulted in Italy temporarily blocking access to ChatGPT but eventually reinstated it after OpenAI made concrete improvements to its age verification and privacy policies. Alongside the monetary penalty, OpenAI is additionally mandated to conduct a six-month public awareness campaign in Italy to educate the Italian public on data collection and individual user rights under GDPR. OpenAI has said that it plans to appeal the Garante's decision, arguing that the fine exceeds its revenue in Italy.

Australian Parliament Approves Privacy Act Reforms and Bans Social Media Use by Minors: The Australian Parliament passed a number of privacy bills in December. The bills include reforms to the Australian Privacy Act, a law requiring age verification by social media platforms, and a law banning social media use by minors under the age of 16. Privacy Act reforms include new enforcement powers for the Office of the Australian Information Commissioner that clarify when "serious" breaches of the Privacy Act occur and allow the OAIC to bring civil penalty proceedings for lesser breaches. Other reforms include requiring entities that use personal data for automated decision-making to include in their privacy notices information about what data is used for automated decision-making and what types of decisions are made using automated decision-making technology.

EDPB Releases Opinion on Personal Data Use in AI Models: In response to a formal request from Ireland's Data Protection Commission asking for clarity about how the EU General Data Protection Regulation ("GDPR") applies to the training of large language models with personal data, the European Data Protection Board ("EDPB") released its opinion regarding the lawful use of personal data for the development and deployment of artificial intelligence models (the "Opinion"). The Irish Data Protection Commission specifically requested EDPB to opine on: (1) when and how an AI model can be considered anonymous, (2) how legitimate interests can be used as the legal basis in the development and deployment phases of an AI model, and (3) the consequences of unlawful processing in the development phase of an AI model on its subsequent operation. With respect to anonymity, the EDPB stated this should be analyzed on a case-by-case basis taking into account the likelihood of obtaining personal data of individuals whose data was used to build the model and the likelihood of extracting personal data from queries. The Opinion describes certain methods that

controllers can use to demonstrate anonymity. With respect to the use of legitimate interest as a legal basis for processing, the EDPB restated a three-part test to assess legitimate interest from its earlier guidance. Finally, the EDPB reviewed several scenarios in which personal data may be unlawfully processed to develop an AI model.

Second Draft of General-Purpose AI Code of Practice Published: The European Commission announced that independent experts published the Second Draft of the General Purpose AI Code of Practice. The AI Code of Practice is designed to be a guiding document for providers of general-purpose AI models, allowing them to demonstrate compliance with the AI Act. Under the EU AI Act, providers are persons or entities that develop an AI system and place that system on the market. This second draft is based on the responses and comments received on the first draft and is designed to provide a "future-proof" code. The first part of the Code details transparency and copyright obligations for all providers of general-purpose AI models. The second part of the Code applies to providers of advanced general-purpose AI models that could pose systemic risks. This section outlines measures for systemic risk assessment and mitigation, including model evaluations, incident reporting, and cybersecurity obligations. The Second Draft will be open for comments until January 15, 2025.

NOYB Approved to Bring Collective Redress Claims: The Austrian-based non-profit organization None of Your Business ("NOYB") has been approved as a Qualified Entity in Austria and Ireland, enabling it to pursue collective redress actions across the European Union ("EU"). Famous for challenging the EU-US data transfer framework through its Schrems I and II actions, NOYB intends to use the EU's collective action redress system to challenge what it describes as unlawful processing without consent, use of deceptive dark patterns, data sales, international data transfers, and use of "absurd" language in privacy policies. Unlike US class actions, these EU actions are strictly non-profit. However, they do provide for both injunctive and monetary redress measures. NOYB intends to bring its first actions in 2025. Click here to learn more and read NOYB's announcement.

EDPB Issues Guidelines on Third Country Authority Data Requests: The EDPB published draft guidelines on Article 48 of the GDPR relating to the transfer or disclosure of personal data to a governmental authority in a third country (the "Guidelines"). The Guidelines state that, as a general rule, requests from governmental authorities are recognizable and enforceable under applicable international agreements. The Guidelines further state that any such transfer must also comply with Article 6 with respect to legal basis for processing and Article 46 regarding legal mechanism for international data transfer. The Guidelines will be available for public consultation until January 27, 2025.

Irish DPC Fines Meta €251 Million for Violations of the GDPR: The Irish Data Protection Commission (DPC) fined Meta €251 million following a 2018 data breach that affected 29 million Facebook accounts globally, including 3 million in the European Union. The breach exposed personal data such as names, contact information, locations, birthdates, religious and political beliefs, and children's data. The DPC found that Meta Ireland violated General Data Protection Regulation (GDPR) Articles 33(3) and 33(5) by failing to provide complete information in their breach notification and to properly document the breach. Furthermore, Meta Ireland infringed GDPR Articles 25(1) and 25(2) by neglecting to incorporate data protection principles into the design of their processing systems and by processing more data than necessary by default.

Additional Authors: Daniel R. Saeedi, Rachel L. Schaller, Gabrielle N. Ganze, Ana Tagvoryan, P. Gavin Eastgate, Timothy W. Dickens, Jason C. Hirsch, Tianmei Ann Huang, Adam J. Landy, Amanda

M. Noonan, and Karen H. Shin

National Law Review, Volume XV, Number 9