troutman pepper

2022 Regulatory Privacy Year in Review

Troutman Pepper
Regulatory Investigations,
Strategy + Enforcement

troutman.com

Table of Contents

INTRODUCTION

Regulators at all levels of government demonstrated their intensifying interest in consumer privacy and cybersecurity matters throughout 2022. The regulatory attention can be attributed in part to the rapid adoption of smart technology, which offers countless benefits to industry and consumers, but also has the potential to encroach upon the most private aspects of life. As regulators attempt to strike a balance that promotes innovation, while also protecting consumer privacy in a data-driven world, regulatory and legislative initiatives that define the contours of domestic consumer privacy rights will continue to be a significant driver of regulatory oversight for the foreseeable future. In the absence of a crystal ball, the best way to predict the regulatory playbook for the rapidly changing landscape in 2023 and beyond is to review the regulatory and legislative priorities that came to pass last year.

Data is the commodity that drives smart technologies and innovation. Many aspects of everyday life are now supplemented or augmented with smart devices (*i.e.*, Internet of Things (IoT) technology), apps, and websites that play an increasingly vital role in critical daily activities involving everything from health care, childcare, education, and finances to how individuals are entertained, socialize with one another, and relax. The websites, apps, and devices that facilitate our connected world generate an incredible amount of data. In 2022 alone, technology generated an estimated 97 zettabytes of data, and it is predicted that 181 zettabytes of data will be generated in 2025. The quantity of data being generated is incomprehensible. Humans currently generate more data every year than they created in all of human history before the internet age. This data acts as the fuel for automated decision-making technology.

The Big Data industry has taken flight in this new data-rich environment, using massive data pools to train machine learning and artificial intelligence applications and algorithms to make predictions, improve efficiency, and help technology interact with the physical world, among other nearly unlimited usages. Much of the data — especially for consumer-facing applications — is sourced from consumers whether they are aware of it or not. With applications collecting geolocation data (including when at sensitive locations, such as places of worship or health care institutions), health data (including mental health and pregnancy data), and data of minor children, the intrusion on individual privacy is manifest. Public disclosure of such sensitive information could have a devastating result for individual consumers who expect a reasonable level of privacy in their daily activities.

Resultingly, regulators charged with consumer protection have increased enforcement of privacy laws and regulations. Where legislation fails to keep up with technology, a belt and suspenders approach is frequently employed by regulators who use existing consumer protection laws (laws not initially contemplated to address data privacy) to justify investigations, file lawsuits, and develop law by consent decree. Unless and until legislation matches the pace of technology advancement, consumer privacy rights will be primarily enforced through regulatory oversight.

In the midst of a complex regulatory and legal environment, companies that utilize consumer data in their business activities should thoughtfully engage with legal counsel to develop defensible information technology systems. A sound and legally enforceable plan may be an important differentiator for both established and upcoming companies — especially in light of the increased regulatory scrutiny. Companies must stay abreast of significant regulatory developments and be prepared to flexibly respond to regulatory pressures to reduce the risk that a company's products and services do not become a regulatory risk factor or existential threat.

Troutman Pepper monitors all developments in the complex and rapidly evolving landscape of consumer privacy and cybersecurity regulations and is proud of its history advising businesses in the context of difficult and novel legal challenges from regulators. We hope that this annual reference will be beneficial to companies seeking to understand the regulatory environment in which they operate and helpful in navigating developments across multiple regulatory dominions in 2023.

CONTRIBUTORS

Ashley L. Taylor, Jr.
Partner
ashley.taylor@troutman.com
804.697.1286

Ryan J. Strasser
Partner
ryan.strasser@troutman.com
804.697.1478

Stephen C. Piepgrass
Partner
stephen.piepgrass@troutman.com
804.697.1320

Michael Yaghi
Partner
michael.yaghi@troutman.com
949.622.2735

Joshua D. Davey
Partner
joshua.davey@troutman.com
704.916.1503

Ketan D. Bhirud
Counsel
ketan.bhirud@troutman.com
202.274.2890

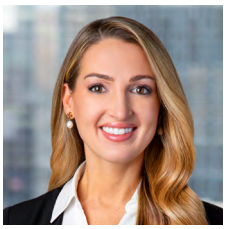
Molly S. DiRago
Partner
molly.dirago@troutman.com
312.759.1926

Daniel Waltz
Associate
daniel.waltz@troutman.com
312.759.5948

Clayton Friedman
Partner
clayton.friedman@troutman.com
949.622.2733

Carson A. Cox
Associate
carson.cox@troutman.com
804.697.1338

Rachel Buck
Associate
rachel.buck@
troutman.com
704.916.1512



Whitney L. Shephard
Associate
whitney.shephard@
troutman.com
617.443.3709

Abigail Hylton
Associate
abigail.hylton@
troutman.com
804.697.1310

Trey Smith
Associate
trey.smith@
troutman.com
804.697.1218

Natalia A. Jacobo
Associate
natalia.jacobo@
troutman.com
213.928.9821

Namrata Kang
Associate
namrata.kang@
troutman.com
202.274.2862

Rachel Miklaszewski
Associate
rachel.miklaszewski@
troutman.com
312.759.5942

STATE PRIVACY LAWS

In 2022, the U.S. witnessed a growing number of states pushing to develop privacy laws. Five states — California, Colorado, Connecticut, Utah, and Virginia — have now enacted comprehensive consumer data privacy acts that are effective and enforceable in 2023. Many other states looked to these acts, as well as the Uniform Law Commission's Uniform Personal Data Protection Act, as models for their own legislation in 2022. Indeed, almost half of the country's state legislatures introduced consumer privacy-related bills last year. Many privacy-related bills were still pending at the end of 2022 of which many will be carried into the 2023 legislative session. Privacy legislation is likely to be considered in a majority of state legislatures next year, especially in states like Florida and Washington where privacy bills were nearly successful. With the amount of state privacy legislation slated to increase in 2023, businesses — particularly those operating across multiple jurisdictions — should take care to craft a comprehensive compliance program that considers each applicable state's potentially different substantive standards, procedural requirements, and enforcement mechanisms.

California Consumer Protection and Consumer Privacy Rights Acts

California was the first state to enact a comprehensive state privacy bill with the California Consumer Privacy Act of 2018 (CCPA). Although the CCPA went into effect on January 1, 2020, it was significantly overhauled during California's November 2020 general election when the California Privacy Rights Act of 2020 (CPRA) was adopted. The CPRA established the California Privacy Protection Agency (CPPA) to adopt, amend, and rescind regulations on 22 topics to carry out the purposes and provisions of the CCPA. The CPRA took effect on January 1, 2023, with important changes like eliminating the automatic 30-day cure period that previously applied to CCPA enforcement.

On July 8, 2022, the CPPA commenced the formal rulemaking process to adopt regulations to implement the CPRA. The proposed regulations provide clarification on many topics of CPRA compliance and enforcement — such as dark patterns, reasonable expectations of privacy, contracting requirements, opt-out preference signals, the right to correct, and notice at collection. Regulations on topics, such as risk assessments, cybersecurity audits, and automated decision-making, are expected to be released at a later date. The CPPA closed its public comment period to the proposed regulations on November 21, 2022, and will decide whether to adopt or further modify the proposed regulations at a future public meeting, yet to be scheduled.

With the upcoming expiration of the notice and cure provision in mind, California Attorney General (AG) Rob Bonta provided a glimpse of what to expect with his August 24, 2022 announcement of a settlement with Sephora, Inc. for $1.2 million — making it the first-ever CCPA settlement.

That same day, the AG also updated its "CCPA Enforcement Case Examples," which provides illustrative examples of situations in which companies were sent a notice of alleged noncompliance and the steps taken by each company. These enforcement cases targeted companies in a variety of industries, including health care services, medical device manufacturers, financial technology, data brokers, clothing retailers, and online advertising and concerned allegations relating to the following:

- A loyalty program that offered financial incentives without a compliant notice of financial incentive;
- Noncompliant opt-out processes, including an opt-out that required consumers to take additional steps by sending them to a third-party trade association's tool;

- Inadequate privacy policies, including one privacy policy whose hyperlinks did not direct consumers to the relevant section; and
- Failures to properly handle consumer requests.

To review important lessons learned from these announcements, check out Troutman Pepper's analysis.

Utah Consumer Privacy Act (UCPA)

On March 24, 2022, Utah Governor Spencer J. Cox signed the UCPA into law, making Utah the fourth state to enact a comprehensive data privacy law. The UCPA is set to take effect on December 31, 2023.

The law applies to both controllers and processors of data. A controller or processor is subject to the UCPA if it (1) conducts business in Utah or produces a product that targets consumers who are Utah residents; and (2) has an annual revenue of $25 million or more and either (a) controls the personal data of 100,000 or more Utah consumers, or (b) derives more than 50% of its gross revenue from the sale of personal data and controls or processes the data of 25,000 individuals. Certain entities are exempt from the UCPA, including state and local government entities, nonprofits, higher education institutions, and financial institutions. Additionally, the UCPA does not apply to data covered by other laws, such as the Gramm-Leach-Bliley Act (GLBA) or Health Insurance Portability and Accountability Act (HIPAA).

The UCPA grants consumers certain rights, such as: (1) confirming if a controller is processing their personal data; (2) deleting personal data that the consumer has not provided to the controller; (3) obtaining a copy of personal data if it is feasible to do so; and (4) opting out of processing their data for the purpose of targeted advertising.

In contrast to other state laws, such as the Virginia Consumer Data Protection Act or the Colorado Privacy Act, the UCPA does not provide consumers with the right to request a correction to inaccuracies in their data. The UCPA also does not create a private right to action. Instead, the Department of Commerce's Consumer Protection Office may consider and investigate a claim without enforcement power. If there is enough evidence of a violation, the claim will be prosecuted by the AG's office at its discretion.

Connecticut Data Privacy Act (CTDPA)

On May 10, 2022, Connecticut Governor Ned Lamont signed the Act Concerning Personal Data Privacy and Online Monitoring, also known as the CTDPA, into law, making Connecticut the fifth state to enact a comprehensive data privacy law. The law is set to take effect on July 1, 2023, and it will apply to both individuals and entities (collectively referred to as controllers) that

(1) conduct business in Connecticut, and (2) control or process personal data during the preceding year of at least either 100,000 consumers (excluding personal data used for completing a payment transaction) or 25,000 consumers who derived more than 25% of their gross revenue from selling personal data.

The CTDPA protects a consumer's "personal data," or information linked to an identifiable individual that does not include de-identified data or publicly available data. The CTDPA also protects "sensitive data," such as racial or ethnic origin, genetic information, immigration status, and geolocation data. Under the law, consumers have the right to (1) confirm whether a controller is processing the consumer's personal data and the right to access their personal data; (2) rectify inaccuracies in the consumer's personal data; (3) remove their personal data; (4) obtain a copy of the consumer's personal data that is portable and easily transferrable; and (5) opt out of the personal data being processed for (a) targeted advertising, (b) the sale of personal data, or (c) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Certain entities are exempt from the CTDPA, including state and local government entities, nonprofits, higher educational institutions, financial institutions subject to the GLBA, and qualifying covered entities subject to HIPAA. Additionally, CTDPA protects Connecticut residents acting in an individual capacity (*i.e.*, consumers) and does not apply to individuals acting in an employment or commercial capacity.

The Connecticut law does not include a private right of action and provides a temporary 60-day right to cure that sunsets on December 31, 2024. For more information on CTDPA click here.

Washington Privacy Act (WPA)

The WPA was first proposed in 2019, but Washington lawmakers have failed for four years to pass the comprehensive privacy law. The original WPA, Senate Bill 5062, passed the Senate in 2021, but failed to earn a floor vote after being sent to the House. This version of the WPA incorporated a number of amendments that interest groups from the private sector lobbies requested but did not include a private right of action, which many other groups wanted.

Several similar bills have likewise failed in Washington. For example, House Bill 1433 or The People's Privacy Act (PPA) was introduced in 2021 as a "pro-consumer" alternative to the WPA. The PPA included a private right of action, a targeted advertising opt-out, and the right to cure. Another bill, House Bill 1850 or the Washington Foundational Data Privacy Act (WFDP), was more similar to the WPA, but proposed the creation of a Washington State Consumer Data Privacy Commission to oversee data security and included a private right of action.

Although Washington has not passed the WPA, the law has served as a blueprint for other states' privacy laws. Specifically, Virginia and Colorado both used the WPA as a template for their comprehensive privacy laws in March and July 2021, respectively. Additionally, both Utah and Connecticut's privacy laws include a right of access and deletion, derived from the WPA. Many states with pending comprehensive privacy laws also borrow heavily from the WPA.

Thus, while Washington has not successfully enacted its own comprehensive privacy law, Washington legislators have had a significant influence on the legislative accomplishments of many other states.

Virginia Consumer Data Protection Act (VCDPA) Amendments

The Virginia legislature passed multiple amendments to the VCDPA during the 2022 legislative session. The first set of amendments established a new exception to the VCDPA's right to delete, applicable when personal data is collected from a source other than the consumer. Under this new exception, data may be considered deleted if: (1) a minimal record of the deletion

request is retained for the exclusive purpose of ensuring the consumer's data is/remains erased; or (2) the consumer is opted out of all nonexempt data processing activities *(e.g.*, targeted advertising and sales). The second set of amendments eliminated the VCDPA's "Consumer Privacy Fund" and diverts all funds collected under this law to the state treasury's Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund. These amendments also redefine "nonprofit organizations" to include tax exempt political organizations.

Other Notable State Law Developments

(a) Age-Appropriate Design Code Act (CA)

On September 15, 2022, California Governor Gavin Newsom signed the California Age-Appropriate Design Code Act (CAADCA) into law. California lawmakers were inspired by the U.K.'s Age-Appropriate Design Code for Online Services, and consistent with its U.K. counterpart, the CAADCA imposes requirements on businesses and prohibits certain data practices and specifically protects children by extending protections to those between the ages of 13 and 18 years of age (which is a broader age range than Children's Online Privacy Protection Rule (COPPA) that extends online protections only to children under 13).

This law "furthers the purposes and intent" of the CPRA and adopts CPRA's definitions (when not defined in the new law). Therefore, businesses subject to the reach of CAADCA have two characteristics: (1) The business is a covered business under the CPRA (defined as a "for-profit entity doing business in California that collects personal information of California residents and meets specific threshold criteria"), and (2) the covered business has online products, features, or services "likely to be accessed by children."

Among other obligations, the CAADCA requires that covered businesses take the following actions:

- **Enhance Privacy Protections.** Covered businesses must offer a high level of privacy unless they can compellingly show that another level would be in the best interest of children.
- **Provide Child-Friendly Privacy Disclosures.** Business must provide privacy information, terms of service, policies, and community standards with language suited to the age of the children likely to access the online service, product, or feature.
- **Create a Data Protection Impact Assessment (DPIA).** The assessment must identify the purpose of the online service, product, or feature; how it uses children's personal information; and the material risks to children that arise from the business's data management practices. The DPIA must be reviewed every other year and, upon written request, provided to the California AG within five business days.

In addition, businesses are restricted from using collected children's information for secondary purposes. The law prohibits covered businesses from collecting, selling, sharing, or retaining any personal information of a child unless the business can show "a compelling reason that the use of the personal information is in the best interest of children."

Although this act does not have a lookback period, businesses must complete their DPIAs prior to the law taking effect on July 1, 2024. The CAADCA authorizes the California AG to assess civil penalties of $2,500 per affected child for negligent violations and $7,500 for intentional violations. The act does not create a private right of action.

(b) Kentucky Genetic Information Privacy Act (GIPA)

On April 8, 2022, Kentucky Governor Andrew Beshear signed the GIPA into law. The law protects data gathered from a biological sample, such as blood, urine, or saliva. The law also protects genetic data, regardless of its format — including raw sequence data extracted from a consumer's DNA, genotypic, and phenotypic information. However, health information already

protected under HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH) is exempt.

GIPA provides consumers with the right to: (1) access their genetic data; (2) delete their account and remove their genetic data; and (3) demand the destruction of their biological sample. The act requires companies to obtain consent before collecting or disclosing a consumer's genetic data. Organizations must also maintain security programs to protect data against unauthorized access, use, and disclosure. The law also changes how law enforcement may use personnel DNA records and requires genetic testing companies to obtain consumer consent before disclosing genetic information to public bodies and law enforcement.

The Kentucky AG has exclusive authority to bring an action on behalf of consumers for violations of GIPA, which may result in a civil penalty up to $2,500 and any actual damages incurred by consumers.

(c) Stop Discrimination in Algorithms Act

Earlier this year, the D.C. Council considered a bill that would impose limitations and requirements on businesses that use algorithms to make credit and other eligibility decisions. However, on November 17, 2022, the chair of the committee reviewing the bill announced that the committee would not proceed with markups to the bill because "there was not enough time … to move this bill forward in a way that effectively bars harmful discrimination without substantially disrupting the central and often positive role that algorithms play in broad swaths of our economy." Despite this pause for 2022, the chair publicly committed "to advanc[e] the bill in the first quarter of 2023."

The proposed bill requires companies to provide individuals with notice on the algorithmic decision-making, explain how the covered entities use the individual's personal information to make decisions, and notify the individual if the covered entity takes an adverse action against that individual based on an algorithmic determination. Finally, the bill requires covered entities to conduct an annual audit of their algorithm programs and provide that report to the D.C. AG. The bill applies to entities that possess or control the personal information of more than 25,000 D.C. residents, have more than $15 million in average annualized gross receipts for three consecutive years, are data brokers, or are service providers.

The bill would create a private right of action (with statutory damages ranging between $100 to $10,000 per violation or actual damages) in addition to granting the D.C. AG authority to bring actions (with civil penalties of $10,000 per violation).

State Privacy Law Survey

State privacy legislation is constantly changing. Our team is releasing an interactive map reflecting the latest changes in comprehensive state consumer privacy law. Please navigate to Troutman Pepper's Privacy Legislation Map in the coming days to learn more.

For an overview of notable state privacy legislation, please see the table at the end of this document.

STATE PRIVACY INVESTIGATIONS AND LITIGATION

State AGs have historically led the national effort to address the myriad and complicated issues arising in the context of a data-driven world. In the face of emerging technologies, the states are the earliest adopters of regulatory framework and a testing ground for the development of policy. State AGs often lead these efforts because many state AGs serve at the will of an electorate. As a result, state AGs are motivated by issues at the forefront of political and social discourse — among which consumer privacy is paramount. The general zeitgeist is a significant driver of targeted enforcement action from the state AGs, meaning that companies not traditionally the targets of regulatory oversight and enforcement might find themselves subject to scrutiny if they run afoul of privacy and cybersecurity norms. In 2022, the state AGs continued to lead the charge on issues of consumer privacy and cybersecurity, utilizing state legislation and regulations to bring about notable investigations and record-breaking settlements.

AG Bonta Secures First-Ever CCPA Settlement With Sephora

Two years after the enactment of the California Consumer Privacy Act (CCPA), California AG Rob Bonta announced the first CCPA settlement with beauty company Sephora, Inc. (Sephora), resolving allegations that the company violated the CCPA.

Sephora is a well-known beauty product retailer with physical and internet stores. On June 25, 2021, Bonta notified Sephora that it may be in violation of the CCPA and had 30 days to cure its privacy practices — specifically Sephora's alleged practice of unlawfully selling personal information without disclosure; failure to provide a conspicuous "Do Not Sell My Personal Information" link on its website; and failure to respond to or process consumer opt-outs according to global privacy controls. After Sephora allegedly failed to cure its violations, AG Bonta initiated an investigation into the company's privacy practices, which culminated in the August 24, 2022 settlement. Concerning

the settlement, Sephora will pay a $1.2 million penalty, be subject to a two-year monitoring period, incur additional reporting requirements, and must conduct a review of its service provider contracts for CCPA compliance.

The settlement represents a bellwether for additional regulatory activity under the CCPA and a reminder to all companies that do business in California to review CCPA compliance policies and practices to avoid regulatory scrutiny.

Texas Sues Facebook for Biometrics Act Violations

In one of the first-ever actions to enforce Texas's Capture or Use of Biometric Identifier Act (CUBI), Texas AG Ken Paxton sued Meta on February 14, 2022, alleging that the Facebook parent illegally collected users' biometric data without their consent. The allegations mimic those in the consolidated action *In re Facebook Biometric Information Privacy Litigation*, which asserted claims under Illinois' Biometric Information Privacy Act (BIPA), and recently resulted in a $650 million settlement. CUBI is similar to BIPA in that it (1) requires businesses to obtain users' informed consent before collecting their biometric data; (2) mandates destruction of the data in a reasonable time; and (3) prohibits selling, leasing, or otherwise disclosing the data except in limited circumstances. Unlike BIPA, however, CUBI does not have a private right of action component and can only be enforced by the Texas AG.

The Texas suit alleges that Facebook violated the CUBI provision that requires a company to obtain consent before capturing "a biometric identifier of an individual." CUBI defines a biometric identifier as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." Facebook previously stored biometric identifiers pulled from photos and videos uploaded by users of the social media app as part the face recognition system, and the lawsuit asserts that Facebook did so secretly and without the permission of users, intentionally avoiding use of the term "biometric data" and failing to properly inform users of their practices. In 2017, Facebook introduced a facial recognition opt-out, and announced in November 2021 that they were ending the face recognition system altogether and no longer automatically recognized users who opted in. The Texas AG felt the move came too late, stating in its suit that "by that point … [Facebook] had spent more than a decade secretly exploiting Texans and their personal information to perfect its AI apparatus."

If Meta is found in violation of the act, state law imposes a $25,000 penalty for each unlawful capture of an identifier, and the additional claims against Meta regarding deceptive trade practices carry up to a $10,000 per violation penalty.

Facebook/Meta Antitrust Case

In 2020, a coalition of 48 state AGs, led by New York AG Letitia James, filed an antitrust lawsuit against Facebook, Inc. (now Meta, Inc.), alleging that the company illegally monopolized and stifled competition by acquiring its competitors, notably Instagram and WhatsApp. The case was dismissed by U.S. District Court Judge James Boasberg in the District of Columbia in 2021, driving the state AGs to appeal to the D.C. Circuit in hopes of reviving the case. In January 2022, the U.S. Department of Justice (DOJ) submitted an amicus brief in support of the states' appeal. During oral arguments the state AGs ceded 10 out of 25 minutes to the DOJ.

In the lawsuit, the state AGs allege that Facebook's anticompetitive practices were in violation of federal antitrust laws, specifically the Sherman Act and the Clayton Act. Along with the allegation that Facebook eliminated competition by acquiring rivals, such as Instagram and WhatsApp, the AGs contend that Facebook unlawfully disadvantaged competitors by cutting off their access to its platform and tools, depriving consumers of choices, increasing profits, while eliminating privacy controls and stifling innovation in social networking. In challenging the lower court's decision to dismiss the case, the AGs and DOJ contended that the lower court viewed the allegations "too narrowly" as individual components as opposed to viewing them cumulatively as a whole.

Facebook argued that its purchases were reviewed by antitrust agencies, including the Federal Trade Commission (FTC), without any challenges and

that consumers benefitted from the acquisitions. Although the FTC approved Facebook's acquisition of Instagram and WhatsApp, the FTC filed its own similar lawsuit contemporaneously with the state AGs. Not only do these lawsuits reflect a regulatory priority to break up Big Tech, but they also exemplify the precarious and sometimes inconsistent regulatory climate in which Big Tech operates.

AG Ferguson Secures a $24.6M Penalty Against Facebook

Washington AG Bob Ferguson obtained a $24.6 million award against Facebook's parent Meta to resolve the AG's second lawsuit over alleged campaign finance transparency law violations.

Washington's campaign finance law from 1972 requires campaign advertisers, including entities that host political ads like Meta, to maintain records on Washington political campaign ads, and make the information available for public inspection in a timely manner. The information that must be made available includes costs and sponsors of the ad, along with targeting and reach information, such as the demographics of Washingtonians targeted, and how many individuals viewed the ad. Meta argued that Washington's disclosure law violated the First Amendment because it unfairly targeted political speech and imposed onerous timelines for disclosing "unreasonable degrees of detail to people who request information about political ads." The court rejected Meta's argument and instead granted Washington's motion for summary judgment, finding that Meta intentionally violated Washington's law 822 times since December 2018.

The first lawsuit by AG Ferguson against Meta in 2018 resulted in a consent decree, requiring Meta to pay $238,000 with a commitment to transparency in campaign finance and political advertising. However, Meta allegedly continued to run ads without maintaining the required information, resulting in the second lawsuit in 2020. Due to the intentionality factor, the court had the option to triple the penalty for a maximum of $30,000 per violation. AG Ferguson requested the maximum penalty, resulting in the $24.6 million judgment that included treble damages for costs and fees incurred by the AG's office.

FEDERAL PRIVACY LEGISLATION AND RULEMAKING

In recent history, federal privacy legislative efforts have lagged those of the states. However, in 2022, federal legislators took a significant (although inchoate) step toward developing comprehensive federal privacy protections for all U.S. residents. The bill, which was introduced in the House, demonstrated that privacy is a popular bipartisan issue. By breaking the federal legislative logjam regarding privacy laws, it is possible that 2023 will bring new legislative initiatives, such as algorithmic accountability, geolocation data, and biometric privacy — and maybe even a comprehensive federal privacy law. In the absence of legislation, however, the Biden administration and federal regulatory bodies will continue to aggressively pursue rulemaking activity to develop regulations in response to emerging technologies as they did in 2022.

Federal Lawmakers Take First Swing at Comprehensive Federal Privacy Law

In July 2022, the House Energy and Commerce Committee approved the first federal comprehensive privacy bill by a bipartisan landslide. However, Speaker of the House Nancy Pelosi of California rejected the American Data Privacy and Protection Act (ADPPA) in its current form, preventing the nation's first data privacy law from advancing to the House floor for a vote. Speaker Pelosi's opposition to the bill arose from concerns with the bill's preemption provisions, which would have prevented states from regulating data privacy under state law.

The ADPPA aims to regulate Big Tech and other companies that collect, share, or sell personal consumer information. The ADPPA would have established a "national standard" for data privacy by regulating "covered" entities. "Covered entities" under the act are defined as any entity collecting, processing, or transferring "any information or device that … can be reasonably linked to a person, as well as biometric, genetic and geolocation data."

However, the ADPPA's preemption provisions would have severely limited the states' abilities to concurrently regulate data privacy under state law. While the act allowed state AGs to bring a civil action under the ADPPA, the act's preemption provisions simultaneously prevented states from adopting and enforcing laws "covered by the provisions of the [ADPPA]." As a result, the act would

have prevented states from creating and enforcing their own data protection laws, rendering the ADPPA as the ceiling on data privacy rights in the United States, rather than a floor.

To date, Congress has been unable to resolve the preemption issues. As a result, the burden is on the next Congress to realize the nation's first data privacy act.

Biden Administration Promotes Privacy and Equality With the Blueprint for Artificial Intelligence Bill of Rights

In October 2022, the White House put forth a Blueprint for an AI Bill of Rights, a nonbinding white paper that establishes principles and guidance on automated or artificial intelligence systems. The paper articulates the Biden administration's position on automated decision-making and offers what some experts believe is a broader contextualization of AI harms in its analysis compared to the final guidance on the regulation of artificial intelligence from November 2020 under the Trump administration. The AI Bill of Rights is the result of the White House Office of Science and Technology's year-long process to seek input from community and industry stakeholders, policymakers, and experts.

The paper identifies five pillars or rights for U.S. individuals: (1) the right to be protected from unsafe or ineffective systems; (2) the right to protection from algorithmic discrimination; (3) the right to data privacy; (4) the right to notice and explanation of how AI systems make decisions; and (5) the right to human alternatives. The blueprint then provides high-level guidance on implementing these principles, but ultimately the document is not binding. Rather, it "should be used to inform policy decisions."

While some critics of the U.S.'s AI Bill of Rights call it "toothless," the U.S.'s move on regulation in this area mirrors other countries. In the European Union, regulators first delivered a broad white paper, espousing foundational principles and a framework, then solicited feedback before publishing the proposed AI Act. The AI Act, which is progressing through the EU committees, focuses on reducing the negative effects of AI by creating a complex regulatory regime. Similarly, in July 2022, the U.K. produced high-level guidance on its approach to regulating AI. The developed AI Action Plan and policy paper comprehensively outlines both the approach, as well as next steps for the U.K. regulators. As 2022 draws to a close and 2023 begins, this AI Bill of Rights likely will influence federal agencies (such as the FTC and CFPB) who are already taking action to protect consumers against the perceived harms associated with AI and automated decision making.

Strengthening America's Cybersecurity Act

In 2022, President Biden strengthened the power of federal agencies to investigate cyberattacks by signing the Strengthening American Cybersecurity Act into law. The measure was passed amid rising concerns that Russia's invasion of Ukraine could lead to Russian hackers attacking critical resources, such as hospitals, power plants, or fuel pipelines. The new law shores up cyber defenses by implementing reporting requirements when a cyberattack occurs, as well as by requiring information sharing of such attacks between federal agencies.

The act is a package consisting of three pieces of legislation:

- Cyber Incident Reporting for Critical Infrastructure Act of 2022
- Federal Information Security Modernization Act of 2022
- The Federal Secure Cloud Improvement and Jobs Act of 2022

This legislative package represents a significant step forward for the communication between private and public sector when it comes to issues involving cybersecurity. While the act applies only to critical infrastructure organizations and federal agencies, the framework provides much needed guidance to the private sector. We anticipate that increased regulatory oversight on matters of cybersecurity and improved communications between the private and public sector will bring cybersecurity to the forefront of private companies and help define industry best practices that will have an impact that extends beyond the infrastructure sector.

Infrastructure in the Spotlight

The regulatory cybersecurity landscape for critical infrastructure and utility operators is changing rapidly to meet the increased threats that cybersecurity attacks present to the national security, health, and safety. The federal government appears to be taking an approach that utilizes both a stick and carrot. Stakeholders in critical infrastructure and public utilities must be prepared to respond to new regulations and should consider taking advantage of public incentives to modernize operations and improve cyber defenses. Policies and procedures must be updated to comport with new federal requirements.

(a) Critical Infrastructure Must Soon Report Cyber Incidents to CISA Immediately

In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) into law. CIRCIA applies to the critical infrastructure sector, which includes entities that are "vital to the United States" and whose incapacitation or destruction would have an adverse effect on national security, the economy, or public health and safety. Entities subject to these requirements (covered entities) are those which operate in certain sectors of the economy, such as chemical manufacturing, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial, food, government facilities, health care, information technology, nuclear energy, transportation, and water systems. CIRCIA has the potential to impact a large segment of the U.S. economy.

Many of CIRCIA's requirements fall under the purview of the Cybersecurity and Infrastructure Agency (CISA), which is an agency of the Department of Homeland Security (DHS). Under CIRCIA, CISA acts as a central hub for information gathering and dissemination in efforts to combat cybersecurity threats to critical infrastructure. CIRCIA requires, among other things, the following:

1. Covered entities must alert CISA of a cyber incident within 72 hours from the time the entity reasonably believes an incident has occurred;
2. Any federal entity that receives notice of a security incident must share it with CISA within 24 hours; and
3. DHS must establish an intergovernmental Cyber Incident Reporting Council to harmonize federal incident reporting requirements.

Ransomware is also addressed under CIRCIA. CISA is required to develop regulations that will require any critical infrastructure entity to report ransomware payment within 24 hours; establish a ransomware vulnerability warning program to notify system owners when a vulnerability that could adversely affect the system owners is detected; and develop a joint ransomware task force.

CISA is presently working to implement such regulations. Since September 21, 2022, CISA has engaged in "public listening sessions" across the country. Written comments were due by November 14, 2022. CIRCIA requires CISA to publish a notice of proposed rulemaking (NOPR) within 24 months, but no later than March 2024, and implement final rules no later than September 2025.

(b) Fixing Leaky Cybersecurity for Public Water Infrastructure

The Biden administration is also focused on fortifying the nation's public water systems against cyber threats. CISA has been tasked with working with the U.S. Environmental Protection Agency (EPA) to improve the public water sector's readiness in light of increasing threats to the water supply, which could pose a risk to national security and health.

The Infrastructure Investment and Jobs Act (effective November 15, 2021) requires the EPA to coordinate with CISA and the FBI to develop a support plan for public water systems. The EPA is directed to identify public water systems that if adversely impacted by a cyber event, could impact the health and safety of the public. According to the EPA, there are approximately 148,000 public water systems in the U.S. at present. In August 2022, the EPA signaled that it would issue a mandate, requiring states to inspect approximately 1,600 water systems for cybersecurity threats pursuant to the agency's authority under the Safe Drinking

Water Act of 2018 (SDWA). CISA and the EPA intend to provide guidance, technology, and support for local water suppliers to improve cyber resiliency.

In August 2022, the EPA provided a report to Congress (here), describing its plan and prioritization framework for addressing the cybersecurity needs of the public water system. The EPA is still in the rulemaking stage concerning its mandate to the states, which has been complicated by staffing shortages at the EPA and challenges to the agency's statutory authority in light of the Supreme Court's June 2022 decision in *West Virginia v. EPA*. The EPA is expected to issue an "implementation memo" in early 2023 that will lay the groundwork for the EPA's plan to combat cybersecurity risk.

(c) FERC Attempting to Energize Energy-Sector Cyber Resiliency

Under the Investment and Jobs Act of 2021, Congress directed the Federal Energy Regulatory Commission (FERC) to implement regulations that incentivize shareholders to invest in advanced cybersecurity technology and participate in sharing of cyber threat information. Under the act, FERC is required to implement a framework for utilities to obtain incentives for investments that increase utility cyber resiliency. On September 22, 2022, FERC took the first step in establishing those rules by issuing a Notice of Proposed Rulemaking (NOPR).

The NOPR sought public comment regarding expenditures that should be eligible for the cybersecurity incentive, including capital investments and participation in the threat-sharing program; expenditures that would appear on an established pre-qualified list of eligible expenditures that qualify for the incentives; and the types of incentives that would be offered to participants. Incentives are expected to help companies with expenses incurred in connection with training costs for new cyber practices; costs associated with audits and assessments; software licensing costs; and expenditures related to sharing of cyber threat information with others. Any utility that receives such an incentive is expected to make an informational filing each year on June 1, which details the investments made and the amount of the expenditure.

FERC commissioners are questioning the wisdom of a voluntary participation program in lieu of mandatory cybersecurity requirements, but acknowledge that mandatory requirements would

take much longer to implement. If FERC proceeds with the voluntary participation program, we expect rulemaking activities to occur throughout 2023. The public comment period closed in November 2022.

(d) TSA Places Railroad Carriers On Track for Improved Security

In October 2022, the Transportation Security Administration (TSA) announced a new directive aimed at improving the cybersecurity of the nation's railroads. The directive involves the collaboration of the TSA, CISA, the Federal Railroad Administration (FRA), and the private sector to implement performance-based measures to improve cybersecurity.

Under the directive, every passenger and freight railroad carrier will be required to establish both a TSA-approved Cybersecurity Implementation Plan and a Cybersecurity Assessment Program. The TSA will also specify certain rail carriers that must take the following action in efforts to prevent disruptions and degradation of railroad infrastructure.

For example, freight and passenger rail carriers will be required to:

1. Segment operational technology from information technology systems, so that unaffected systems can continue to operate if one is compromised;
2. Implement strong access control policies to protect against unauthorized access;
3. Develop continuous monitoring systems to detect threats and remediate issues that impact critical systems; and
4. Implement patch management software to ensure that all software is updated.

These directives are in addition to prior directives that required rail carriers to, for example, report cybersecurity incidents to CISA, establish a cybersecurity point of contact, and adopt an incident response plan. The TSA has also indicated that it will begin rulemaking to establish regulatory requirements for the rail sector in the future.

FEDERAL TRADE COMMISSION (FTC)

Lina Kahn completed her first full year as FTC chair in 2022. During that time, the FTC stayed true to its statement of regulatory priorities published in December 2021, which announced the FTC's intent to initiate rulemakings on issues, such as privacy, security, algorithmic decision-making, and unfair methods of competition in the context of cybersecurity and privacy. The statement also highlighted the FTC's emphasis on topics, such as the FTC's review of the COPPA Rule, the Negative Option Rule, and the Endorsement Guides. The FTC has not published a statement of priorities for 2023, but we expect the FTC to continue its aggressive pursuit of companies under Chair Kahn with an emphasis on children's privacy, dark patterns, deceptive advertising, and cybersecurity accountability. Companies should ensure they follow industry best practices for privacy and data security and think carefully about how they use or sell consumer data to avoid becoming the target of an FTC investigation.

FTC Cracks Down on Illegal Online Surveillance of Children

Virtual learning programs and classroom technology use remain critical tools in the modern education system. As students log into these platforms and provide personal information, however, privacy concerns regarding their data have surfaced.

In May 2022, the FTC unanimously adopted a policy statement, committing to protecting children from illegal surveillance as they complete online coursework and attend class remotely. The FTC reaffirmed education technology companies' obligations under COPPA and announced its intent to vigilantly enforce these obligations. In other words, the agency will closely monitor educational technology companies "to ensure that parents are not being forced to surrender to surveillance for their kids' technology to turn on."

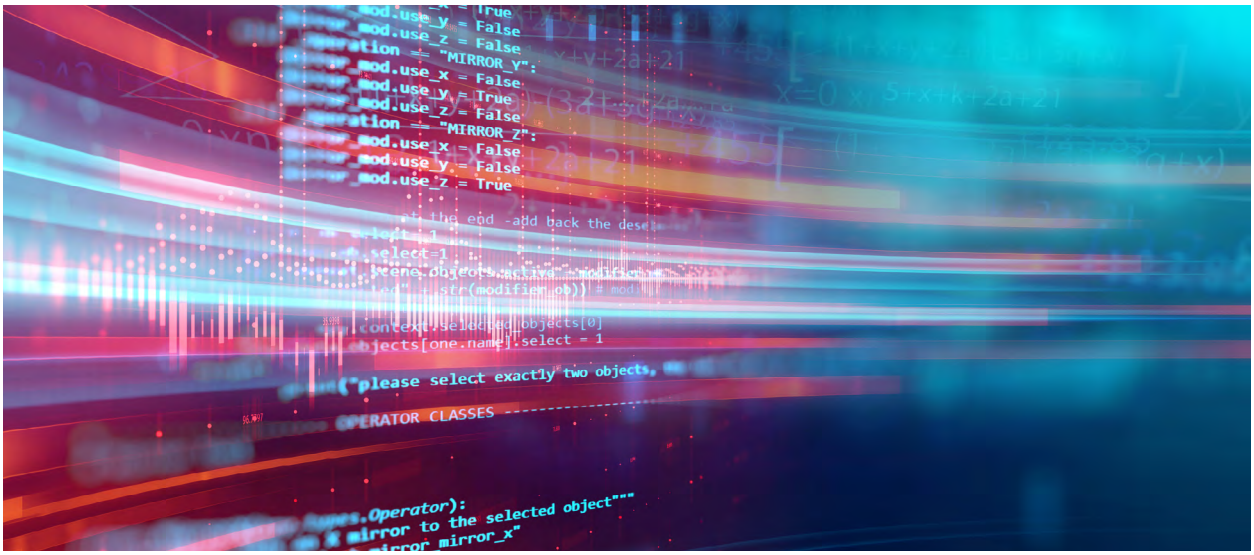
Education technology companies should pay particular attention to constraints regarding data collection, use, retention, and security. Specifically, companies should:

- Only require children to provide information that is reasonably needed for participation in the online educational activity.
- Not use a child's personal information for any other commercial purpose, including marketing or advertising.
- Not retain personal information for longer than necessary to fulfill the purpose for which it was collected.
- Establish reasonable procedures to protect the confidentiality and security of personal information.

Though these requirements are not new, the FTC plans to crack down on education technology companies that improperly collect, use, and store children's personal information with renewed vigor. Companies that utilize data from children should carefully adhere to these principles and develop a stringent compliance program to avoid regulatory scrutiny and hefty civil penalties.

FTC Developing Data Privacy and Cybersecurity Rules

On August 11, 2022, the FTC published an advance notice of proposed rulemaking (ANPR) aimed at commercial surveillance and data security. The FTC invited comments on whether it should undertake rulemaking on the ways companies collect, aggregate, protect, use, analyze, and retain consumer data. The FTC also seeks information on the ways companies transfer, share, sell, or otherwise monetize data using unfair or deceptive methods.



The ANPR highlights the FTC's concerns over commercial surveillance practices, automated systems that analyze data collected by companies, and the increasing use of dark patterns or marketing "to influence or coerce consumers into sharing personal information." In its announcement, the FTC noted that its past work in exercising its authority under the FTC Act to bring enforcement actions against companies for privacy and data security violations suggests that the enforcement of the FTC Act on its own may not be sufficient to protect consumers. The questions raised by the FTC cover a wide range of topics, including the potential harms to consumers and children; the relative costs and benefits of any current practice, as well as those for any responsive regulation; algorithmic error, algorithmic discrimination, and the pros and cons of automated decision-making; the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices; and notice, transparency, and disclosure.

The ANPR included a deadline for filing comments by October 21, 2022, but the FTC extended the deadline until November 21, 2022 to provide adequate time to respond to the questions raised by the ANPR, as well as to help facilitate the creation of a more complete record. Issuing this ANPR is the beginning of the FTC rulemaking process, but its broad scope provides little insight into what formal rule or rules the FTC might formally adopt in the future.

Epic Games Pays Record $520M for Alleged COPPA Violations

Maker of the popular Fortnite video game, Epic Games (Epic), settled with the FTC for $520 million to resolve claims brought against the company. The FTC alleged, among other things, that Epic violated COPPA by improperly collecting children's personal information and violated the FTC Act by using "dark patterns" to dupe millions of players into making unintentional purchases.

Of the $520 million Epic will pay, $275 million is a penalty for violating COPPA by collecting information from children under the age of 13 who played Fortnite without obtaining parental consent. Epic was also accused of violating the FTC Act's prohibition against unfair practices by enabling real-time voice and text chat communications for children and teens by default. The FTC asserted that these default settings, along with Epic's role in matching children and teens with strangers to play Fortnite together, led to scenarios of adult gamers coercing children into sending sexually explicit images, meeting offline, and engaging in other harassing behaviors.

The remaining $245 million of the settlement will be used to refund those who acquired unauthorized charges as a result of "dark patterns" in the Fortnite game, which resulted in users incurring hundreds of millions of dollars in authorized charges.

"Dark patterns" refers to a user interface that is designed to deliberately mislead and coerce users into making unintended or uninformed decisions. Specifically, the FTC took issue with Fortnite's counterintuitive and inconsistent button configuration, which the FTC alleges led users to incur unwanted charges based on a single pressing of the button — and in some instances players were illegally charged for unwanted purchases when waking the game from sleep mode while the game displayed a loading screen.

The $275 million penalty for violating COPPA is the largest penalty ever imposed for violating FTC rules. This historic settlement signals the FTC's commitment to crack down on illegal dark patterns and protecting children's online privacy.

WW International Settles With FTC Over Alleged Collection of Children's Data

In February 2022, WW International (formerly known as WeightWatchers) and its subsidiary Kurbo, Inc. agreed to pay a $1.5 million settlement after the FTC filed a lawsuit in the U.S. District Court of the Northern District of California, alleging that WW engaged in the unauthorized collection of the data of minors.

According to the FTC, WW and Kurbo illegally collected the names, email addresses, and other personal identifying information of Kurbo program users under the age of 13 without first notifying their parents and obtaining parental consent as required by COPPA and Section 5 of the FTC Act. The FTC alleged the Kurbo app's advertising specifically targeted minors as young as eight, used a "non-neutral age gate" that suggested minor app users could register without parental consent so long as they indicated that they were at least 13, and allowed children who entered a false date at the gate to continue using the app even after they later changed their birthdate to reflect their actual age. The FTC also alleged the companies violated COPPA by indefinitely retaining minors' data and only deleting their personal information upon a parent's specific request.

In addition to the civil penalty, WW and Kurbo agreed to delete all minors' data they may have already collected without proper notice and parental consent and to remove any algorithms they used to collect such data. Going forward, under the terms of the settlement, the companies are permanently enjoined from violating COPPA and are only permitted to use data collected from an underage user after properly giving direct notice to the child's parents and receiving parental consent within 30 days. The companies also must develop a publicly available data retention plan that will prevent them from holding any child's data the Kurbo app collects for more than a year after the child's last use of the app.

WW and Kurbo denied targeting children in the app's advertising, inappropriately collecting or monetizing any personal data, and all other alleged wrongdoing, while emphasizing the benefits of their app's healthy lifestyle program.

Twitter Pays $150M After Failing to Comply With 2011 Settlement

In May 2022, the FTC and DOJ filed a complaint against Twitter, Inc. based on alleged violations of a 2011 FTC order that prohibited the company from misrepresenting its privacy and security practices. The FTC alleged that the social media company collected the data of more than 140 million users under the guise of data security protection, but then allowed advertisers to use the data to target users with custom advertisements. After a three-year investigation, Twitter agreed to pay a $150 million penalty and implement significant privacy and security programs and practices.

The 2011 administrative order resolved previous charges that Twitter deceived its customers and put them at risk by neglecting to protect their personal information. The FTC alleged that poor data security allowed hackers to gain control of Twitter and access public and private user information, as well as send tweets from any account. As a result of the incident, the settlement barred Twitter from misleading consumers about security, privacy, and confidentiality of consumer information for 20 years.

Yet, from 2013 through 2019, Twitter collected users' phone numbers or email addresses to improve account security, which it did by implementing two-factor authentication and enabling account resets. However, Twitter also used this data to

allow advertisers to serve specific consumers targeted ads by allowing advertisers to match phone numbers and email addresses to information separately collected from data brokers. Twitter allowed such use of consumer data without adequately disclosing the practice to consumers in violation of the 2011 order.

In addition to the $150 million penalty, Twitter agreed to notify users who joined Twitter after 2019 of the company's alleged misuse of their information, conspicuously post the company's privacy and security policies, and allow users to use multifactor authentication methods that do not rely on a phone number. Twitter is also required to implement comprehensive security and privacy policies, notify the FTC if the company experiences a data breach, and limit employee access to user personal data. Some have questioned whether the $150 million penalty was sufficient when most of Twitter's $3.5 billion revenue is derived from advertising sales.

FTC Sues Kochava for Selling Sensitive Geolocation Data

Kochava aggregates and sells data to customers for use in advertising and marketing initiatives. The data includes precise, timestamped location information from consumers' mobile devices. In addition to monthly subscription sales, Kochava offered a free data sample to the public until June 2022.

The FTC filed a lawsuit against Kochava in August 2022, alleging violations of the FTC Act and seeking to enjoin Kochava's business practices. More specifically, the lawsuit alleged that distributing sensitive data, such as precise timestamped location data, constitutes a violation of the FTC Act because the practice could cause substantial unavoidable injury to consumers. The concern stemmed from the fact that the geolocation data allowed the public to track consumers' movements to and from sensitive locations like reproductive health clinics, places of worship, mental health care providers, addiction recovery centers, homeless shelters, and shelters for survivors of domestic abuse.

Because the location data is timestamped, those with access to the database may be able to ascertain a specific consumer's home address and discover the user's identity. The FTC alleges that access to such sensitive location information can expose identified consumers to "stigma, discrimination, physical violence, emotional distress, and other harms."

Kochava moved to dismiss the lawsuit in October 2022. It argued not only that there was no violation of the act, but also challenged the FTC's constitutional authority to prosecute the claims in the first place. The ongoing litigation demonstrates the FTC's commitment to privacy-related policy goals in 2022. Looking ahead to 2023, the litigation will also serve as an important part of the national conversation regarding the scope of federal agencies' influence under broad legislative grants of authority, such as the FTC Act.

CafePress Investigated for Data Breach Coverup

In June 2022, the FTC finalized a consent order against former CafePress owner Residual Pumpkin Entity LLC and current owner PlanetArt LLC for failure to implement reasonable security measures to protect sensitive buyer and seller information, such as passwords and Social Security numbers, stored on its network. CafePress provides online storefront and website hosting, order management, fulfillment management, and payment processing, among other activities, for its customers.

The complaint, which the FTC brought in March 2022, alleged that CafePress' failure to implement basic security measures resulted in multiple data breaches. CafePress later fixed the errors but failed to investigate for several months after learning of the breaches. Eventually, foreign governments warned CafePress about the breaches and urged it to notify customers. Instead of issuing an urgent notification to affected users, the company simply instructed customers to reset their passwords as part of an update to the password policy. In some instances, CafePress closed user accounts and charged each of them a $25 account closure fee.

As part of the consent order, CafePress' former owners were required to pay $500,000 to the affected businesses and bolster security measures by adding encryption, multifactor authentication, and complete mandatory third-party assessments of the company's security measures. Given the alleged security failures, troublesome business practices, and concealment of the compromises, the $500,000 settlement could be viewed as a lenient outcome for CafePress and its owners.

FTC Holds Drizly CEO Individually Accountable

In October 2022, the FTC announced a proposed consent order with Drizly and its CEO, stemming from a 2020 data breach at the company. The order holds company CEO Cory Rellas individually accountable, signaling the FTC's focus on executive and management accountability for a company's cybersecurity practices.

Drizly is an online marketplace through which consumers can place orders for the delivery of alcoholic products from local retailers. In connection with this service, Drizly collects customers' personal information, including email, mailing addresses, phone numbers, device identifiers, and other information. After a 2020 data breach — resulting from the use of a compromised employee account — the FTC issued an administrative complaint and the order. The complaint alleges that Drizly and Rellas failed to implement basic security measures, such as multifactor authentication, written security procedures, employee security training, secured storage of personal information, or monitoring for security threats.

The order is unusual in that it names Drizly's CEO personally. In a joint statement, FTC Chair Lina Khan and Commissioner Alvaro Bedoya said: "Holding individual executives accountable … can further ensure that firms and the officers that run them are better incentivized to meet their legal obligations." The order requires that Rellas implement an information security program at any company he may move to during the next 10 years. In addition, the order requires Drizly to provide an annual certification from its CEO that Drizly has implemented the requirements of the order and is not aware of any material noncompliance.

If the order is finalized, Drizly must (1) implement a mandated information security program, (2) destroy and confirm the destruction of all data not being used to provide services to customers, (3) not misrepresent the way it uses customer data, and (4) obtain a biennial assessment from a "qualified, independent, third-party" assessor.

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB)

CFPB Director Rohit Chopra had an active year in 2022 as the Bureau made its priorities under the Biden administration clear. From empowering states to enforce federal consumer financial laws, to developing cybersecurity rules for the nonbank financial sector, the CFPB sought to assert itself as one of the nation's most active regulatory bodies when it comes to consumer protections and privacy/cybersecurity related topics. The end of 2022 saw the Bureau commence an enforcement action on October 18, 2022 into ACTIVE Network's alleged use of dark patterns, which may have major ramifications for Big Tech, fintech, and all consumer-facing subscription-based services. The Bureau's activity in 2022 was shadowed by the Fifth Circuit Court of Appeals decision, which held that the Bureau's funding mechanism was unconstitutional. While the Bureau has filed a certiorari petition for review to the Supreme Court, the pending appeal and related uncertainty may significantly impact CFPB activity in 2023.

CFPB Takes Action to Protect the Public From Cybersecurity Failures

On August 11, 2022, the CFPB confirmed that entities may violate the prohibition on unfair acts or practices as described in the Consumer Financial Protection Act of 2010 (CFPA) when they lack sufficient cybersecurity practices, even in the absence of a breach or intrusion. The CFPA defines practices to be "unfair" when they "cause or are likely to cause substantial injury that is not reasonably avoidable or outweighed by countervailing benefits to consumers or competition." Although a violation of this provision of the CFPA is "fact-specific" the Bureau highlighted a few common practices that increase a company's probability of violating the law.

In a circular published by the CFPB, the Bureau informed the nonbank financial services industry that inadequate security measures, such as inadequate authentication, password management or software update policies or practices for company's collection, processing, maintenance, or storage of sensitive consumer information can constitute an unfair practice. The CFPB maintains that such practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, for example, data breaches, cyberattacks, exploits, or ransomware attacks.

Consumers are typically unaware of a company's practices and do not have control to prevent the injury or risks of harm associated with cybersecurity shortcomings. Further, a company's failure to implement sound cybersecurity practices does not provide countervailing benefits to consumers such that the risks are outweighed by any benefit. Accordingly, the CFPB noted that "[g]iven the harms to consumers from breaches involving sensitive financial information, this is not surprising." The Bureau cited numerous examples to support its claim, including its 2019 complaint against Equifax in which the Bureau alleged an "unfairness violation based on Equifax's failure to provide reasonable security for sensitive personal information it collected, processed, maintained, or stored within computer networks."

The Bureau specifically highlighted the three common practices that increase a company's chances of violating the CFPA:

1. Not utilizing multifactor authentication;
2. Not enforcing strong password management policies; and
3. Failing to update and patch software on a timely cadence.

While the three practices highlighted by the Bureau do not complete or substitute for a comprehensive cybersecurity program, the specific guidance is a welcome occurrence in a regulatory environment that is historically vague when it comes to cybersecurity expectations. Companies that fail to adhere to the basic guidance from the CFPB do so at their own risk.

CFPB Begins Comprehensive Privacy Rulemaking Process

In October 2022, the CFPB began weighing options to give consumers increased access to their own data under Section 1033 of the Dodd-Frank Act. For example, the Bureau proposed a policy that would require financial institutions to make consumer financial information — such as payment history and other banking transaction records — available at the consumer's request. Consumers would also be able to request that financial institutions make such records available to third parties.

The CFPB hopes that its proposed changes will facilitate consumers' ability to switch between financial institutions, which will in turn "fuel market competition" and incentivize institutions to provide improved services. The CFPB also hopes to protect consumers by allowing financial institutions to use consumer data only for purposes that the consumer intends. By clarifying consumers' data rights, the CFPB aims to give individuals more leverage and bargaining power in the marketplace.

In other words, the CFPB took the first step toward major change in 2022. As required by Dodd-Frank, the Bureau also started soliciting feedback on its initial proposals from a small business review panel. 2023 will bring additional information about the Bureau's plans for new policies that are certain to have a significant impact on the consumer financial services industry and data privacy moving forward.

CFPB Sues Payment Platform Over Dark Patterns

On October 18, 2022, the CFPB sued ACTIVE Network, a third-party registration and payment processing company, for alleged unfair, deceptive, and abusive acts and practices. The company's services are used by organizers of charity races, youth camps, and other events, such as YMCA, Girl Scouts, and other charity race organizers. In the complaint, allegations involve use of dark patterns, which are design features used to deceive, steer, or manipulate users into behavior that is profitable for a company but often harmful to users or contrary to their intent. Specifically, the CFPB alleges that ACTIVE engaged in dark patterns in violation of the Consumer Financial Protection Act (CFPA) and the Electronic Fund Transfer Act (EFTA) by unlawfully enrolling consumers into a discount club and charging junk fees among other violations. This lawsuit demonstrates the CFPB's efforts to fight against a rising epidemic of deceptive marketing practices through the use of dark patterns.

According to the complaint, ACTIVE engaged in dark pattern marketing by offering a free trial enrollment in a discount club membership called "Active Advantage" during the registration process for a charitable event. Many consumers clicked on the highlighted button — usually labeled "Accept" — under a reasonable belief that they were accepting charges to participate in the event. However, the consumers actually enrolled in the Active Advantage membership, which automatically converted to a paid subscription with an annual fee unless affirmatively canceled. CFPB alleged that ACTIVE generated more than $300 million in membership fees as a result of the dark pattern practices.

CFPB Director Rohit Chopra articulated the Bureau's position by stating that the CFPB is "closely watching whether financial services firms are deploying digital dark patterns. … [CFPB has] also worked to give designers and other tech workers more tools to serve as industry whistleblowers," and the CFPB is looking at a range of ways to reduce unwanted junk fees. At the National Association of Attorneys General Capital Forum on December 7, 2022, Chopra reiterated how junk fees in financial industry are prevalent all around us and stated that we "cannot live in a country of junk fees."

U.S. DEPARTMENT OF JUSTICE (DOJ)

For the DOJ, 2022 showcased the department's broad oversight in the realm of regulatory privacy and cybersecurity. In the first full year of its Civil Cyber Fraud Initiative, the department made headlines prosecuting and securing large settlements and civil penalties from companies and individuals alike — often doing so in conjunction with other federal agencies and state AGs. The DOJ, particularly its Office of Privacy and Civil Liberties, is set to have a busy 2023 as the department continues its cyber initiative, looks to implement several of President Biden's privacy-related executive orders, continues to support other state and federal regulatory investigations and initiatives, and faces calls to reconsider the enforcement and development of privacy policies in light of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*.

Civil Cyber Fraud Initiative Secures Two False Claims Act Settlements

Through its Civil Cyber Fraud Initiative, the DOJ obtained two sizeable settlements this year with Comprehensive Health Services (CHS) and Aerojet Rocketdyne, Inc. (Aerojet) for alleged FCA violations. These settlements emphasize that government contractors must comply with cybersecurity and privacy requirements in federal contracts and the applicable Federal Acquisition Regulations (FARs).

In October 2021, the DOJ announced the launch of its Civil Cyber Fraud Initiative, which is tasked with mitigating risk from emerging cyber threats by combining the department's expertise in civil fraud enforcement, government procurement, and cybersecurity. The initiative targets companies and individuals that place U.S. information or systems at risk by providing products or services not consistent with federal cybersecurity and privacy requirements. As relevant to the CHS and Aerojet settlements, the initiative also employs the FCA as an avenue to pursue cybersecurity-related fraud by government contractors and grant recipients.

As to CHS, the government asserted that CHS did not disclose its failure to consistently store patients' medical records on a secure electronic medical record (EMR) system, as was required under its contract. CHS charged the State Department

for EMR but failed to disclose that it also stored the records in unsecure locations, which led the government to assert that it did not receive the benefit of its bargain with CHS (*i.e.*, secure storage of medical records). CHS ultimately agreed to pay $930,000 to resolve the FCA allegations.

As to Aerodyne — which provides propulsion and power systems for launch vehicles, missiles, satellites, and other space vehicles to the Department of Defense, NASA, and other federal agencies — the government asserted that the company violated the FCA by misrepresenting its compliance with cybersecurity requirements for federal contracts. Aerojet agreed to pay $9 million to resolve the allegations.

These settlements make clear that the DOJ has renewed its focus on combatting cyber fraud. The DOJ will continue to target companies that knowingly provide products and services that do not comply with contractual cybersecurity requirements, so companies must carefully evaluate the requirements that apply to their contracts — both before and during their contractual performance. Whether concerning fraud, cybersecurity misrepresentations, or other types of misconduct, we expect a new wave of state and federal FCA cases — potentially spurred by whistleblower action — to surface in the coming years.

Uber CSO Convicted for Covering Up Data Breach

In a first-of-its-kind prosecution and conviction, former Uber Security Chief Joseph Sullivan was found guilty on charges related to a 2016 data breach at the company. During that breach, hackers stole the personal information of 57 million Uber passengers and drivers and extorted $100,000 from the company. Sullivan was accused of making the payoff to the criminals without notifying in-house counsel or the regulators who were investigating an earlier breach at Uber.

In 2014, the FTC was investigating another data breach at Uber. During the course of the investigation, Sullivan prepared and signed off on submissions to the FTC, but concealed the 2016 incident, which occurred in the course of the FTC's 2014 investigation. He also failed to disclose the incident to company attorneys working on the FTC investigation. Ultimately, Sullivan's lack of candor led to the DOJ's successful prosecution of two criminal counts: obstructing a government investigation and concealing the theft of personal data. In 2018, the company agreed to a $148 million settlement with all 50 U.S. states related to the data breach coverup. Sullivan's prosecution and conviction followed.

Sullivan faces a maximum sentence of eight years in prison, as well as several hundred thousand dollars in fines. While the details of this event make it unique, it serves as a warning to cybersecurity professionals to be transparent in the wake of a data breach. Regulators are increasingly holding company management individually accountable for cybersecurity and privacy failures — especially when there is an element of knowing disregard or intentional obfuscation.

SECURITIES EXCHANGE COMMISSION (SEC)

SEC Seeks to Hold Management Accountable for Cybersecurity

In March 2022, the SEC proposed amendments to its rules concerning cybersecurity risk management, strategy, governance, and incident disclosure. The rules, which are designed to enhance standardized cybersecurity-related disclosures, would apply to public companies. In addition, the SEC intends for the rules to "strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting," according to SEC Chair Gary Gensler.

In particular, the rules would require a series of additional reporting requirements. These include: (1) current reporting about material cybersecurity incidents, as well as periodic reporting providing updates about past cybersecurity incidents, (2) periodic reporting about the company's policies and procedures to identify and respond to security incidents, (3) periodic reporting about the board of directors' oversight of cybersecurity risk, (4) periodic reporting about management's oversight and management of cybersecurity risk and policies, and (5) annual reporting or proxy disclosures regarding the board of directors' cybersecurity expertise. The imposition of obligations on the boards of directors of public companies represents a significant change in the SEC's public reporting requirements.

While the notice and comment period for the rules ended on May 9, 2022, a final implementation date has not yet been announced. Nevertheless, publicly traded companies should review their cybersecurity policies to ensure that the company is documenting the involvement of the board and management in matters pertaining to the company's cybersecurity program, risk management, and decision-making processes.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Proposed Rulemaking for Recognized Security Practices Under HIPAA and HITECH

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) sought feedback on certain provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) in April 2022. The request for information focused on two primary topics: (1) implementation of recognized security practices and (2) distributing monetary penalties to individuals harmed by HIPAA violations.

First, OCR requested information on covered entities' voluntary implementation of recognized security practices. Under HITECH, OCR must consider successful implementation of these practices when making determinations about fines, audits, and other resolutions of potential HIPAA violations. To better comprehend the policy and its effects, OCR sought additional information about how covered entities understand and implement these recognized security practices, including the specific policies that entities planned to use. Finally, it requested feedback on best practices for demonstrating the existence of recognized security practices within an organization.

Second, OCR requested feedback regarding a proposal to distribute civil monetary penalties or settlements to harmed individuals. Many of the specific questions that OCR revolved around defining "compensable individual harm" and identifying the circumstances in which harmed individuals would qualify for compensation.

The comment period ended in June 2022. OCR released a video presentation in November 2022, explaining how entities can reduce liability through recognized security practices and clarifying the process for demonstrating successful implementation. Nevertheless, OCR has not yet taken significant action based on the solicited comments. In the new year, stakeholders should continue to watch for guidance and rulemaking with respect to these policies — indeed, successful implementation of recognized security practices could help entities better guard against costly HIPAA compliance issues by defining objective criteria to measure cybersecurity compliance.

STATE PRIVACY LAW SURVEY

Current as of 12/1/2022

Currently Enacted State Privacy Legislation

State	Title	Purpose	Effective Date
California	California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 et seq.)	To give California consumers control over the personal information businesses collect about them by giving consumers the right to know, right to delete, right to opt out of sale, and right to nondiscrimination relating to their personal information. The act also requires businesses, such as data brokers, to provide certain notices explaining their privacy practices.	Jan. 1, 2020
	California Consumer Privacy Rights and Enforcement Act of 2020 (Proposition 24)	To significantly amend and expand the CCPA's consumer protections and business requirements, create the California Privacy Protection Agency, and remove businesses' ability to remedy violations before being penalized.	Jan. 1, 2023
	Political Reform Act of 1974: Business Entities: Online Advocacy and Advertisements (CA SB 746)	To require a business entity to report to the secretary of state any use of its products or services to alter online search results to emphasize or deemphasize materials containing express advocacy, or to target online advertisements for political purposes.	Sept. 30, 2022
	The California Age-Appropriate Design Code Act	To require businesses that provide online services, products, or features likely to be accessed by children to comply with specified requirements, including configuring all default privacy settings offered by social media platforms using clear language suited to the age of children accessing the platform. The act also strictly limits the permitted use of child user's information and requires social media companies to consider the best interest of the child when doing so.	July 1, 2024

State	Title	Purpose	Effective Date
Colorado	Colorado Privacy Act of 2021 (SB 21-190)	To enact a comprehensive consumer privacy and data protection act designed to protect the personal data of Colorado residents when they act in an individual or household context.	July 1, 2023
Connecticut	Personal Data Privacy and Online Monitoring Act of 2022 (SB 6)	To enact a comprehensive consumer privacy and data protection act that will give Connecticut consumers the right to request information about whether their data is being proceeded, to opt out of processing activities like targeted advertising, to obtain copies of their collected data, and to request corrections to their collected data.	July 1, 2023
Kentucky	Genetic Information Privacy Act (KY HB 502)	To regulate the collection, use, and disclosure of genetic information. The bill also creates a civil cause of action for violations to be brought by the state AG.	June 1, 2022
Maine	Data Collection Protection Act (ME HB 669)	To prohibit data collectors from collecting or aggregating, selling, or using certain types of public documents or information from those documents to determine a consumer's eligibility for consumer credit, employment, or residential housing. The act also creates the Maine Data Protection Agency.	Aug. 8, 2022
Maryland	Genetic Information Privacy: Consumer Protection and Forensic Genealogy (MD HB 0866)	To regulate the use of genetic data by direct-to-consumer genetic testing companies.	Oct. 1, 2022
Virginia	Virginia Consumer Data Protection Act of 2021 (HB 2307, SB 1392)	To enact a comprehensive consumer privacy and data protection act, regulating the collection and processing of Virginia residents' personal data and giving them rights to control such data.	Jan. 1, 2023
Wyoming	Wyoming Genetic Data Privacy Act (WY HB 0086)	To protect consumers' genetic information by prohibiting the collection, retention, or disclosure of genetic data. The bill also provides for a civil cause of action to be brought by the state AG.	July 1, 2022

Selection of Significant Pending State Privacy Legislation

State	Title	Purpose	Status
Arizona	AZ HB 2790	To enact a comprehensive state consumer privacy and data protection bill relating to personal data, processing, and security standards.	Pending in committee
California	CA SB 1189	To require private entities in possession of biometric information to develop and make publicly available a written policy establishing a retention schedule and guidelines for permanently destroying the biometric information. The bill would also severely restrict the collection and use of such information.	Voted from committee with no further action on Nov. 11, 2022
	CA AB 2486	To create the Office for the Protection of Children Online within the California Privacy Protection Agency (CPPA).	Voted from committee with no further action on Nov. 11, 2022
Illinois	IL HB 4569, 4692, 5396 I IL SB 3413, 3782, 3874	To amend certain provisions of the BIPA, including by changing the definition of biometric information, establishing a one-year statute of limitation, providing a 30-day cure period, eliminating statutory damages, and eliminating the private right of action.	Pending in committee
	IL HB 3453	To enact the Geolocation Privacy Protection Act, which would provide that a private entity that owns, operates, or controls a location-based application on a user's device may not disclose geolocation information from a location-based application to a third party unless the private entity first receives the user's affirmative express consent after providing a specified notice to the user.	Pending in committee
	IL HB 2404	To enact the Right to Know Act, which would require companies to inform consumers of the types of information they collect and disclose to third parties.	Pending in committee

State	Title	Purpose	Status
	IL SB 2080	To enact the Automatic Listening Exploitation Act, which would make it unlawful for a person who provides any smart service through a proprietary smart speaker or security monitoring through a video doorbell to make, store, or transmit recordings without express informed consent.	Pending in committee
	IL SB 2081	To enact the Keep the Internet Devices Safe Act, which would provide that no private entity may turn on or enable a digital device's microphone unless the registered owner or person configuring the device is provided certain notices in a consumer agreement or privacy notice.	Pending in committee
	IL SB 3081	To enact the Do Not Track Act, which would prohibit a party to a user action from tracking another user whenever the party receives a do-not-track signal, indicating a user preference not to be tracked with some exceptions.	Pending in committee
Massachusetts	MA HB 142	To enact the Massachusetts Information Privacy Act, a comprehensive consumer privacy and data protection act.	Pending before the House
	MA HB 521	To regulate the collection, use, disclosure, and dissemination of personal information from customers of telecommunications or internet service providers.	Pending before the House
	MA HB 4514	To enact the Massachusetts Information Privacy and Security Act, updating and expanding many state data privacy and security laws.	Pending before the House
	MA SB 46	To enact the Massachusetts Information Privacy Act, a comprehensive consumer privacy and data protection act also covering biometrics.	Pending in committee

State	Title	Purpose	Status
	MA SB 220	To enact the Biometric Information Privacy Act, regulating the collection, retention, destruction, and disclosure of consumers' biometric data.	Pending before the Senate
Michigan	Mi HB 5989	To create a comprehensive consumer privacy and data protection act.	Pending in committee
Missouri	MO HB 2716	To establish the Biometric Information Privacy Act, which would prohibit collection of biometric information absent written informed consent and require entities in possession of such information to develop a publicly available retention and destruction policy.	Pending in committee
New Jersey	NJ AB 505	To enact the New Jersey Disclosure and Accountability Transparency Act, a comprehensive consumer privacy and data protection act, establishing requirements for the disclosure and processing of personal information and creating the Office of Data Protection and Responsible Use in Division of Consumer Affairs.	Pending in committee
	NJ AB 525	To define DNA samples and genetic information obtained from DNA analyses as the property of the person sampled or analyzed.	Pending in committee
	NJ AB 2951	To enact the Microphone Enabled Devices Act, which would require user consent before a device's microphone can be enabled.	Pending in committee
	NJ AB 3262 | NJ SB 1413	To enact the Reader Privacy Act, which would extend reader privacy protections to book purchases, including the purchase of electronic books.	Pending in committee
	NJ AB 3503	To prohibit television voice recognition features from being activated without notice and to prohibit the use or sale of voice recordings for advertising purposes.	Pending in committee

State	Title	Purpose	Status
New York	NY AB 27 | NY SB 1933	To enact the Biometric Privacy Act, which would require entities in possession of biometric information to develop a publicly available retention and destruction policy.	Pending in committee
	NY AB 405 | NY SB 2886	To enact an online consumer protection act, requiring advertising networks to post clear and conspicuous privacy policy, data collection, and use practices related to its advertising activities.	Pending in committee
	NY AB 589 | NY SB 5879	To require retailers to post warning signs if they track consumers through cell phones or other devices and to provide civil penalties if they fail to warn consumers.	Pending in committee
	NY AB 680 | NY SB 6701	To enact the New York Privacy Act, requiring companies to disclose their methods of de-identifying personal information, placing special safeguards around data sharing, and allowing consumers to obtain the names of all entities with whom their information is shared.	Pending in committee
	NY AB 733	To require express consent before an entity may collect, store, or transmit any personal information obtained from a smart home connected system.	Pending in committee
	NY AB 3586 | NY SB 4021	To enact the It's Your Data Act, which would provide protections and transparency in the collection, use, retention, and sharing of personal information.	Pending in committee
	NY AB 3709 | NY SB 567	To grant consumers the right to request from businesses the categories of personal information a business has sold or disclosed to third parties.	Pending in committee
	NY AB 4137 | NY SB 154	To require signed written consent before a manufacturer of a smart speaker may store any voice recordings.	Pending in committee
	NY AB 6042	To enact the Digital Fairness Act, a comprehensive consume privacy and data protection act.	Pending in committee

State	Title	Purpose	Status
	NY AB 9027 | NY SB 8317	To require the disclosure to a parent of the personal information and content about a minor collected by an operator of an internet platform upon request.	Pending in committee
	NY SB 6727	To enact the Data Economy Labor Compensation and Accountability Act, establish the Office of Consumer Data Protection, and impose a tax on data controllers and processors who are required to register with that office.	Pending in committee
Ohio	OH HB 376	To enact the Ohio Personal Privacy Act, a comprehensive consumer privacy and data protection act.	Pending before the House
	OH HB 414	To enact the Not on My Walk Act, which would regulate the sale and connectivity function of consumer electronic devices, or "attached consumer devices" that are capable of sending or receiving data over the internet and permitting other ancillary consumer devices to connect to the internet through the attached consumer device.	Pending before the House
Pennsylvania	PA HB 1126, 2202, 2257	To enact a comprehensive consumer privacy and data protection act.	Pending in committee
	PA HB 1908	To identify and protect information collected by smart technology devices, to establish the Smart Technology Disclosure Fund, and to provide the state AG with powers and duties to safeguard consumers.	
	PA HB 2283	To protect consumer genetic privacy by regulating the disclosure of information collected by genetic material testing entities.	Pending in committee
Rhode Island	RI HB 5509	To prohibit the sale for profit of consumer generated internet data by a social media platform without the consent of and compensation paid to the consumer.	Held in committee for further study

State	Title	Purpose	Status
	RI HB 5959	To enact the Rhode Island Transparency and Privacy Protection Act, which would require online service provides and commercial websites that collect, store, and sell personally identifiable information to disclose what categories of such information they collect and third parties that purchase the information.	Held in committee for further study
	RI HB 7400	To enact the Rhode Island Data Transparency and Privacy Protection Act, identifying information collected by online service providers and commercial websites.	Held in committee for further study
	RI HB 7917	To enact the Rhode Island Information Privacy Act, allowing an individual to access and learn what personal information about the individual has been collected and stored by covered entities.	Held in committee for further study
Virginia	VA SB 419	To protect consumer genetic information privacy by establishing certain notice requirements and disclosure prohibitions for genetic testing companies.	Continued by the Senate to 2023
Washington, D.C.	DC B 451	To enact the Uniform Personal Data Protection Act, which would establish information practice principles applicable to the collection and use of personal data from consumers by businesses.	Pending in committee