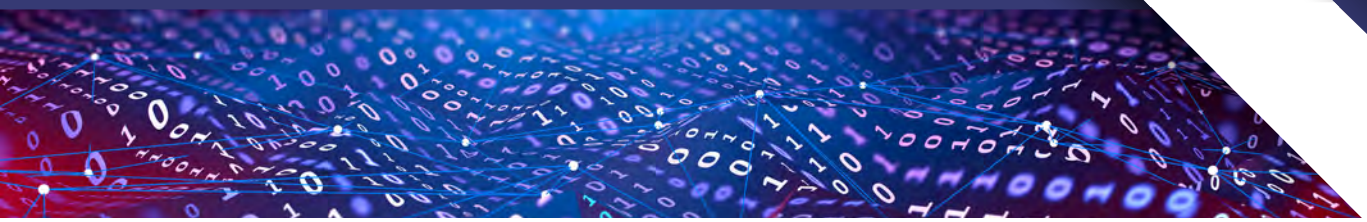
WILLKIE FARR & GALLAGHER LLP

BRUSSELS CHICAGO FRANKFURT HOUSTON LONDON LOS ANGELES MILAN NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON

Willkie Privacy, Cybersecurity & Data Strategy Review: *Data Privacy Day 2023*



CONTENTS

WELCOME

Dear Friends and Colleagues:

January 28 is recognized around the world as Data Privacy Day, a day to raise awareness and promote privacy. In last year's Data Privacy Day Review, we talked about the increasing complexity and uncertainty triggered by "the legal, regulatory, ethical and business issues associated with privacy and data security," but we did not predict how the pace of change would accelerate in 2022, nor how the sources of uncertainty would multiply. Last year, across the globe, and from city councils to national capitals, privacy, data security, and cybersecurity issues were at the forefront:

- In the United States, the greatest source of uncertainty was the U.S. Supreme Court. In *Dobbs v. Jackson Women's Health Organization*, the Court upended decades of precedent and common understandings of the constitutional right to privacy, and in the process created significant concern about how the rapidly proliferating information collected via apps and other digital tools might be used to prosecute doctors and women.
- Other sources of uncertainty were more predictable. Congress debated, but ultimately did not enact, a federal privacy law, thanks in part to heated opposition from California lawmakers. But numerous federal agencies — including the Federal Trade Commission, the Securities & Exchange Commission, and the Consumer Financial Protection Bureau — initiated rulemakings proposing to adopt rules related to companies' collection, use, disclosure, and securing of personal information.
- On the cybersecurity front, Russia's invasion of Ukraine in early 2022 sharpened the focus of both the U.S. public and private sectors on the importance of robust cybersecurity strategies and tactics. While concerns raised by U.S. government officials of a possible impending "cyber war" against U.S. targets have thus far failed to materialize, the federal government continues to move forward with policies, rules, and legislation designed to encourage continued vigilance and information sharing.
- Outside the United States, privacy and cybersecurity laws continued to evolve. In Europe, regulators escalated their enforcement of the General Data Protection Regulation ("GDPR") against social media and other major Internet platforms, even as the announcement of a new Trans-Atlantic Data Privacy Framework between the U.S. and EU offered some hope, at least among optimists, that a workable compromise between European privacy concerns and U.S. national security interests had been achieved to allow personal data to flow freely across the Atlantic. Meanwhile, in Argentina, India, Israel, and other countries around the world, policymakers proposed new laws to import concepts from GDPR and make those countries better candidates for "adequacy" status.
- Last year also saw Australia become the target of several massive ransomware attacks, spurring the Australian Parliament to introduce and quickly enact legislation that would significantly increase penalties for data breaches to a minimum of AU $50 million.

Against this backdrop, we see Data Privacy Day 2023 as an opportunity to look ahead at the major issues that businesses, policymakers, and regulators are likely to face in the coming months. If 2023 is anything like 2022, it will be quite a journey — we look forward to taking it with you.

Daniel Alvarez
Partner
Co-Chair, Privacy, Cybersecurity & Data Strategy Practice Group

1875 K Street, N.W.
Washington, DC 20006-1238
T 202 303 1125
F 202 303 2125

Laura Jehl
Partner
Co-Chair, Privacy, Cybersecurity & Data Strategy Practice Group

1875 K Street, N.W.
Washington, DC 20006-1238
T 202 303 1056
F 202 303 2000

NOTABLE PRIVACY AND CYBERSECURITY DEVELOPMENTS OF 2022

January

January 1: California SB 41, the Genetic Information Privacy Act, took effect. The Act requires direct-to-consumer genetic testing entities to receive consent from individuals with respect to the collection, use, and disclosure of their personal information, and provides rights of access and deletion. The Act also requires in-scope companies to, among other things, implement reasonable security practices to protect against the unauthorized access, use, modification, or disclosure of genetic data. The California Attorney General may enforce the law, with fines up to $1,000 per incident for negligent violations and up to $10,000 for intentional violations.

January 4: The FTC asserted its authority over cybersecurity and broader data security matters, warning companies that failure to identify and patch instances of the Log4j vulnerability could violate the FTC Act, and that the FTC would use "its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j or similar vulnerabilities in the future."

January 19: President Biden signed a National Security Memorandum ("NSM") requiring national security systems to deploy the same network cybersecurity measures as those required in President Biden's Executive Order 14028 ("EO 14028"), Improving the Nation's Cybersecurity. The NSM establishes timelines and guidance for implementation of cybersecurity requirements under EO 14028; improves the visibility of cybersecurity incidents that occur on national security systems; requires agencies to secure cross-domain tools that transfer data between classified and unclassified systems; and requires agencies to act to protect or mitigate cyber threats to national security systems.

February

February 3: The Department of Homeland Security announced the establishment of the Cyber Safety Review Board ("CSRB"), as directed in EO 14028, Improving the Nation's Cybersecurity. The CSRB is a public-private initiative that brings together government and industry leaders to elevate national security. According to a DHS press release, the CSRB will review and assess significant cybersecurity events so that government, industry, and the broader security community can better protect the country's infrastructure and networks. The first review was focused on Log4j software vulnerabilities, with a report released in July 2022 highlighting a number of recommendations for organizations to manage both the immediate risks presented by the Log4j vulnerability and longer-term risks related to software supply chain issues.

February 9: The SEC proposed rules related to cybersecurity risk management for registered investment advisers, as well as amendments to certain rules that govern investment adviser and fund disclosures. Among other things, the proposed rules would require advisers and funds to (i) adopt and implement written cybersecurity policies and procedures; (ii) report significant cybersecurity incidents to the SEC; (iii) publicly disclose significant cybersecurity incidents that have occurred over the last two years in registration statements; and (iv) establish new recordkeeping procedures to protect the availability of cybersecurity-related information. (As of January 2023, the proposed rules had yet to be adopted.)

February 24: Utah SB 227, the Utah Consumer Privacy Act, passed the Utah Senate. It subsequently passed the Utah House of Representatives on March 3, 2022, and was signed into law by Utah Governor Spencer Cox on March 24, 2022. The law will take effect on December 31, 2023.

March

March 9: The SEC proposed rules to enhance and standardize disclosures regarding cybersecurity risk management strategy, governance, and incident reporting by public companies. Among other things, the proposed rules would require reporting of "material cybersecurity incidents" to the SEC within four days, as well as significant new annual disclosure requirements related to the company's cybersecurity risk management efforts, and information about any board members with cybersecurity expertise or experience. As of January 2023, the proposed new rules have not been adopted.

March 15: President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), which creates new obligations for owners and operators of critical infrastructure, including an obligation to report certain cyber incidents to CISA within 72 hours and an obligation to report ransomware payments within 24 hours. These reporting obligations will take effect when CISA promulgates implementing regulations. As of January 2023, CISA has initiated, but not yet completed, its rulemaking.

March 25: President Biden and European Commission President von der Leyen announced that the U.S. and the EU had reached an agreement in principle regarding the Trans-Atlantic Data Privacy Framework. U.S. Secretary of Commerce Gina Raimondo and EU Commissioner Didier Reynders announced that they would intensify negotiations to memorialize the Framework in appropriate legal documents. In December 2022, the European Commission released a draft Adequacy Decision on the Framework which must go through an extensive adoption process which incorporates the opinions of other EU regulatory authorities. This process is estimated to take approximately six months.

April

April 13: The California Privacy Protection Agency ("CPPA") announced its plan to hold stakeholder sessions in anticipation of its rulemaking to implement the California Privacy Rights Act of 2020 ("CPRA"). These stakeholder sessions took place May 4-6, 2022; the CPPA would finally commence the formal rulemaking process in July 2022 (see below).

April 19: New Jersey's A.B. 3950, prohibiting certain employer use of tracking devices, took effect. Unlike the comprehensive, omnibus privacy legislation that has been enacted in a number of other states, this law is an example of state efforts to fill targeted gaps in privacy/data protection absent comprehensive federal privacy legislation, and requires employers to provide notice to any employee who is tracked through a vehicle.

April 28: India's data protection regulator issued guidance relating to "information security practices, procedure, prevention, response and reporting of cyber incidents." In particular, the guidance requires parties to report cyber incidents to India's Computer Emergency Response Team ("CERT-In") within six hours of noticing such incidents or being notified about such incidents.

May

May 3: The European Parliament adopted the final recommendations of the Special Committee on Artificial Intelligence in the Digital Age. These recommendations are intended to inform parliamentary work both at the EU and Member State level, as part of the Commission's Horizon Europe and Digital Europe programs.

May 7: New York's Senate Bill S2628, requiring prior written notice to employees of electronic monitoring in the workplace, took effect. As with New Jersey's A.B. 3950, this legislation highlights the growing role of targeted privacy/data protection laws at the state level.

May 9: The American Civil Liberties Union announced the settlement of its biometric privacy litigation with Clearview AI. According to the ACLU's announcement, the settlement bans Clearview AI from selling access to its facial recognition database "across the United States."

May 12: The U.S. Department of Justice Civil Rights Division, together with the Equal Employment Opportunity Commission released guidance titled "Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring," explaining how the use of certain technologies in hiring decisions may violate the Americans with Disabilities Act.

June

June 21: H.R. 8152—the American Data Privacy and Protection Act ("ADPPA") was introduced in the U.S. House of Representatives. The ADPPA was the result of extensive bicameral and bipartisan negotiations, and would have resulted in a broad private right-of-action (a priority for Democrats) with extensive, but not total, preemption of state privacy efforts (a Republican priority).

June 24: The U.S. Supreme Court announced its decision in *Dobbs v. Jackson Women's Health Organization*. The decision,

which expressly overturned *Roe v. Wade* and *Casey v. Planned Parenthood*, has profound implications for the constitutional right to privacy, as well as significant practical implications for women's privacy with respect to reproductive health care. In response, the Biden Administration mobilized a whole-of-government effort to maximize protection of any information that companies and healthcare providers collect related to women's reproductive health.

June 29: The U.S. Department of Health and Human Services, Office for Civil Rights, released guidance regarding patient privacy protections in the wake of the Supreme Court's *Dobbs* decision, including how patient medical information should be safeguarded when using mobile phones and certain apps.

July

July 8: The CPPA initiated the formal rulemaking process to implement the CPRA by issuing proposed amendments to conform existing regulations under the California Consumer Privacy Act ("CCPA") to the new requirements of the CPRA. The CPPA requested written comments on the proposed regulations by August 23, 2022. The CPPA would release revised proposed amendments in November 2022 (see below); as of January 2023, the amendments had not yet been formally adopted.

July 11: Consistent with the Biden Administration's efforts to protect women's access to reproductive healthcare in the wake of the Supreme Court's *Dobbs* decision, the FTC issued a blog post affirming the agency's commitment to fully enforcing the law against illegal use and sharing of highly sensitive location and health data.

July 29: The New York Department of Financial Services ("NYDFS") proposed amendments to 23 NYCRR Part 500, its Cybersecurity Regulation. Among other things, the proposed amendments would add a new 24-hour notice requirement for any cybersecurity event where an extortion payment has been made, heighten oversight responsibilities of the board of directors and senior management, and create additional cybersecurity requirements for large covered entities by establishing a new class of covered entities called "Class A companies." NYDFS is expected to formally adopt the regulations in the first quarter of 2023.

August

August 11: The FTC initiated a long-awaited rulemaking on commercial surveillance and data security issues by adopting an Advance Notice of Proposed Rulemaking. The FTC cited numerous harms to consumers presented by surveillance issues, and sought comment on the prevalence of these practices and harms, its ability to address them absent some specific rules, and what kind of rules might help to address these harms. The FTC issued this Advance Notice pursuant to its Magnusson-Moss rulemaking authority, which includes a number of procedural steps that the FTC must undertake before it can come to final rules.

August 29: The FTC announced a lawsuit against Kochava Inc. for the sale of sensitive geolocation personal information. According to the FTC, "Kochava's data can reveal people's visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities," and "Kochava is enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence" without the knowledge or consent of the people to whom the data relates.

September

September 5: The Irish Data Protection Commissioner imposed a €405 million fine, one of the largest GDPR fines to date, against Meta Platforms Ireland Ltd. ("Meta"), alleging violations of the GDPR rules on the processing of children's personal data on Instagram.

September 12: Argentina's Data Protection Authority published a draft bill that would update Argentina's data protection law and bring it more in line with GDPR. Among other things, the bill requires data controllers to document and notify the Agency of data breaches within 48 hours of becoming aware of a breach.

September 12: Consistent with its obligations under CIRCIA, CISA issued a Request for Information seeking public

comment on the implementation of cyber incident reporting requirements. Numerous stakeholders filed comments, largely focusing on issues such as the proper threshold for reporting to CISA, what would need to be included in any report, and how quickly such reports must be filed.

September 15: California Governor Gavin Newsom signed AB 2273—the California Age Appropriate Design Code Act. Among other things, the Act requires certain websites to establish default privacy protections for children's data, and establishes a Children's Data Protection Working Group that is required to report best practices for implementation of the Act to the California legislature by January 2024. The Act will take effect on July 1, 2024.

September 30: Colorado Attorney General Phil Weiser published draft rules implementing the Colorado Privacy Act. Interested parties may submit written comments until February 1, 2023. The announcement also highlighted three public meetings, which took place in November 2022, to discuss the proposed draft rules.

October

October 7: As part of fulfilling the United States' obligations under the Trans-Atlantic Data Privacy Framework, President Biden signed an Executive Order on Enhancing Safeguards for U.S. Signals Intelligence Activities. Shortly thereafter, the Attorney General released new rules to establish a process for handling complaints under the Executive Order. The European Commission announced that in response to the Executive Order, it would prepare a draft adequacy decision.

October 24: The FTC issued a proposed order against both Drizly, LLC and its CEO for violations of Section 5 of the FTC Act in connection with Drizly's cybersecurity practices. The FTC's imposition of penalties on the CEO in his personal capacity has significant implications for executives at companies large and small, whose decisions to invest in and prioritize (or not) data security will now be subject to second guessing by regulators and carry the risk of personal liability. The order was finalized and adopted on January 10, 2023.

October 27: The Consumer Financial Protection Bureau ("CFPB") announced a rulemaking to give consumers greater control over their financial data. In particular, the CFPB's proposed rule would establish portability requirements for consumer data collected by financial firms. According to the CFPB, under its proposed rules "consumers would be able to more easily and safely walk away from companies offering bad products and poor service and move towards companies competing for their business with alternate or innovative products and services."

November

November 3: The CPPA released a revised version of proposed amendments implementing the CPRA changes to the CCPA and requested comments on the revised versions of the proposed amendments. Among other things, the revised amendments included language suggesting that the CPPA would take into consideration questions related to the timing of the amendments' adoption in making decisions about enforcement — a concession to commenters who highlighted the practical issues of compliance given the January 1, 2023 effective date of the CPRA's changes to CCPA.

November 9: NYDFS released a second round of amendments to the Cybersecurity Regulation. Among other things, the revised proposed amendments would require that where a covered entity is affected by and aware of a cybersecurity event on the systems of a third-party service provider, notification to NYDFS must be provided within 72 hours. Public comment on the revised proposed amendments was due to NYDFS by January 9, 2023.

November 15: The FTC announced a six-month extension of the deadline for compliance with its updated Safeguards Rule. The update imposed a number of new requirements for covered financial institutions, including designating a qualified individual to oversee their information security program; developing a written risk assessment; limiting and monitoring who can access sensitive customer information; encrypting all sensitive information; training security personnel; developing an incident response plan; periodically assessing the security practices of service providers; and implementing multi-factor authentication for individuals who access customer information. Companies now have until June 9, 2023 to come into compliance.

November 25: The Irish Data Protection Commissioner issued another significant fine to Meta, this time €265 million for violations of GDPR arising from a data leak that resulted in the personal data of approximately 533 million Facebook users worldwide being made available on the Internet.

November 28: Australia's Parliament passed amendments to existing Australian privacy law to increase the maximum penalties for serious or repeated privacy breaches from the prior AU $2.22 million penalty to whichever is the greater of (i) AU $50 million; (ii) three times the value of any benefit obtained through the misuse of information; or (iii) thirty percent of a company's adjusted turnover in the relevant period.

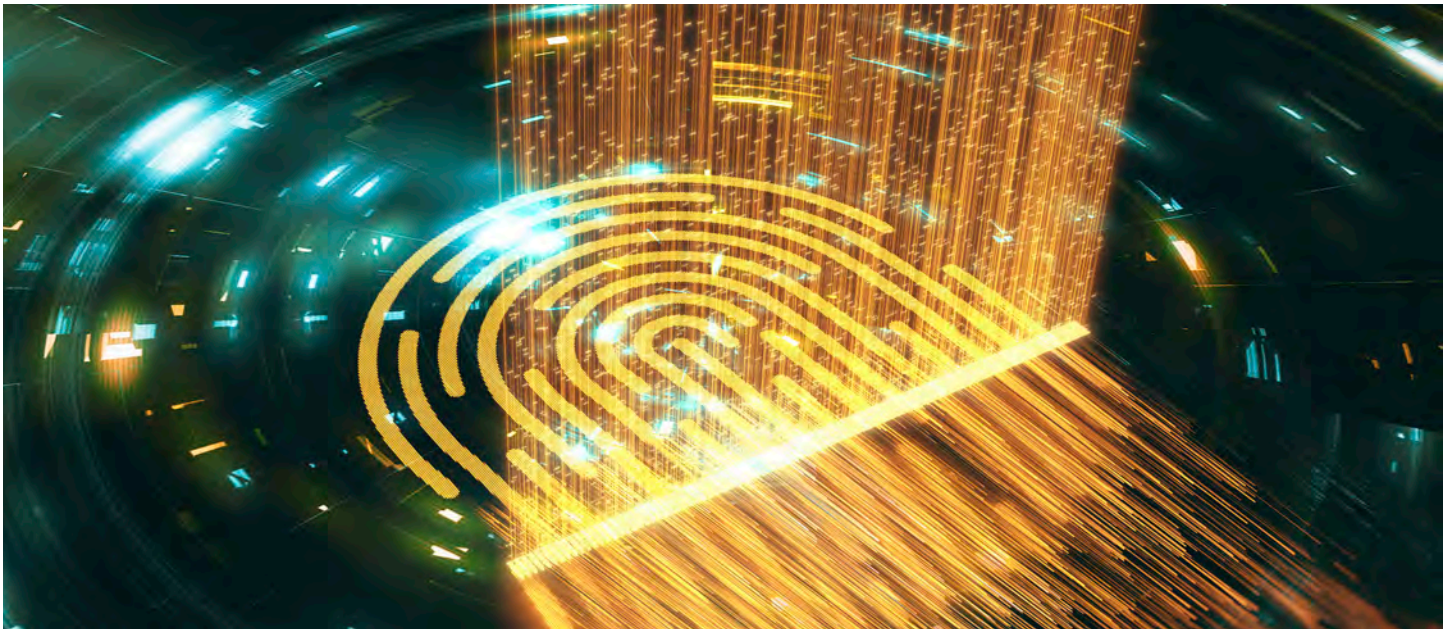
December

December 13: The European Commission released a draft adequacy decision that would, if formally adopted, make the Trans-Atlantic Data Privacy Framework ("Framework") a legitimate mechanism for companies transferring personal data from the EU to the U.S. The draft adequacy decision follows President Biden's Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, which endeavors to address European concerns about U.S. government access to personal data of EU data subjects. Among other things, companies seeking to use the new Framework must commit to complying with a detailed set of privacy obligations, including, for example, deleting personal data when it is no longer necessary for the purpose for which it was collected.

December 16: The CPPA held a public meeting regarding the status of the CPRA rulemaking process. Among other things, the CPPA announced that the earliest the proposed amendments to the CCPA regulations would likely come into effect would be April 2023, and that it had established a subcommittee to consider regulations regarding risk assessments, cybersecurity audits and automated decision-making, including profiling — the next step in completing the rulemaking directives set forth in the CPRA.

December 19: The FTC announced a "record-breaking settlement with Fortnite owner Epic Games" — $275 million — for alleged violations of the Children's Online Privacy Protection Act ("COPPA"), as well as a second significant settlement — $245 million — related to allegations that Epic was using so-called "dark patterns" that "dupe[d] millions of Fortnite players into making unintentional purchases." The FTC's action highlighted two priorities of Chair Lina Khan: children's privacy and the use of dark patterns.

December 27: The transition period to implement the new EU Standard Contractual Clauses ("SCCs") expired. The European Commission issued the new SCCs in June 2021, requiring companies to update the SCCs for already-executed contracts within 18 months (provided that processing operations remained unchanged during that period).



CURRENT LAWS AND GUIDANCE GOVERNING BIOMETRIC INFORMATION AND ARTIFICIAL INTELLIGENCE TECHNOLOGIES

U.S. and multinational businesses are increasingly offering products and services, including virtual reality and other interactive platforms, based on cutting-edge algorithmic technologies that may incorporate or use significant amounts of biometric information. These new offerings present novel questions about how companies may innovate in this space while meeting their regulatory and compliance obligations. For the moment, significant gaps persist in the legal and regulatory regimes governing the use of such data, but rules and standards are beginning to emerge to address the incorporation of biometric information into artificial intelligence ("AI"), and a variety of federal, state and non-U.S. regulators are focusing on these issues. Given the ambiguity in the current legal landscape, however, companies working on the cutting edge of innovation would be wise to monitor the existing and emerging rules at the intersection of biometric information and artificial intelligence.

Biometric Privacy

Like most of U.S. privacy law, biometric privacy is governed by a patchwork of state and federal rules. No federal law is in force that specifically governs the collection, use, or sharing of biometric information or biometric identifiers by private entities. Instead, the Federal Trade Commission ("FTC") has issued guidance, backed by its enforcement authority under Section 5 of the FTC Act, to set standards for biometric privacy practices undertaken by private entities. Several states have stepped into the void to enact their own biometric privacy laws, most notably in Illinois, as well as to address biometric privacy in comprehensive laws. In addition, a number of state legislatures are currently considering biometric-specific laws or general privacy laws that mimic certain aspects of existing state-level laws.

Federal Guidance and Enforcement

Section 5 of the FTC Act prohibits businesses from engaging in "unfair or deceptive acts or practices."[1] In the absence of a federal law specifically addressing biometric privacy, the FTC has used this broad consumer protection authority in a number of ways. First, the FTC set forth its expectations for businesses' use of facial recognition technologies — a particularly sensitive use of biometric information — in a 2012

1 5 U.S.C. § (a)(1).

report titled "Facing the Facts: Best Practices for Common Uses of Facial Recognition Technologies."[2]

The FTC put this guidance into action in May 2021 when it approved a settlement with Everalbum, Inc. ("Everalbum"), a photo app developer. The FTC alleged that Everalbum automatically enabled a facial recognition feature for every user (outside of a small number of states), which could not be disabled despite promises to the contrary, and ignored FTC guidance to obtain affirmative consent and to allow users to turn off data collection.[3] Everalbum then used the data it collected to train its own commercial facial recognition software; the company also failed to delete users' photos after account deletion, despite having explicitly stated that it would do so.[4]

In addition to more standard requirements found in most FTC consent orders (e.g., to refrain from misrepresenting its practices), the FTC's Everalbum settlement also required the company to provide a transparent description of the purposes for which it uses biometric information and to obtain affirmative consent to use such information, consistent with the FTC's 2012 guidance.[5] Perhaps most importantly, Everalbum was required to delete both the data it obtained without consumers' express consent and the data it retained from users who deleted their accounts, *as well as any models or algorithms developed using such data*.[6]

This sanction, if indicative of the FTC's ongoing approach to biometric privacy, could have a significant negative impact on companies found to have improperly collected and processed biometric data.

State Laws Governing Biometric Information

Several states have enacted their own laws regulating the use of biometric information. These laws take one of two forms: (1) biometric-specific laws (enacted in Illinois, Texas, and Washington); or (2) general privacy laws that expressly incorporate biometric information within the scope of personal data governed by the laws (enacted in California, Colorado, Connecticut, Utah, and Virginia).

Each of the biometric-specific state laws in Illinois, Texas, and Washington requires covered businesses to disclose to individuals that their biometric information is being collected, specify the purposes for such collection and the retention period for such information, and obtain the individual's affirmative consent for such collection. However, there are some key provisions that distinguish Illinois' law and make Illinois a significantly riskier jurisdiction in which to collect biometric information than either Texas or Washington:

- Illinois Biometric Information Privacy Act ("BIPA"). BIPA is the best known biometric privacy law because it provides a private right of action with significant statutory damages that has frequently been leveraged by the plaintiffs' bar. BIPA also differs significantly from the Texas and Washington laws in its general prohibition on private entities selling, leasing, trading, or "otherwise profiting from" biometric information/identifiers.[7] The context, structure, and wording of the "profiting" provision suggest that it is focused on activities involving the transfer of covered data to third parties in exchange for monetary consideration, but the language is sufficiently broad, and the provision sufficiently unclear, that a court could readily find that it prohibits *any form of profit* from the use of biometric information/identifiers.[8]

2 Fed. Trade Comm'n, Facing the Facts: Best Practices for Common Uses of Facial Recognition Technologies, available here.

3 *See* Fed. Trade Comm'n, Press Release, "California Company Settles FTC Allegations It Deceived Consumers About Use of Facial Recognition in Photo Storage App" (May 7, 2021), available here.

4 *Id.*

5 *Id.* at 4.

6 *Id.* at 4-5.

7 740 ILCS 14/20, 14/15(c).

8 *Cf. Vance v. Microsoft Corp.*, 534 F. Supp. 3d 1301, 1307 (W.D. Wash. 2021) (describing the legislative intent behind BIPA § 15(c) as "prohibiting a market in the transfer of biometric data, whether through a direct exchange—sale, lease or trade—or some other transaction where the product is comprised of biometric data" and noting that "BIPA, and § 15(c) in particular, aims to "eliminate the incentive" behind marketing biometric data").

- Texas Capture or Use of Biometric Information ("CUBI"). While BIPA includes an outright prohibition on selling, leasing, etc., biometric identifiers, CUBI prohibits such activities only if the company has not obtained consent to do so. Importantly, CUBI does not provide a private right of action, and is enforceable only by the Texas Attorney General, whose office has recently filed its first action under the law.[9]

- Washington Biometric Identifiers Law. Washington's biometric identifiers law is distinct insofar as it applies only in the narrow context of the collection of biometric identifiers for the purpose of selling or disclosing that information to a third party for a new purpose. Like CUBI, the Washington law is only enforceable by the state attorney general.

Of the five states which have enacted general privacy laws that expressly cover biometrics, only two are currently in effect: the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"), and the Virginia Consumer Data Protection Act ("VCDPA"). New laws in Colorado,[10] Connecticut,[11] and Utah[12] will come into effect later this year. Accordingly, businesses that collect, process, disclose, or otherwise use biometric information in any of these states must, by mid-2023, do so in compliance with each of these laws. Helpfully, these laws all tend to regulate the use of biometric information in similar ways, and each treats biometric information as "sensitive," requiring notice and affirmative consent for the collection, use, and disclosure of biometric information. There are, however, some important differences. For example, Colorado, Virginia, and Connecticut will require companies that collect biometric information and other sensitive information to conduct a data protection assessment to ensure that the purposes of the activity justify that data collection.[13]

The Future of Biometric Regulation

Given the significant interest in, and important concerns raised by, the collection and use of biometric information, it is not surprising that members of Congress and state legislators have undertaken efforts to pass legislation that would regulate the use of such information. Although 2023 legislative sessions have just begun, two state legislatures have already introduced biometric privacy bills and we expect more will follow.[14] Whether any of these bills will become law remains to be seen, but biometric privacy is now squarely in legislators' sights.

AI and Automated Decision-Making Technologies

The regulatory landscape in the United States governing AI and Automated Decision-Making ("ADM") technologies is similar to that governing biometric information, although in many ways it is even less developed. There is no federal data protection law governing the use of AI or ADM, although there is some federal regulatory guidance.

Unlike biometric privacy, there are no AI-specific laws at the state level. Instead, the legal regimes governing AI and ADM at the state level are general privacy laws that impose restrictions and obligations on companies related to the collection, use, and sharing of personal information. For instance, recently enacted laws in Virginia, Colorado, and Connecticut grant consumers the right to opt out of certain ADM activities (such as profiling) performed by businesses, although the definitions and scope differ among the states.

9 Tex. Att'y Gen., Press Release, "Paxton Sues Google for its Unauthorized Capture and Use of Biometric Data and Violation of Texans' Privacy" (Oct. 20, 2022).

10 Colorado Privacy Act, S.B. 21-190, Gen. Assemb., 2021 Sess. (Colo. 2021) (hereinafter "CPA").

11 Connecticut Data Privacy Act, S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022) (hereinafter "CTDPA").

12 Utah Consumer Privacy Act, S.B. 227 Gen. Assemb., Gen. Sess. (Utah 2022) (hereinafter "UCPA").

13 These requirements are in addition to the other requirements of these laws that apply generally to any covered personal information, such as with respect to the reach and limitations of any consumer rights to request deletion of, access to, etc., their personal information held by a company. *See, e.g.*, VCDPA § 59.1-576(4).

14 H.B. 0033, 2023 Reg. Sess. (Md. 2023); H.B. 467, 2023 Reg. Sess. (Miss.).

Federal Guidance

FTC Guidance[15]

In the past few years, the FTC has signaled through guidance, blog posts, and public statements an increased focus on algorithmic and discriminatory bias in AI and ADM systems.[16] In particular, the FTC has focused on the extent to which the development and/or use of AI or ADM results in unfair or discriminatory impacts on consumers. FTC guidance strongly suggests that the FTC expects companies to ensure that both the inputs and outcomes of their algorithmic, automated decisions are non-discriminatory, and the FTC has indicated that investigating allegations of algorithmic bias will be among its priorities.[17]

Generally, the FTC has emphasized that the use of AI tools should be "transparent, explainable, fair, and empirically sound, while fostering accountability."[18] These principles should serve as guideposts for a business' design and deployment of AI systems and other ADM technologies.

Biden Administration

In mid-2021, the Biden Administration launched the National AI Research Resource Task Force[19] and in October 2022, the White House Office of Science and Technology Policy ("OSTP") issued a blueprint for an "AI Bill of Rights."[20] The AI Bill of Rights includes the rights to: (a) know when and how AI is influencing a decision that affects civil liberties; (b) be subject to AI that has been carefully audited to ensure the accuracy and sufficiency of the data; (c) be free from pervasive or discriminatory surveillance and monitoring; and (d) meaningful recourse if an algorithm causes harm.[21] To enforce these rights, OSTP officials have suggested — although no formal mechanism is yet in place — that executive agencies either be prohibited from buying software/technology products that fail to respect these rights, or otherwise be required to purchase technologies from vendors that affirmatively adhere to the AI Bill of Rights.[22]

State Laws and Guidance

At the state level, no AI-specific laws are currently in force, but some comprehensive state privacy laws — such as the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA") — generally implicate the use of personal information in AI and ADM processes. As these laws come into force and state regulators promulgate regulations, the rules and norms concerning AI and ADM systems will likely take shape.

California

The CPRA amendments to the CCPA include provisions relating to the automated processing of personal information.[23] To clarify the scope of these provisions, the CPRA directs the California Privacy Protection Agency ("CPPA") to promulgate rules and regulations to govern consumers' access and opt-out rights with respect to a business' use of ADM and the "meaningful logic" involved in the decision-making process,[24] and to require that businesses conduct, and submit to the CPPA, risk assessments with respect to such processing activities. Although the CPRA took effect at the first of this year, the CPPA's rulemaking process remains a work in progress. Once finalized, these regulations are expected to clarify the legal obligations around automated processing for companies subject to the CCPA.

Further, guidance from the California Attorney General highlights the complexity of regulating AI and ADM. Guidance issued in March 2022 addresses "inferences"

15 In addition to the guidance, blog posts, and public statements addressed in this section, we would also note that the FTC "is considering initiating a rulemaking under section 18 of the FTC Act to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination." However, there are no further details at this time. *See* Office of Information & Regulatory Affairs, OMB, available here (last accessed July 5, 2022).

16 *See, e.g.*, Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC Business Blog (Apr. 19, 2021), available here.

17 *FTC Streamlines Consumer Protection and Competition Investigations in Eight Key Enforcement Areas to Enable Higher Caseload,* Fed. Trade Comm'n (Sept.14, 2021), available here.

18 *See* Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC Business Blog (Apr. 8, 2020), available here.

19 *The Biden Administration Launches the National Intelligence Research Resource Task Force*, The White House (June 10, 2021), available here.

20 *The Biden Plan to Build Back Better by Advancing Racial Equity Across the American Economy,* Joebiden.com, available here.

21 *Americans Need a Bill of Rights for an AI-Powered World*, The White House (Oct. 22, 2021), available here.

22 *Id.*

23 Cal. Civ. Code § 1798.140(z).

24 Cal. Civ. Code § 1798.185(a)(16).

drawn about individuals using automated systems, and advises that, while an algorithm itself may be a trade secret, the CCPA requires a business to treat the product of the algorithm (e.g., an inference about a consumer) as personal information, which must be disclosed to the consumer upon request.[25] This guidance demonstrates the difficulty of balancing consumers' privacy rights against the technological and practical challenges of separating discrete personal information from an algorithm and identifying any inferences drawn using AI. Determining where to draw this line may present significant operational issues for AI developers.

Virginia

The VCDPA, which also took effect on January 1, 2023, allows consumers to opt out of a business' use of their personal data for profiling purposes, but this right is limited only to instances "that produce legal or similarly significant effects concerning a consumer."[26] Unwinding how and in which contexts profiling is used for specific decision making (and to what effect) will likely be a highly fact-specific effort.

Unlike in California, data controllers subject to the VCDPA must prepare data protection assessments for any processing activities involving profiling, or which present a heightened risk of unfair or deceptive treatment, unlawful disparate impact on, or any physical, financial, or reputational injury (including intrusion into private affairs) to consumers.[27] These assessments must be performed prior to any processing, and should identify and weigh any benefits of that processing against any risks posed to consumers, which should include the "reasonable expectations of consumers."[28]

Conclusion

Moving forward, we expect to see a renewed focus on both biometric privacy and AI/ADM technologies from federal and state legislators and regulators. Legislation at the federal level, in particular, has gained some traction, but in the current political context, it is unclear whether any of these efforts will bear fruit. At the state level, new comprehensive privacy bills, and bills targeted specifically at biometric privacy, have already been introduced in 2023 and, if passed, will likely create new areas of inconsistency, requirements, and complexities. In addition, foreign jurisdictions, including the European Union, have proposed AI-specific legislation to address the proliferation of the development of AI systems. While emerging algorithmic technologies, and virtual or augmented reality that leverages biometric data present exciting new commercial opportunities, those offerings will not be immune from old-fashioned regulation and compliance obligations.

25 *Op. of Cal. Att'y Gen.*, No. 20-303 (Mar. 10, 2022).

26 VCDPA § 59.1-573(5).

27 *Id.* § 59.1-576(3).

28 *zId.* § 59.1-576(5)(B).

DEVELOPMENTS IN CHILDREN'S AND TEENS' PRIVACY IN 2022

As the pandemic and the ubiquity of social media have pushed many children and teens to live much of their lives online, regulators and legislators have increasingly turned their attention to protecting children's privacy. President Joseph Biden underscored this priority in his 2022 State of the Union address, stating "it's time to . . . demand tech companies stop collecting personal data on our children."[1] That declaration presaged a year of major efforts to improve children's and teens' privacy in the United States through methods including increased FTC enforcement, new state laws, and proposed federal legislation, as well as a major legislative effort in the United Kingdom. As these laws, legislative efforts and enforcement actions demonstrate, regulating content that is "likely to be accessed by children" is inherently complex because it involves developing and implementing age verification procedures, designing parental consent standards, and determining which content should be considered "harmful" in a way that is consistent with the First Amendment — in addition to deciding what sites and types of content are "likely to be accessed by children."

1 Joseph R. Biden Jr., *Remarks of President Joe Biden – State of the Union Address As Prepared for Delivery* (Mar. 1, 2022), available here.

Federal Actions

FTC Actions

In 2022, the Federal Trade Commission ("FTC"), led by Chair Lina Khan, focused on improving children's online privacy and safety through active enforcement of the Children's Online Privacy Protection Act ("COPPA").[2] In May 2022, the FTC released a policy statement that underscored its intent to vigorously enforce COPPA, especially with respect to education technology designed for schools[3] and emphasized that it will "scrutinize compliance with the full breadth of the substantive prohibitions and requirements" of the law[4] — an effort its actions in 2022 underscored, and which we can expect to see in future enforcement and regulatory action undertaken by the FTC.

In March 2022, the FTC reached a settlement with WW International, Inc. and its subsidiary Kurbo, Inc. ("Weight Watchers") after alleging that Weight Watchers had failed to

2 Children's Online Privacy Protection Act, 5 U.S.C. § 6501 *et seq.*

3 *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act*, Federal Trade Commission, available here (last accessed Jan. 19, 2023).

4 *Id.*

obtain parental consent prior to collecting personal health information from children under the age of 13 through an app that tracked food intake, activity, weight, birthdates, and other personal information.[5] The settlement requires Weight Watchers to pay a $1.5 million civil fine and to destroy all personal information previously collected from children in violation of COPPA and all work product created from such personal information, unless Weight Watchers obtained subsequent parental consent to retain such personal information.[6]

In December 2022, the FTC announced a "record-breaking settlement" of $520 million with Epic Games, the creator of the popular game, Fortnite.[7] The FTC alleged, in part, that Epic Games violated COPPA by operating a website directed to children under the age of 13 that collected information from children without parental consent, and by enabling in-game chat features by default. The FTC alleged that these features caused a risk of harm to children, including online bullying. Unrelated to COPPA, the FTC also alleged that Epic Games was using so-called "dark patterns" that "dupe[d] millions of [Fortnite] players into making unintentional purchases."[8]

These actions are a clear signal by a resurgent FTC intent on using its authority, in the absence of new federal legislation, to "closely scrutinize" providers of online services to children.

Proposed Congressional Updates to U.S. Federal Children's Privacy Law

Congress has also recently attempted to amend federal children's privacy laws, although those efforts have been unsuccessful. Two bills, one that would have amended and expanded COPPA and another that would have created an additional children's privacy law, were reported out of the U.S. Senate Committee on Commerce, Science, and Transportation on December 25, 2022, but neither bill passed prior to the end of the 117th Congress.[9]

The Children and Teens' Online Privacy Protection Act ("CTOPPA") was introduced by Senator Edward Markey on May 13, 2021. CTOPPA proposed expanding the group covered by COPPA's protections to "minors" — defined as individuals aged 13 through 16 years old — and "children" — defined as individuals age 12 and younger, and the bill also would have included in its scope operators of general audience websites and online services "reasonably likely to be used by children or minors" if they collect, use, or disclose personal information from children or minors.

The Kids Online Safety Act ("KOSA") was introduced by Senator Richard Blumenthal on February 16, 2022. Among other things, KOSA would have assigned a duty of care to covered platforms to "act in the best interests of a minor that uses the platform's products or services" and to take reasonable measures to prevent and mitigate potential harm to minors, including limiting compulsive usage of the platform and allowing users to opt out of algorithmic recommendation systems that use minors' personal information.

State Actions

California Age-Appropriate Design Code Act

On September 15, 2022, California Governor Gavin Newsom signed into law the California Age-Appropriate Design Code Act ("Design Code Act"),[10] which is closely modeled on a similar set of principles developed by the UK Information Commissioner's Office ("ICO") in 2021. The Design Code Act, which will take effect July 1, 2024, is intended to protect children's privacy online, but represents a considerable — and potentially burdensome — shift from existing federal requirements under COPPA. In light of these concerns, a trade group, NetChoice, which includes a number of prominent Internet and social media companies among its

5 *United States v. Kurbo Inc. and WW International, Inc.*, 3:22-cv-00946-TSH (N.D. Ca. Mar. 3, 2022), available here.

6 *Kurbo Inc. and WW International, Inc.*, 3:22-cv-00946-TSH, at 7-9.

7 *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges*, Federal Trade Commission (Dec. 19, 2022), available here.

8 *Id.*

9 S.3663, "Kids Online Safety Act," available here; S.1628, "Children and Teens' Online Privacy Protection Act," available here.

10 Assembly Bill No. 2273, "The California Age-Appropriate Design Code Act," available here.

members, has already filed a lawsuit challenging the Design Code Act on First Amendment grounds.[11]

Scope

The Design Code Act applies to businesses that provide an online service, product, or feature "likely to be accessed by children" under the age of 18 (a "Covered Business"). An online service is "likely to be accessed by children" if:

- it is "directed to children," as defined by COPPA;[12]
- it is routinely accessed by a significant number of children or is substantially similar to an online service, product, or feature routinely accessed by a significant number of children;
- it has advertisements marketed to children; or
- internal company research determines that children make up a significant portion of the audience.

Although these criteria are intended to limit the Design Code Act's applicability to websites most likely to be accessed by children, some of the standards — such as sites "routinely accessed by a significant number of children" — are so vague as to arguably include most major websites. For that reason, companies not previously subject to COPPA or other laws concerning children's activities online may now need to make significant changes to the structure of their online services and products to comply with the Design Code Act. Moreover, several of the obligations imposed by the Design Code Act on Covered Businesses may be intended to protect children's privacy but in practice have a cumulative anti-privacy — and perhaps unconstitutional — effect because they either require increased collection of consumers' data, or limit the content, features and functionality available to adult users.

Prohibited Activities

In addition to imposing the obligations described above, the Design Code Act also prohibits certain practices. For example, Covered Businesses are prohibited from using a child's personal information for any reason other than that for which it was collected, and from collecting, selling, or sharing any precise geolocation information regarding a child. Many of the Design Code Act's prohibitions include an exemption if there is a "compelling reason" that the use of the information is in the best interests of the child. However, Covered Businesses are prohibited from using a child's personal information in any way known or believed to be "materially detrimental" to a child's physical or mental health and well-being.

Enforcement

The Design Code Act is enforceable only by California's Attorney General, who may seek an injunction or civil penalty against any business that violates the Design Code Act up to $2,500 per affected child for each negligent violation, and up to $7,500 per affected child for each intentional violation. Before an enforcement action may be brought, the Design Code Act provides a 90-day cure period for Covered Businesses that substantially comply with the Design Code Act.

Problematic Aspects of the Design Code of Act

The Design Code Act presents a number of issues that will make both compliance and enforcement challenging. Provisions of the Design Code Act, including the threshold standard for covered entities that are "routinely accessed by a significant number of children," are broad enough to cover a large number of websites.

Additionally, age verification requirements could adversely impact the privacy of all users because Covered Businesses will likely need to collect more information from users than they otherwise would. For example, one prominent social media site implemented age verification in June 2022. Users who had entered an age under 18 were required to verify their age by (a) uploading a picture of their government-issued ID, (b) uploading a "video selfie" which would be analyzed by a third-party facial analysis technology company, or (c) ask three adult users to confirm the user's age. Because of the Design Code Act, other websites may implement similarly intrusive procedures to ensure that the website accurately verifies a user's age.

11 Cat Zakrzewski, *Tech Industry Group Sues to Block California Children's Safety Law*, Washington Post (Dec. 14, 2022), available here.

12 Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 *et seq.*

Copycat and Similar Legislation

Following the enactment of the Design Code Act, other states have recently introduced similar and not-so-similar bills with similar goals. As to the former, New Jersey and New York introduced Assembly Bill NJ A4919[13] and Senate Bill S9563,[14] respectively. These bills are modeled on California's law and include provisions intended to protect children's privacy by limiting the collection of personal information of a child.

As to the latter, Louisiana's Act 440 requires adult-content websites to screen website visitors using reasonable age verification, including reviewing government-issued identification.[15] The law prohibits companies from retaining information used for age verification purposes,[16] but the collection of this information in the first instance raises privacy concerns. While Act 440 is more limited in scope than the Design Code Act, it provides an additional indication that states are increasingly willing to mandate children's privacy protections, even if doing so means (counterintuitively) collecting additional personal information from all users, regardless of age.

NetChoice Lawsuit

On December 14, 2022, NetChoice sued to block the Design Code Act.[17] In its complaint, NetChoice argued that social media companies and tech companies have a First Amendment right to make "editorial decisions" about the content they publish and remove, but that the Design Code Act would require these companies to engage in "over-moderation" of the content on their platforms "to avoid the law's penalties for content the State deems harmful."[18] NetChoice also agrued that the Design Code Act is preempted by COPPA.[19] NetChoice alleged that the Design Code Act undermines user privacy because companies are required to track and store information to identify which users are children. The NetChoice lawsuit suggests that providers of social media and other popular websites will continue to push back against states' efforts to limit their platforms.

13 New Jersey Assembly Bill 4919, available here.

14 New York Senate Bill S9563, available here.

15 Act 440, available here. In December of 2022, Senator Mike Lee of Utah introduced a similar bill in Congress that would require adult websites to conduct age verification. See Shielding Children's Retinas from Egregious Exposure on the Net Act, available here.

16 *Id.*

17 Complaint, *NetChoice, LLC v. Bonta*, 5:22-cv-08861 (N.D. Ca. Dec. 14, 2022), available here.

18 *Id.*

19 *Id.*

United Kingdom Online Safety Bill

In the year since the Age Appropriate Design Code ("AADC") came into force in the UK, the ICO and the government have been pushing for increased transparency requirements and enforcement actions directed at businesses handling children's data. In particular, Parliament has been debating a significant piece of legislation, the Online Safety Bill ("OSB"),[20] which would establish a new regulatory regime to protect both children and adult users from illegal and "harmful" content available online. In response to criticism — not unlike that leveled against the Design Code Act — about the draft's unclear language and potential unintended consequences, the OSB has already been amended and is likely to undergo further changes before it takes its final form.

Organizations and Services in Scope

If the bill becomes law in its present form, the OSB will apply to providers of user-to-user services (such as social media sites)[21] and search services (e.g., search engines). Importantly, the OSB has extra-territorial application, so a service may fall within its scope even if it is not based in, but "has links with," the UK.[22] A service "has links with" the UK if:

- it has a significant number of users in the UK ("significant" is not defined in this context);
- UK users are targeted by the service; or
- it is capable of being used by individuals in the UK *and* "there are reasonable grounds to believe that there is a material risk of significant harm to individuals" in the

20 Bill 220 2022-23, "*Online Safety Bill*," available here.

21 *Id.*, at Part 2 (2)(1)(defining user-to-user services as "an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service").

22 *Id.*, at Part 2 (3)(6).

UK presented by the content present on the service or search content of the service.[23]

Duties for Services Likely to Be Accessed by Children

The OSB introduces specific duties designed to protect children from user-to-user services "likely to be accessed by children" such as:

- mitigating the risk of harm to children in different age groups;
- removing illegal content, including child sexual abuse and terrorist content;
- enforcing age limits and age verification measures;
- ensuring the risks and dangers posed to children on the largest social media platforms are more transparent, including by publishing risk assessments; and
- providing parents and children with clear and accessible ways to report problems online.

Similarly to the AADC, the initial draft of the OSB does not clearly identify the scope of online services that are "likely to be accessed by children." As a result, the OSB leaves user-to-user services with different interpretations of what "likely to be accessed by children" means in practice.[24]

Enforcement

The OSB authorizes the UK's communications regulator, the Office of Communications ("Ofcom"), to enforce the new law. Ofcom may seek the following sanctions:

- Fines of up to £18 million, or 10% of a provider's annual global revenue, whichever is highest;
- A court order to disrupt the activities of non-compliant providers (or to block access to their services altogether); or
- Criminal action against named senior managers whose companies do not comply with Ofcom's requests for information.

Conclusion

Children's and teens' privacy remains a high priority for U.S. and UK government regulators as this group is increasingly active online. With the success of legislative efforts in California culminating in the Design Code Act, several states have already introduced copycat bills, and it appears more states are likely to introduce children's privacy legislation in 2023. Companies should take steps now to determine whether their data collection activities may implicate these laws and to incorporate practices that affirmatively protect children's privacy.

23 *Id.*, at Part 2 (2)(6). The OSB does not define which type of content may present "significant harm to individuals" but the Online Harm White Paper published by the UK Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department provides additional information defining harm as a "reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals." *See* UK Government Department for Digital, Culture, Media and Sport, *Online Harms White Paper: Full Government Response to the Consultation* at 24 (2020).

24 *See Id.*, at Part 3, 32. The OSB generally provides that a service is "likely to be accessed by children" if "a children's access assessment carried out by the provider of the service concludes that – (a) it is possible for children to access the service or a part of it, and (b) the child user condition is met in relation to – (i) the service, or (ii) a part of the service that is possible for children to access."

HOPE AND UNCERTAINTY FOR TRANS-ATLANTIC DATA FLOWS

On December 13, 2022, the European Commission ("EC") published a draft adequacy decision on the new Trans-Atlantic Data Privacy Framework (the "Data Privacy Framework").[1] The goal of the Data Privacy Framework is to "restore an important legal basis for transatlantic data flow" by addressing the concerns raised by the Court of Justice of the European Union ("CJEU").[2] Publishing the Draft Adequacy Decision is an important step towards finalizing the significant work by representatives of the European Union ("EU") and the United States ("U.S."). Once the draft is finalized, the Data Privacy Framework should become a useful option for companies that transfer personal data from the European Economic Area ("EEA") to the U.S., although uncertainty about it's long-term viability will remain, given the likelihood of legal challenges.

Background

The EU General Data Protection Regulation ("GDPR") governs the processing of personal data of natural persons in the EU.[3] GDPR restricts the transfer of personal data to jurisdictions outside the EEA, including to the U.S., unless the data transfer is made through certain mechanisms specified in the GDPR and approved by the EC, such as adequacy decisions, standard contractual clauses ("SCCs"), or binding corporate rules ("BCRs"). As set forth in GDPR Article 45, an adequacy decision memorializes the EC's determination that the applicable legal regime in a particular third country offers a level of data protection that is "adequate" to protect EU data subjects' privacy interests.

The back and forth over data transfers from the EEA to the U.S. has been ongoing for almost a decade. Prior to July 2020, an EC adequacy decision permitted companies to use the EU-U.S. Privacy Shield Framework ("Privacy Shield") to transfer personal data from the EEA to the U.S.[4] Privacy Shield was itself

1 *See* European Commission, "Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework" (December 13, 2022), available here ("Draft Adequacy Decision").

2 *See* Press Release, The White House, "FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework" (October 7, 2022), available here ("White House Fact Sheet").

3 *See* REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (General Data Protection Regulation) (April 27, 2016), available here.

4 *See* European Commission, Decision 2016/1250/EC (July 12, 2016), available here. *See also* Privacy Shield Framework "Key New Requirements – EU-U.S. Privacy Shield Framework – Key New Requirements for Participating Companies" available here.

a response to a 2015 CJEU decision that struck down the longstanding, pre-GDPR EU-U.S. Safe Harbor Framework.[5] Under Privacy Shield, companies subject to the jurisdiction of the Federal Trade Commission could self-certify (and re-certify annually) compliance with Privacy Shield — failure to abide by the requirements of Privacy Shield would constitute an unfair and deceptive practice and subject the company to potential FTC enforcement action. In addition, Privacy Shield included a number of mechanisms — such as an ombudsperson to whom individuals could bring complaints — intended to address concerns raised about the potential for EU data subjects' personal data to be swept up in U.S. intelligence gathering activities. But in July 2020, the CJEU invalidated Privacy Shield, holding that the EC was wrong to conclude that U.S. surveillance laws, even with the protections set forth in Privacy Shield, adequately protected the personal data of EU data subjects.[6] Since that decision, companies that need to transfer personal data from the EEA to the U.S. have had to use other mechanisms — principally, the SCCs — to legitimize those personal data transfers.

2022 Developments—A New Data Privacy Framework

On March 25, 2022, after more than a year of negotiations, U.S. and EC officials announced an agreement "in principle" to replace the invalidated Privacy Shield with the Data Privacy Framework. In particular, the U.S. announced that it would establish new protections and redress mechanisms to address the concerns raised by the CJEU.[7] These protections would include, among other things, new safeguards to ensure that U.S. government surveillance activities are both necessary and proportionate in the pursuit of defined national security objectives, and an independent redress mechanism with binding authority to direct remedial measures. Notably for private companies considering whether to use this new Framework, Commerce Secretary Raimondo explained that the Framework would "update the privacy principles that companies adhere to under the Privacy Shield Framework and rename them as the EU-U.S. Data Privacy Framework Principles."[8]

Adoption and Implementation of Executive Order 14086

The next major step toward implementing U.S. commitments under the Data Privacy Framework came on October 7, 2022, when the White House issued Executive Order 14086, Enhancing Safeguards for Signals Intelligence Activities (the "EO").[9] Among other things, the EO directs relevant agencies throughout the U.S. government to establish the safeguards and redress mechanisms first identified in the March 2022 announcement.

In particular, the multi-layer review mechanism would be comprised of an initial review of any qualifying complaint by the Civil Liberties Protection Officer, a position that already exists within the Office of the Director of National Intelligence ("ODNI"), followed by a subsequent, independent review by a new Data Protection Review Court ("DPRC") to be established by the U.S. Attorney General in the Department of Justice. Shortly after the EO was released, the Attorney General issued Department of Justice regulations establishing the DPRC.[10] The ODNI followed that by releasing Intelligence Community Directive 126, "Implementation Procedures for the Signals Intelligence Redress Mechanism under Executive Order 14086," to clarify the process by which qualifying complaints would be handled.[11]

5 *See Maximillian Schrems v Data Protection Commissioner*, Case C-362/14 (Oct. 6, 2015), available here. Our discussion here focuses on the invalidation of Privacy Shield and efforts to develop a post-Privacy Shield framework, but the fact that CJEU already has struck down two efforts at addressing the issue of transatlantic data flows highlights the obstacles policymakers face in developing a framework that will survive judicial scrutiny.

6 *See Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Case C-311/18 (July 16, 2020), available here.

7 *See* Press Release, The White House, "United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework" (March 25, 2022), available here.

8 *See* Press Release, Department of Commerce, "Statement from U.S. Secretary of Commerce Gina Raimondo on Enhancing Safeguards for United States Signals Intelligence Activities Executive Order" (October 7, 2022), available here.

9 *See* Exec. Order No. 14086, 87 Fed. Reg. 62,283 "Enhancing Safeguards for United States Signals Intelligence Activities" (October 7, 2022), available here.

10 *See* The United States Department of Justice, Office of Privacy and Civil Liberties, "Redress in the Data Protection Review Court" (October 20, 2022), available here.

11 Office for the Director of National Intelligence, Intelligence Community Directive 26, "Implementation Procedures for the Signals Intelligence Redress Mechanism under Executive Order 14086" (December 14, 2022), available here.

Draft Adequacy Decision

On the European side of the Atlantic, the Draft Adequacy Decision is the next step towards ultimate adoption of the Data Privacy Framework as a mechanism to legitimize transfers of personal data from the EEA to the U.S. According to the EC, the Draft Adequacy Decision reflects an "in-depth assessment of the Data Privacy Framework, including the limitations and safeguards on access by U.S. public authorities to data transferred to the U.S. for criminal law enforcement and national security purposes."[12] The Draft Adequacy Decision reviews the Data Privacy Framework principles to which companies would be required to self-certify, but focuses primarily on the steps taken in the EO to address the concerns of the CJEU and finds that access to EU data subject personal data by U.S. intelligence agencies will be limited to what is necessary and proportionate to protect national security and that EU individuals will have the ability to obtain independent and impartial redress before the newly created DPRC. Therefore, it concludes that the new Framework ensures an adequate level of protection for EU data subject personal data transferred from the EEA to the U.S.[13] In a press release announcing the Draft Adequacy Decision, European Commissioner for Justice Didier Reynders stated that "our analysis has showed that strong safeguards are now in place in the U.S. to allow the safe transfers of personal data between the two sides of the Atlantic," and the "[F]ramework will help protect the citizens' privacy, while providing legal certainty for businesses."[14]

Next Steps and Expected Challenges

The Draft Adequacy Decision must now go through an adoption process that incorporates the opinions of other EU regulators, including the European Data Protection Board[15] and a committee of EU Member State representatives.[16] This process is expected to take approximately six months.

Even if the Draft Adequacy Decision is finalized, that will almost certainly not be the end of the matter. Both privacy advocates and EU data protection authorities ("DPAs") have expressed criticism of the EO, highlighting concerns regarding the differences between the EU and U.S. regimes and their overarching privacy values.[17] The Draft Adequacy Decision tries to preempt these arguments by noting that "adequacy does not require a third country's data protection system to be identical to the EU, but is based on the concept of essential equivalence between the two standards." Nevertheless, statements from organizations like data watchdog group None of Your Business[18] and the Electronic Privacy Information Center[19] strongly suggest that a challenge to this latest effort is likely to find its way to the CJEU.

What's Next?

While all of this activity has taken place between the EU and the U.S., negotiations continue between representatives of the United Kingdom ("UK") and the U.S. Department of Commerce on a draft UK-U.S. adequacy agreement.[20] The two governments have indicated in public statements that negotiations have accelerated, and that the UK government — including the Information Commissioner's Office — is in the process of reviewing the enhanced safeguards and redress mechanism set forth in the EO. Although no official timeline has been provided, many expect action on this front in early 2023.

12 *See* Press Release, European Commission, "Questions and Answers: EU-U.S. Data Privacy Framework, draft adequacy decision" (December 13, 2022), here.

13 *See Draft Adequacy Decision, supra* n.1.

14 *See*Press Release, Data Protection: Commission starts process to adopt adequacy decision for safe data flows with the U.S. (December 13, 2022), available here.

15 *See* Press Release, European Commission, "Questions & Answers: EU-U.S. Data Privacy Framework" (October 7, 2022), available here.

16 *See* International Association of Privacy Professionals, "From Privacy Shield to the Trans-Atlantic Data Privacy Framework" (April 2022), available here ("The approval required 55% of EU countries (15 out of 27) representing at least 65% of the total EU population; the blocking minority must include at least four council members representing more than 35% of the EU population.").

17 For example, a German DPA commissioner from Baden-Wurttemberg stated that while the EO is "an important step in the right direction," there is "considerable legal ambiguity" that exists. *See* John Bethan, et al., Global Data Review, "German regulator and MEP slam U.S. Executive Order" (October 26, 2022), available here.

18 Press Release, None of Your Business, "First Reaction: Executive Order on U.S. Surveillance unlikely to satisfy EU law" (October 7, 2022), available here.

19 *See* Press Release, Electronic Privacy Information Center, "European Commission Publishes Draft Adequacy Decision of EU-U.S. Data Privacy Framework" (December 13, 2022), available here.

20 *See* Press Release, Department for Digital, Culture, Media, and Sport and the Foreign, Commonwealth & Development Office, "UK and U.S. meet to make positive progress on data and tech" (October 7, 2022), available here.

Given the uncertainty over the future of the Data Privacy Framework — both with respect to whether it is ultimately adopted and to whether it will survive any legal challenges — there will be significant incentives for companies that are already using other mechanisms, such as BCRs or the SCCs, to maintain that approach. But some companies may find that transitioning to the new Framework may be beneficial despite the uncertainties. As a result, companies that transfer personal data from the EEA (or the UK) to the U.S. will want to closely monitor developments over the course of 2023 to make smart decisions about what approach will work best for their business.

SIGNIFICANT DEVELOPMENTS IN THE GLOBAL DATA PROTECTION LANDSCAPE IN 2022

The global data protection landscape continued to evolve in 2022, with several noteworthy legislative and regulatory developments in jurisdictions around the world. In this article, we highlight some of the most significant developments in 2022 in jurisdictions outside the United States ("U.S.") and the European Union ("EU"), including: (1) regulatory and legislative developments in China, Australia, and Indonesia, each of which took steps with significant implications for companies that operate in those jurisdictions, and (2) new legislation proposed in Canada, Argentina, India, Israel, and Nigeria that would import to those jurisdictions many concepts of the EU's General Data Protection Regulation ("GDPR") — sometimes in an express effort to improve the likelihood of an "adequacy" finding from the European Commission ("EC") for cross-border data transfers. As the pace of privacy developments increases, the challenges for multinational organizations trying to monitor applicable data protection regimes increases as well.

Developments in China, Australia, and Indonesia Have Important Implications for Companies Operating in Those Jurisdictions and Beyond

Chinese Regulators Publish a Series of Guidelines Supplementing the Personal Information Protection Law

With China's Personal Information Protection Law ("PIPL")[1] having taken effect in 2021, 2022 saw a number of efforts from Chinese data protection authorities to implement and enforce specific provisions of PIPL. For example, on January 4, 2022, the Cybersecurity Administration of China ("CAC") released Cyber Security Review Measures outlining the obligations of Critical Information Infrastructure Operators ("CIIOs") to carry out a national security review as provided under the PIPL and the factors that should be taken into consideration when assessing national security risks, including the risk of illegal control, destruction of key information infrastructure and important data. And one of the most significant enforcement matters of the year — a $1.2 billion USD fine against ride-hailing firm DiDi Global —

1 Chairman's Order No. 91, Personal Information Protection Law of the People's Republic of China, available here.

arose out of alleged violations of and non-compliance with the PIPL.[2]

The other issue that garnered significant attention from regulators and businesses was cross-border data transfers. PIPL includes limits on such transfers that roughly parallel those under GDPR. The CAC and other agencies provided guidance on this by publishing a series of releases on the scope of and requirements for each of the three available mechanisms for transferring data out of China: (i) security certification; (ii) China's standard contractual clauses ("SCCs"); and (iii) the CAC security assessment. These releases underscore the extremely high hurdles — and significant risks — companies face when engaging in cross-border data transfers under PIPL.

Security Certification

On June 24, 2022, China's National Information Security Standardization Technical Committee (TC 260) released the final version of the Network Security Standards Practice Guide — Technical Specifications for the Security Certification of Personal Information Cross-Border Processing.[3] The security certification is only available in the case of intra-group cross-border transfer of personal data, similar to the "binding corporate rules" under GDPR. For example, it requires a legally binding and enforceable agreement to cover the key terms and conditions of the processing of cross-border data transfers, including key internal controls (such as establishing a data protection department, appointing a data protection officer, and conducting data protection impact assessments).

China's SCCs

On June 30, 2022, the CAC released the draft Regulations for Standard Contracts for Cross-border Transfer of Personal Information. Under the draft regulations, a data exporter is allowed to transfer personal data abroad using the SCCs if *all* of the following conditions are satisfied:

- The data exporter is not a CIIO;
- The data exporter processes personal data of fewer than 1 million individuals residing in China;
- Since January 1 of the previous calendar year, the data exporter has provided personal data of fewer than 100,000 individuals residing in China to a foreign jurisdiction; and
- Since January 1 of the previous calendar year, the data processor has provided sensitive personal data of fewer than 10,000 individuals to a foreign jurisdiction.

The substantive requirements of China's SCCs are similar to those in the SCCs under GDPR. For example, they require the performance of privacy impact assessments, and executed SCCs must be filed with the CAC. However, the threshold for using the SCCs may be too low to be useful for many large companies, particularly for those Internet platforms employing an advertising-based business model.

CAC Security Assessment

On July 7, 2022, the CAC released the final Measures on Cross-Border Data Transfer Security Assessment (the "Security Assessment"), which came into effect on September 1, 2022. The Security Assessment is required for: (i) cross-border transfers of "important data"; (ii) cross-border transfers of personal data by CIIOs; (iii) cross-border transfers by data exporters processing personal data of 1 million or more individuals; (iv) any transfer (in aggregate) of personal data of more than 100,000 individuals or sensitive personal data of more than 10,000 individuals that has occurred since January 1 of the preceding year; and (v) other situations requiring security assessment in accordance with PRC laws and regulations. Even if a company "de-identifies" certain personal data (e.g., by replacing individuals' names with serial numbers) and transfers only the non-identifiable parts of the data overseas, these requirements may still apply if the data has not been irreversibly anonymized.

A critical aspect of this assessment is that it must be conducted by the CAC, and any cross-border data transfers

2 On July 21, 2022, the CAC imposed a fine of RMB 8.026 billion (around $1.2 billion USD) on China's largest ride-hailing company, DiDi Global Co., Ltd, for a total of 16 violations of PIPL, the Data Security Law, and the Cybersecurity Law, following an investigation. *See* Press Release, "The CAC Issues Administrative Punishment Against DiDi Global Co., Ltd." Cybersecurity Administration of China, (Jul. 21, 2022), available here (in Chinese). *See* also "Official CAC Q&A with Journalists on the DiDi Case Outcome" CYBERSECURITY ADMINISTRATION OF CHINA, (Jul. 21, 2022), available here (in Chinese).

3 Practice Guide on Cybersecurity Standards Specification for Security Certification for Cross-border Processing of Personal Information, China's National Information Security Standardization Technical Committee, (June 24, 2022), available here.

that happen without the CAC's approval are potentially subject to significant fines. As a result, companies that do not qualify for the SCCs — including larger multinational companies — will need to present proposed cross-border transfers of personal information to the CAC for approval, a process which could open those companies to intense scrutiny of the nature and scale of their data processing activities.

Australia Adopts Harsher Penalties for Data Breaches

In the past year, Australian companies have been the targets of a series of particularly disruptive cyberattacks. Australia's second-largest telecom provider, Optus, experienced a massive data breach in September 2022 that exposed the personal information of over 10 million customers — about 40% of Australia's population.[4] Shortly thereafter, in October 2022, a Woolworth online shopping site experienced a data breach exposing the personal information of an estimated 2.2 million customers.[5] This surge in data breaches and personal data exposure prompted lawmakers to introduce the Privacy Legislation Amendment Bill 2022, which was passed by both Houses of Parliament in less than a month.[6] These amendments make fundamental changes to Australia's existing privacy law, including:

- **Increased Penalties.** Significant increases to penalties for data breaches — from AU $2.2 million to the greater of: (i) AU $50 million, (ii) three times the value of the benefit obtained through the misuse of information, or (iii) 30% of adjusted turnover in the relevant period.
- **More Enforcement Authority for the Information Commissioner.** Increases the enforcement powers of Australia's data protection authority, the Office of the Australian Information Commissioner, to ensure that companies respond appropriately to security incidents and data breaches.
- **Extraterritorial Reach.** Expands the extraterritorial applicability of Australian privacy law to organizations or operators carrying on "business in Australia or an external Territory."[7]

This focus on enforcement against companies who have experienced a data breach stands in contrast to the broad U.S. response to increased data security incidents, which has employed both carrots (including legislation to encourage companies to notify the federal government of cyber-attacks against critical infrastructure and to share cyber threat information through public-private partnerships) and sticks (regulators at the Federal Trade Commission, the Securities & Exchange Commission, state Attorneys General, and other state and federal agencies continue to bring enforcement actions against companies that fail to adequately protect personal information). If Australia's "get tough" approach shows signs of success, it will likely inform cybersecurity policy in the U.S. and around the world in the coming years.

Indonesia Passes Its First Data Protection Act

On September 20, 2022, Indonesia's Parliament passed the Personal Data Protection Act ("PDPA"),[8] which was signed into law by the country's President on October 17, 2022. The PDPA provides a two-year transitional period.

The PDPA includes requirements and concepts that are similar to those of the GDPR, including the concepts of controller and processor, lawful grounds for processing, data subject rights, the appointment of a data protection officer, and data protection impact assessments. The PDPA has broad extraterritorial reach: by its terms, the PDPA applies to the processing of personal data of Indonesian data subjects outside Indonesia if such processing has a legal impact in Indonesia. Other notable features of the PDPA include a new data protection authority and potential civil and criminal penalties.

4 *See* Optus Notifies Customers of Cyberattack Compromising Customer Information, OPTUS.COM.AU, (Sep. 22, 2022), available here.

5 *See* Woolworths Says Data of Online Unit's 2.2 Million Users Breached, REUTERS.COM, (Oct. 14, 2022), available here.

6 Bills No. 30, 2022-23 "Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022," available here.

7 Note, however, the scope of application in which an organization would be considered "carrying on business in Australia" has yet to be confirmed by the parliament and requires further clarification.

8 Personal Data Protection Act, available here (in Indonesian).

Change Will Be a Hallmark of the Global Privacy Landscape for the Foreseeable Future

Canada Introduces the Digital Charter Implementation Act 2022

In June 2022, The Digital Charter Implementation Act was introduced in Canada's House of Commons.[9] The Act includes three pieces of legislation — the Consumer Privacy Protection Act ("CPPA"), the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act — that would:

- Replace the existing Personal Information Protection and Electronic Documents Act ("PIPEDA") with the CPPA;
- Establish a new Data Protection Tribunal charged with enforcing the new law, with fines up to 5% of global revenue or C$25 million, whichever is greater; and
- Regulate businesses' use and development of artificial intelligence by prohibiting certain conduct that may harm individuals or their interests.

If enacted, the CPPA would apply to every organization processing personal information during commercial activities or employee recruitment, and would require an organization to obtain an individual's prior, informed, and specific consent before it collects, uses, or discloses personal information. Further, the CPPA would import data subject rights from the GDPR, including the rights to access, correct, erasure, and data portability.

Argentina's Data Protection Authority Proposes Updating the Personal Data Protection Act

In August 2022, Argentina's Agency of Access to Public Information ("AAPI") initiated the reform of the existing Personal Data Protection Act ("PDPA").[10] The current law was enacted in 2000 but has not been substantially amended since. The draft bill was released on September 12, 2022,[11] and largely mirrors the GDPR in many aspects, including in its proposed terms and definitions, data minimization, data subject rights, and legal bases for data processing. In some respects, however, it is even more burdensome than the GDPR; for example, in the event of a security incident involving personal data, a data controller would be required to notify the data protection authority within 48 hours — rather than 72 hours — of becoming aware of a breach.

If enacted, the PDPA would apply to an organization located outside Argentina if the organization processes data in Argentina or carries out processing activities related to the offering of goods or services to individuals located in Argentina. The AAPI is currently evaluating submissions from the public consultation process, and adjustments to the text are expected before it is transferred to the Federal Executive Branch for subsequent introduction in Congress.

India Releases the Draft of the Digital Personal Data Protection Bill

In November 2022, India's Ministry of Electronics and Information Technology released the Digital Personal Data Protection Bill ("DPDP").[12] The scope of the proposed legislation is limited to "digital personal data" (in other words, it excludes personal data collected or processed offline), but its geographic reach is broad: it would apply to organizations processing digital data outside India if such processing involves offering goods and services to or profiling of Indian data subjects.

Similar to a bill proposed in 2019,[13] the DPDP would grant broad powers to the central government, such as allowing the government to exercise control over the appointment of the members of the Data Protection Board, which has the authority to impose penalties and determine non-compliance. With respect to substantive obligations, the DPDP introduces a concept of "deemed consent," which is different from explicit "consent" and a novel concept in privacy law. "Deemed consent" is implicated where the consent of a data principal is deemed *necessary*, including situations where a data principal is reasonably expected to

9 Bill C-27, the Digital Charter Implementation Act, available here.

10 Presentación del Proyecto de Ley de Protección de Datos Personales, Agencia de Acceso a la Información Pública, (Nov. 10, 2022), available here.

11 Ley 25.326 de Protección de Datos Personales, Agencia de Acceso a la Información Pública, available here.

12 The Digital Personal Data Protection Bill, 2022, Ministry of Electronics & Information Technology, Government of India, available here.

13 The Personal Data Protection Bill, 2019, available here.

voluntarily provide personal data for public interest or other fair and reasonable purposes.

The public consultation period for the DPDP closed in December 2022, but it remains to be seen whether the DPDP will be introduced in the Indian Parliament.

Israel Publishes Draft Provisions to Maintain Its Adequacy Decision

On November 29, 2022, the Israeli Ministry of Justice published the draft "Provisions Regarding Information Transferred to Israel from the [European Economic Area ("EEA")]" (the "Draft Provisions"),[14] in an effort to maintain Israel's adequacy status that allows transfers of personal data from the EEA.[15]

Israel was granted its adequacy status in 2011, prior to the 2016 adoption of the GDPR; Article 45 of the GDPR stipulates that the EC must conduct a periodic review of third countries' level of protection to ensure they remain adequate. The EC is currently in the process of examining whether to reaffirm Israel's 2011 adequacy decision, but the existing Israeli data protection regime has gaps that must be filled to satisfy the GDPR's standards for protection of personal data — for example, extending the definition of sensitive data so that it aligns with the requirement to protect special category data under the GDPR.

The Draft Provisions aim to better align Israel's privacy law with GDPR to preserve Israel's adequacy status. In particular, the Draft Provisions would introduce four main obligations for Israeli database controllers with respect to the personal data transferred from the EEA to Israel: (1) deletion of personal data upon a data subject's request, subject to certain conditions and exceptions; (2) ensuring deletion of personal data that is no longer required or necessary; (3) ensuring that data is correct, complete, and up-to-date; and (4) notification to a data subject regarding details of the personal data received or transferred. Additionally, the Draft Provisions would amend the definition of sensitive data to include information about a person's origin, national affiliation, and trade union membership. Note that these requirements would only apply to personal data transferred from the EEA to Israel, not data collected from Israeli data subjects.

The public consultation period closed on December 20, 2022, and no further information has been communicated by the Israeli Ministry of Justice regarding the finalization of the Draft Provisions.

Nigeria Releases a Draft of Its Data Protection Bill

In October 2022, the Nigerian National Information Technology Development Agency ("NITDA") released the Data Protection Bill 2022 ("DPB"),[16] which mirrors the concepts and requirements of the GDPR in many aspects, including definitions, use of key terms (e.g., controllers and processors), data subject rights, acceptable legal bases for processing, and appointment of a data protection officer. There are some differences, for example, the DPB provides that data controllers should respond to data subject rights without unreasonable delay but, unlike the GDPR, the DPB does not specify the number of days or otherwise establish an express timeline for responding to such requests.

For implementation and enforcement, the DPB would establish the Nigeria Data Protection Commission. Additionally, an organization in violation of the DPB would be subject to a penalty of NGN 10 million (approximately $22,000) or 2% of its annual gross revenue derived from Nigeria, whichever is greater.

On October 26, the NITDA announced that the Nigerian Minister received the bill for transmission to the Federal Executive Council for approval.[17] The final decision of the Federal Executive Council on the DPB is yet to be announced.

14 Provisions Regarding Information Transferred to Israel from the European Economic Area 5782 – 2022, MINISTRY OF JUSTICE, (Nov. 29, 2022), available here (in Hebrew).

15 An Accompanying Document in Accordance with the Principles of Regulatory Impact Assessment, MINISTRY OF JUSTICE, (Nov. 29, 2022), available here (in Hebrew).

16 Nigeria Data Protection Bill, 2022, NIGERIAN NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY, (Oct. 4, 2022), available here.

17 *See* Press Release, "Minister Receives Draft National Data Protection Bill," Nigeria Data Protection Bureau, (Oct. 26, 2022), available here.

PRIVACY'S GREATEST HITS? OLDER PRIVACY LAWS MAKE A COMEBACK IN 2022

While new privacy laws — and updates to existing privacy laws — have garnered the lion's share of attention from the media, advocates, and in-house counsel in 2022, plaintiffs' attorneys have been seeking to revive older privacy laws using novel theories to apply them to new circumstances, forcing companies to dust off and update old advice and research to ensure they are compliant. Three laws in particular have been at the center of this trend: the California Invasion of Privacy Act (also known as the "California Wiretap Law"), first enacted in 1967;[1] the 1980s-era Video Privacy Protection Act ("VPPA");[2] and the Drivers' Privacy Protection Act ("DPPA"),[3] enacted in 1994. The efforts at reinvigorating and creatively reapplying these statutes serve as a reminder of the labyrinth of existing privacy law, particularly in the United States, and the importance to companies of a comprehensive review and understanding of their data collection, use, and disclosure activities.

Hotel California? California Wiretap Law Makes a Call from Far Away

Originally passed in 1967 — the same year as *Katz v. United States*, the Supreme Court's seminal Fourth Amendment wiretapping case — the California Wiretap Law establishes a baseline-level of privacy for personal communications in California. Under the California Wiretap Law, it is unlawful for someone to:

> willfully and without the consent of all parties to the communication . . . read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable . . . or to communicate in any way, any information so obtained.[4]

Importantly, the California Wiretap Law provides a private right of action that entitles plaintiffs to seek statutory damages of $5,000 per violation, as well as injunctive relief to stop further violations.[5]

In the past two years, plaintiffs' attorneys have revived interest in the California Wiretap Law by introducing a novel cause of action: suing website operators that use session replay software and the third parties that provide the software. The plaintiffs' theory is that the third-party session replay software provider is intercepting the individual's communications to the website provider without the individual's consent, and that the website provider is aiding and abetting that unlawful interception.[6]

Given the widespread use of session replay software on consumer-focused websites, particularly for e-commerce sites, plaintiffs have found fertile ground for these suits. However, courts in California are not universally sold on this theory.[7] For example, in the Northern District of California, different courts have come to very different conclusions on generally similar claims.[8] Until higher courts or the California legislature take steps to preclude these claims or otherwise clarify what obligations attach to the use of session replay software, companies will have to accept either the risk of using such software, or the loss of visibility in avoiding it.

1 Cal. Pen. Code § 630 et seq.

2 Video Privacy Protection Act of 1988, Pub. L. No. 100-618 102 Stat. 3195 (codified at 18 U.S.C. § 2710) (hereinafter "VPPA").

3 Drivers' Privacy Protection Act of 1994, Pub. L. 103-322 Title XXX, 108 Stat. 1796, 2099 (codified at 18 U.S.C. §§ 2721-25) (hereinafter "DPPA").

4 Cal. Pen. Code § 631(a).

5 *Id.* §§ 637.2(a), (b).

6 *See, e.g., Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 508 (C.D. Cal. 2021). Session replay software is a technology that records a user's interaction with a website (e.g., where their cursor moved, what links the user clicked on) so the website operator can better understand the website's usability, customer experience, and customer interest.

7 *See* Jones & Rockey, *Is Your Website Violating California's Wiretap Act?*, JD Supra, (Sept. 2, 2022) available here.

8 *Compare Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 BL 413488, at *2 (N.D. Cal. Oct. 23, 2019) (holding that plaintiff "adequately alleges that [the session replay software provider] acted as a third party that eavesdropped on his communications with [the website operator] because the code embedded into the [web] pages functioned as a wiretap" and that the website operator enabled that wrongdoing) *with Graham v. Noom, Inc.*, No. 20-cv-06903-LB, 2021 BL 306839 (N.D. Cal. Aug. 13, 2021) (holding that a session replay software provider is acting as an agent of the website operator, and is thus a party to the communication with the customer, so cannot be said to be intercepting those communications).

The Video Privacy Protection Act Killed the Internet Star?

The VPPA was enacted in 1988, in response to the unauthorized publication of then-Supreme Court nominee Robert Bork's video rental records. The VPPA prohibits "video tape service providers" from disclosing information about "specific video materials or services" that an individual has requested or obtained from a video tape service provider, without the individual's prior consent. Violations of the VPPA are enforceable through a private right of action.

As the video market shifted from tape and DVD rentals to streaming over the Internet, plaintiffs' attorneys sought to expand the VPPA to cover the new video streaming platforms. Relying on language in the VPPA suggesting that a video tape service provider might use "similar audio visual materials," between 2007 and 2009 a series of decisions clarified that the VPPA was, in fact, applicable to modern video streaming platforms.[9] Following those rulings, streaming platforms had to change their practices to better protect against disclosure of information,[10] and some even sought to amend the VPPA to make it easier for consumers to direct the streaming providers to share information with social media platforms.[11]

Following legislative amendments in 2012, VPPA lawsuits slowed down for several years. But that changed in 2022, when a flurry of class-action lawsuits were filed against news outlets, sports leagues, and other streaming sites that track individuals' video consumption habits via a third-party tracking tool.[12] According to these plaintiffs, using third-party tracking tools qualifies as disclosing "specific video materials or services" information to a third party without the consumer's consent. While it may be too soon to know whether this line of argument will succeed in the same way as the expansion of VPPA to streaming services, some of these cases have moved to the discovery phase, indicating that at least some courts believe these claims have merit.[13] Given the potentially significant penalties for non-compliance,[14] this new wave of actions seems likely to result in additional changes to how video streaming services share information with third-party partners.

I Saw the Driver's Privacy Protection Act and It Opened up My Eyes

Enacted in 1994, the DPPA was passed in response to several high-profile incidents in which stalkers were able to obtain the home address of their victims from state departments of motor vehicles ("DMVs").[15] The DPPA prohibits state DMVs (or their employees or contractors) from sharing information obtained from an individual's motor vehicle record — outside of certain specified uses — without the individual's consent. The DPPA grants aggrieved individuals a private right of action, but may also be enforced by government officials and could carry criminal fines.

In the years since its enactment, the DPPA has been the subject of several class actions targeting entities — such as state DMVs, data brokers, insurance companies, consumer reporting agencies, and even media and retail corporations that held DPPA-protected information — whose purported disclosures or use of personal information

9 *See Doe v. Netflix*, C09-05903-JW-PVT (N.D. Cal. filed Dec. 17, 2009) (alleging Netflix violated the VPPA by sharing subscribers' video rental information to third parties participating in a contest to improve Netflix's recommendation algorithm); *See also Harris v. Blockbuster Inc.*, No. 3:09-cv-00217 (N.D. Tex. filed Feb 03, 2009) (class action claim alleging Blockbuster violated the VPPA by sharing video rental information from its website visitors with third-party advertisers).

10 Michael Lewis, *Netflix Changes Privacy Policy*, Toronto Star (July 30, 2012), available here.

11 Video Privacy Protection Act Amendments Act of 2012, Pub. L. 112-258, 126 Stat. 2414 (codified at 18 U.S.C. § 2710(b)(2)(B)) (amending the VPPA to allow consumers to consent over the internet to video tape service providers sharing their personally identifiable information, provided the consumer can withdraw that consent).

12 *See, e.g., McDaniel et al. v. Home Box Office, Inc.*, No. 1:22-cv-01942 (S.D.N.Y. filed Mar. 8, 2022); *see also Stark v. Patreon, Inc.*, No. 22-cv-03131-JCS (N.D. Cal. filed May 27, 2022); *Wright v. Buzzfeed, Inc.*, No. 1:22-cv-04927 (N.D. Ill. filed Sept. 12, 2022).

13 *See Ambrose v. Bos. Globe Media Partners LLC*, No. 21-10810-RGS, 2022 BL 330307, at *3 (D. Mass. Sept. 19, 2022) (court holding that an allegation that the use of certain tracking technologies that communicated information about what videos a website user had accessed was sufficient to survive a motion to dismiss).

14 VPPA § 2710(c)(2) (courts are able to award "(A) actual damages but not less than liquidated damages in an amount of $2,500; (B) punitive damages; (C) reasonable attorneys' fees and other litigation costs reasonably incurred; and (D) such other preliminary and equitable relief as the court determines to be appropriate").

15 *See The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*, Elec. Privacy Info. Ctr., available here (last visited Jan. 17, 2023).

went beyond the statute's permitted uses.[16] For example, in one case, plaintiffs filed class actions against more than 75 defendants, alleging that "buying [DMV] records in bulk with an expectation and purpose of valid potential use is not [in itself] a permissible use under the DPPA."[17] Ultimately, the case was dismissed, and that dismissal upheld by the 5th Circuit, which held that the defendants' practices did not fall outside the scope of the DPPA's permitted uses.[18]

Recently, some plaintiffs' attorneys have sought to expand the potential use of DPPA by filing claims against companies following data breaches that exposed individuals' motor vehicle records. These efforts have not been successful thus far, but courts reviewing these arguments have not shut the door on this theory entirely. The most high-profile example of such an effort — as well as the significant hurdles to the success of this theory — is the $65 billion class action filed against Vertafore, Inc. following a 2020 data breach.[19] Plaintiffs contended that the breach, which may have exposed numerous drivers' license numbers to unauthorized parties, constituted an unauthorized disclosure of motor vehicle records, entitling them to compensation under the DPPA.[20] However, in March 2022, the 5th Circuit disagreed with the plaintiffs and affirmed the lower court's dismissal of the case, holding that (i) the DPPA requires a *knowing* disclosure on the part of a defendant, and (ii) insufficiently securing protected information does not meet that bar.[21] However, the court noted that plaintiffs did not allege that the defendants' servers were so insecure that the DPPA-protected information was exposed to public view and suggested that, if this data were stored in such a way as to be "in plain view of any 'digital passer-by,'" such an instance could give rise to a plausible DPPA claim.[22]

The other issue that has presented a significant hurdle to plaintiffs is standing; specifically, whether they can plead sufficient facts to show concrete harm as required for standing under recent Supreme Court precedent. For instance, a Wisconsin district court found that the mere fact that a plaintiff's DPPA-protected personal information was involved in a data breach was insufficient to meet the concrete injury requirement for standing.[23] A court in the Northern District of California came to a similar conclusion, writing that "[n]ow or in the future, it would be difficult to trace any future identity theft or fraud to" the defendant's data breach.[24]

Despite the losses thus far, plaintiffs continue to file class actions and otherwise initiate litigation in the wake of major data breaches, hoping to find the right combination of facts to satisfy a court that this new theory deserves a more thorough examination. As a result, companies holding DPPA-protected information should continue to monitor these efforts, and otherwise be sure they have taken appropriate steps to shield that data from "digital passers-by."

16 *See, e.g., Siegler v. Best Buy Co. of Minn., Inc.*, 519 F. App'x 604, 605 (11th Cir. 2013) (per curiam) (affirming the district court's ruling that plaintiff could not allege a violation of the DPPA where the personal information disclosure at issue did not originate from the state DMV); *see also Welch v. Theodorides-Bustle*, 273 F.R.D. 692, 697 (N.D. Fla. 2010) (certifying the formation of a class in a DPPA action against the Florida DMV consisting of all Florida driver's license holders whose personal information was disclosed to a third-party contractor).

17 *See Taylor v. Acxiom Corp.*, 612 F.3d 325, 334 (5th Cir. 2010), *cert. denied*, 562 U.S. 1169 (2011).

18 *Id.* 612 F. 3d at 339 (holding that "a person who buys DMV records in bulk does so for the purpose of making permissible actual use of information therein [under the DPPA], even if that person does not actually use every single item of information therein [and the DPPA] allows resale of DMV records to one who is authorized and proposes to make actual use thereof . . . notwithstanding that the seller does not actually use or intend to use the records before resale").

19 *See*, *Allen v. Vertafore, Inc.*, 28 F.4th 613, 617 (5th Cir. 2022), *cert. denied*., No. 21-1555 (U.S. Oct. 3, 2022).

20 *Id.* 28 F.4th at 616.

21 *Id.* 28 F.4th at 616 – 617 (holding that "the inference Plaintiffs ask us to draw—from 'stored on unsecured external servers' to 'disclosed'—is not reasonable").

22 *Id.* (comparing this instance to *Senne v. Village of Palatine, Ill.*, 695 F.3d 597, 603 (7th Cir. 2012) (en banc) which held that a police officer disclosed personal information subject to the DPPA when that officer placed a parking ticket in plain view on plaintiff's windshield).

23 *Maxim v. Midvale Indem. Co.*, No. 21-cv-394-wmc, 2022 BL 134901, at *3 (W.D. Wis. Apr. 19, 2022), *appeal docketed*, No. 22-1892 (7th Cir. May 20, 2022) (stating "the court is compelled to find that the risk of harm posed by the disclosure of driver's license numbers is not imminent and too speculative to satisfy Article III standing.").

24 *Greenstein v. Noblr Reciprocal Exch.*, No. 21-cv-04537-JSW, 2022 BL 433299, at *5 (N.D. Cal. Dec. 5, 2022).

DESCRIPTION OF OUR PRACTICE

In the 21st century, information is a mission-critical asset. Managing legal risks related to that asset—from developing incident response plans to ensuring regulatory compliance—requires the kind of depth and breadth of legal experience that Willkie's Privacy, Cybersecurity & Data Strategy attorneys can provide.

Our practice provides leading-edge, practical counsel on the ever-changing digital legal landscape, the design, development, and implementation of privacy, data protection, and cybersecurity programs, and innovation in new data-driven products and services at the forefront of the digital economy. Leveraging their broad base of knowledge and experience on these issues - including as regulators and senior in-house lawyers - our attorneys help clients manage their legal risks and achieve their business goals.

Our multidisciplinary practice includes attorneys with in-depth experience in all aspects of privacy, data protection, and cybersecurity law, as well as key commercial and technological developments, that we apply to helping our clients achieve their strategic business priorities. We collaborate with complementary practices across Willkie's platform, including the Willkie Digital Works group and our corporate, tech transaction, private equity, intellectual property, antitrust, and litigation practices, to provide clients with comprehensive, practical counsel for their data-related challenges and opportunities.

We provide practical guidance to companies and counsel clients on all aspects of privacy and cyber risk, including:

- Designing and implementing global compliance programs, including performing privacy and security risk and impact assessments; advising on product development and digital innovation; development and drafting privacy, data governance, and security policies; and negotiating vendor contracts;
- Global security incident preparation, response, and remediation, including crisis management services
- Litigation related to privacy and security practices and data security incidents, including regulatory investigations and proceedings instigated by regulators in the U.S., UK, and EU;
- Strategic advice on investments, mergers and acquisitions, and other transactions, including diligence and deal negotiation; and
- Legislative and regulatory policy advice and advocacy.

Our attorneys have substantive experience advising clients on numerous privacy and cybersecurity laws and regulations in the United States and around the world, including CCPA, FTC Act, BIPA, GLBA, NYDFS Cybersecurity Regulation, FCRA/FACTA, HIPAA, COPPA, GDPR, and the UK Data Protection Act 2018.

OUR CLIENTS & EXPERIENCE

For over 20 years, our Privacy, Cybersecurity & Data Strategy attorneys have advised a diverse set of clients across a wide range of industries and at every stage of the business life cycle on managing the risks and taking advantage of the opportunities presented by the evolving commercial, technological, and regulatory landscape related to the collection and use of data.

Willkie's notable experience includes the following representative matters:

- We advised Kaseya on its response in the wake of one of the largest and most highly publicized ransomware attacks in history. This included briefings with senior law enforcement and national security stakeholders and coordinating notifications to customers and regulators around the world.
- We advise social media platforms, consumer electronics companies, media companies, and financial companies on the strategic, commercial, and legal issues raised by cutting edge uses of data - including artificial intelligence and algorithmic decision-making technologies, biometric data, Internet of Things data, and geolocation data.
- We have advised clients in connection with investigations by the New York Department of Financial Services related to alleged violations of the Cybersecurity Regulation.
- We work closely with our corporate and tech transaction colleagues throughout the U.S. and Europe to advise on investment, M&A, and other transactions involving companies leading innovation in big data, artificial intelligence, autonomous vehicles, healthtech, insurtech, and fintech.
- We have represented numerous clients before regulators in the U.S (FTC, FCC, CPPA, State Attorneys General), the UK (Information Commissioner's Office), and the EU with respect to rulemakings, enforcement inquiries, and other proceedings.
- We advise major technology, media, social media, and financial services companies on critical compliance issues arising from statutory and regulatory obligations, particularly those arising from legal regimes such as GDPR and CCPA/CPRA, as well as compliance issues arising from enforcement activities and consent decrees.
- We counseled the manufacturer of widely used software in response to the discovery of a critical vulnerability in its software, including by notifying U.S. governmental authorities about the vulnerability, counseling the company on customer communications, and collaborating with technical consultants and the client development team to develop and execute remediation strategies.
- We advise major publicly traded companies and financial institutions on SEC policymaking, rulemakings, investigations, and enforcement activities related to cybersecurity and privacy.

WHO WE ARE

Daniel K. Alvarez
Partner
Co-Chair, Privacy, Cybersecurity & Data Strategy Practice Group
+1 202 303 1125
dalvarez@willkie.com

Laura E. Jehl
Partner
Co-Chair, Privacy, Cybersecurity & Data Strategy Practice Group
+1 202 303 1056
ljehl@willkie.com

Simona Agnolucci
Partner
Litigation
+1 415 858 7447
sagnolucci@willkie.com

Michael G. Babbitt
Partner
Intellectual Property
+1 312 728 9070
mbabbitt@willkie.com

Elizabeth Bower
Partner
Litigation
+1 202 303 1252
ebower@willkie.com

Elizabeth P. Gray
Partner
Litigation
+1 202 303 1207
egray@willkie.com

Michael J. Gottlieb
Partner
Litigation
+1 202 303 1442
mgottlieb@willkie.com

Benedict Y. Hur
Partner
Litigation
+1 415 858 7401
bhur@willkie.com

Aliceson (Kristy) Littman
Partner
Litigation
+1 202 303 1209
aklittman@willkie.com

Stefan Ducich
Associate
Privacy, Cybersecurity & Data Strategy
+1 202 303 1168
sducich@willkie.com

Nicholas Chanin
Associate
Privacy, Cybersecurity & Data Strategy
+1 202 303 1164
nchanin@willkie.com

Michelle Bae
Associate
Privacy, Cybersecurity & Data Strategy
+1 202 303 1166
ebae@willkie.com

Samuel Lewis
Associate
Privacy, Cybersecurity & Data Strategy
+1 202 303 1175
slewis@willkie.com

Kari Prochaska
Associate
Privacy, Cybersecurity & Data Strategy
+1 312 728 9080
kprochaska@willkie.com

Amal Ibraymi
Associate
Privacy, Cybersecurity & Data Strategy
+1 212 728 3524
aibraymi@willkie.com

Amelia Putnam
Associate
Privacy, Cybersecurity & Data Strategy
+1 202 303 1089
aputnam@willkie.com