SheppardMullin

EYE ON PRIVACY: 2023 YEAR IN REVIEW

These articles appeared in the "Eye On Privacy" Blog in 2023
(www.eyeonprivacy.com)

Sheppard Mullin's 2023 Eye on Privacy Year in Review

It is hard to believe that another year is upon us! As we have done in years past (2022, 2021, 2020, 2019 and 2018), we have created a comprehensive resource of all our www.eyeonprivacy.com posts from 2023. As you move forward with your privacy program and risk management for 2024, we hope that this compilation of developments from 2023 is helpful.

From the expansion of "general privacy" laws in US states and concerns over cross-border data transfers, to global focus on artificial intelligence, surveillance and dark patterns, 2023 was a busy year. We hope that this is again a useful tool to help prepare for privacy and cybersecurity program plans for the year.

Sheppard Mullin Privacy & Cybersecurity Team

Our group includes some of the most respected lawyers in the privacy space, including a lawyer who literally "wrote the book" on data breach, award-winning privacy class action litigation practitioners, and leading EU-based data protection experts. Our accolades include being highly ranked by Legal 500 USA (Cyber Law) and Legal 500 Europe (EU Data Protection), and we were one of only 25 firms ranked in the inaugural ATL Top Law Firm Privacy Practice Index.

Nearly every facet of a company's operations—from internal employment practices to online operations, data collection, and customer contact—is subject to a complex array of legal and business challenges related to privacy. Our team recognizes that companies need practical advice from experienced counsel who thoroughly understand privacy law. We partner with clients to help them extract value from the data they collect, while identifying and addressing regulatory compliance requirements, and ensuring that data is appropriately protected.

Our lawyers have experience responding to high-profile data breaches and the regulatory investigations, Congressional oversight, and litigation that often follow such incidents. In addition, as data becomes more entwined with the enterprise value of businesses, we conduct data and privacy compliance due diligence in connection with mergers and acquisitions and other corporate and strategic transactions.

CONTENTS

CONTENTS

ARTIFICIAL INTELLIGENCE

What is the Privacy Impact of the White House AI Order for Businesses?

Posted November 28, 2023

Biden's sweeping AI Executive Order sought to have artificial intelligence used in accordance with eight underlying principles. The order, while directed to government agencies, will impact businesses as well. In particular, the order has privacy and cybersecurity impacts on companies' use of artificial intelligence. Among other things, companies should keep in mind the following:

- **NIST Guidelines:** The order calls for industry guidelines and best practices for deploying AI systems. These are to be created by the end of July 2024 by NIST, and include guidelines for AI developers as well as guidelines for assessing the safety and security of AI systems.
- **Critical Infrastructure**: The order outlines steps to be taken to manage AI in critical infrastructure and cybersecurity. Included in these is requiring the Treasury to issue a best practices report to financial institutions by the end of March 2024.
- **Protect Consumers from Harm**: The order outlines several steps to promote competition and protect individuals from potential harm. This includes potential FTC rulemaking. The order also asks all independent regulatory agencies to consider steps to protect consumers from AI-related risks. These include privacy risks. Listed agencies include HHS, the Department of Transportation the Department of Education, and the Federal Communications Commission. Time frames for the agencies to take action range from three months to a year.
- **Federal Agency Procurement**: The order calls for the Office of Management and Budget to review what "commercially available information" (CAI) is procured by agencies. Especially when the CAI includes personal information and/or is obtained from data brokers. After that review OMB is called on to take issue recommendations on how these activities can be done in a way that "mitigates privacy and confidentiality risks."

As illustrated from the Fact Sheet accompanying the order, these are just some of many directives it contains. Other issues covered in the order include intellectual property, federal use of AI, and national security.

PUTTING IT INTO PRACTICE: There is time before we see the outcome of the action agencies have been directed to take under the order. In the meantime, companies are reminded that the measures it outlines -protecting consumers from privacy and security harm- are already expected by the FTC.

FTC Vocalizes AI Voice Cloning Challenge

Posted November 17, 2023

The FTC continues its focus and concern on use of technologies that integrate artificial intelligence, this time turning to potential consumer harm with voice cloning technology. Today the commission announced a challenge looking for solutions to help monitor and prevent malicious voice cloning. In the announcement, the FTC pointed to current scams where threat actors use cloned voices -created using AI tools- to conduct scams. For example, money requests from a person's "relative." The winner will receive a $25,000 prize, and entries will be accepted in the first weeks of January.

PUTTING IT INTO PRACTICE: The FTC has used challenges in the past for issues that are of particular concern within the agency, including one in 2017 to address security vulnerability for IoT devices. We expect to see continued focus on AI from the FTC (and others), as this challenge and its enforcement actions demonstrate.

Scraping the Bottom of the Barrel: X Corp. Sues Bright Data Over Site Scraping

Posted August 29, 2023

X Corp., the company formerly known as Twitter, recently sued Bright Data over its site scraping activities. Bright Data is a data collection company and advertises—among other services—its "website scraping" solutions. Scraping is not new, nor are lawsuits attempting to stop the activity. We may, though, see a rise in these suits with the rise in companies using them in conjunction with generative AI tools.

This case -and the counts X is alleging- serves as a reminder of the concerns that platforms have about scraping practices. In particular, social media sites that allow users to post personal information. (Indeed, in January Meta filed a similar suit against a different data collection platform). Namely, X has argued:

- *Breach of contract*: X's terms of service, like those of most platforms, prohibits scraping ("scraping the Services without our prior consent is expressly prohibited"). X argues that by scraping usernames, tweets, and even more granular data about users, Bright Data violated that online contract with X.
- *Tortious interference with contract:* Bright Data, in addition to scraping itself, also sells scraping tools. Third parties can use these tools to scrape the data on their own. X argues that by providing these tools, Bright Data is helping others violate X's contracts with those third parties.
- *Unjust enrichment*: Finally, X argues that Bright Data's receipt of financial benefits (selling the data obtained from scraping) constitutes unjust enrichment.

In addition to a preliminary and permanent injunction, X is also asking that Bright Data identify all recipients of information scraped from the X platform.

PUTTING IT INTO PRACTICE: With the rise of artificial intelligence and other passive information collection activities, this case is a reminder to those considering using information gathering tools. If using online information gathering tools, do diligence to understand how the information has been gathered.

OpenAI – FTC OpensAnInvestigation

Posted August 28, 2023

As many who are keeping track of generative AI developments are aware, the FTC recently announced that it is investigating OpenAI's ChatGPT product. For the privacy practitioner this investigation is important given that among other things, the agency wants to understand better how OpenAI is using personal information, and if its privacy representations are sufficient.

Areas that the FTC has requested to learn more about in the civil investigative demand sent to OpenAI suggest that these will be things that the FTC looks at for any creating -or using- AI tools. Those areas include:

- How OpenAI retains or uses personal information and what information it collects. Also asked are the methods it gives for individuals to opt-out and have their information deleted.
- What data OpenAI uses to develop and train Large Language Models ("LLMs"), and how personal information is kept out of training data.
- The policies and procedures in place that impact generation of statements about individuals. In particular the FTC has asked about mitigation strategies for statements that are possibly false, misleading, or disparaging.
- Information about data security measures/policies and actual or suspected incidents.

Not surprisingly, this investigation aligns with the FTC's previous guidance and concerns about potential AI consumer harms.

PUTTING IT INTO PRACTICE: The FTC's investigation into OpenAI signals that the agency is looking closely at the privacy implications of this tool. Those either using tools like this or creating their own will want to keep prior advice from the FTC in mind.

NY AI Laws Going Live Next Month

Posted June 14, 2023

New York's Local Law 144 of 2021 will finally go into effect on July 5, 2023, after several delays. As we previously discussed, the law requires employers to provide candidates for employment and promotion with notice about the use of an AI system, offer them an opt out, and audit any such systems for bias. The law is intended to benefit job applicants and may provide useful guidance for employers who wish to use AI to help eliminate workplace bias.

Although the law was effective as of January 1, 2023, the New York City Department of Consumer and Worker Protection, just recently published their final rules on April 6, 2023. This has left companies with a reduced timeframe to comply with the new rules.

The final rules included:

- **Clarifying definitions for Automated employment decision tools ("AEDT").** This included providing a definition for "substantially assist or replace discretionary decision making for making employment decisions" to cover decisions that rely on a simplified output or overrule human decision-making. The rules also clarified the definition of "machine learning, statistical analysis, modeling, data analytics, or artificial intelligence" to be a group of mathematical, computer-based techniques that generate predictions or classifications and for which the computer at least in part determined the inputs, priorities, or other parameters to make the classification.
- **Bias audit examples**. The final rules offer several illustrative examples and methods for calculating bias scores. Those scores must be included in published results.
- **Historical data**. The final rules also offer examples of when companies may rely on a bias audit conducted with historical data, test data, or historical data from other companies

Businesses should remember that non-compliance does have consequences. Forgoing a bias audit or not providing notice are two separate violations and subject to civil penalties. Each day of noncompliance is considered a separate violation that could result in civil penalties.

PUTTING IT INTO PRACTICE: Businesses that use automated decision making for hiring and promotional decisions should start considering now whether they need to modify these tools. Additionally, businesses should start looking for ways to complete an independent bias audit to ensure that they remain in compliance.

Connecticut Enters AI Fray

Posted June 13, 2023

The Connecticut governor recently signed SB 1103, bringing the state into the artificial intelligence regulation fray. The law regulates state agencies, and calls on the Department of Administrative Services to perform regular assessments of systems use by these agencies. The assessment is to identify which systems use artificial intelligence and to ensure that the use does not result in unlawful discrimination or disparate impacts. The systems inventory must be conducted by December 31 of this year, and the assessment by February 1, 2024. These inventories and assessments must thereafter be conducted on an annual basis.

The law also calls on the Office of Policy and Management to implement policies and procedures about how state agencies can use artificial intelligence. Among other things, state agencies will not be able to use the tools in a way that unlawfully discriminates or creates a disparate impact on individuals. Additionally -and importantly for those who do business with Connecticut state agencies- these procedures will govern how state agencies can procure systems from vendors that include artificial intelligence. Finally, beginning October 1, 2023, state contracting agencies must include provisions that require businesses working with them to comply with Connecticut's comprehensive/general data privacy law.

Putting It Into Practice: This new law will have limited scope, applying to Connecticut state agencies and to a much lesser extent those who do business with them. It is, though, a reminder that artificial intelligence, and systems that incorporate them, are of concern for regulators. We may thus see other similar laws in the future.

BIOMETRICS

Don't Forget Deception: FTC and Biometrics

Posted June 13, 2023

With the ongoing BIPA litigation activity in Illinois surrounding collection of biometrics, it can be easy to forget that other issues might surround this practice. Last month the FTC reminded companies not to forget general privacy and data security concerns. Concerns as most know, it enforces under Section 5 of the FTC Act (which prohibits deception and unfairness).

The FTC recognized that there may be an uptick in companies desire to collect biometrics through machine learning. Or, to use biometric information to understand people's characteristics. The FTC's issuance of this policy statement suggests it may bring biometric-related actions in the coming months. Its warnings can thus be a helpful signal of things *not* to do.

Some recommendations to avoid potential allegations of deception and unfairness include:

- *Not making unsubstantiated or false claims about the efficacy of technologies that use biometrics*. For example, selling products to business consumers that do not work, and the result being consumer harm.
- *Avoiding deceptive claims about how the company uses biometrics*. This includes both misleading a consumer about what biometric information is collected. It also means not deceiving people about how information might be used.
- *Assessing and addressing foreseeable harms*. Potential harms could be where a company knows technology is prone to errors, but fails to take steps to prevent them. Appropriate steps would be to find and put in place "readily available tools" to reduce risks.

- *Not "surreptitiously" collecting biometric information*. This also covers "unexpected" collection of that information that exposes someone to harm. Those might include, for example, stalking or reputational harm.
- *Evaluating the third parties that will have access biometric information*. Appropriate measures, according to the FTC, include both contractual obligations for vendors to minimize risks to consumers and vendor oversight.
- *Training employees*. In particular, those who interact with biometric information or technologies that collect or use it.

PUTTING IT INTO PRACTICE: The FTC has signaled with this policy statement what activities it deems unfair or deceptive in the biometric space. Companies can keep these in mind, in addition to state law obligations of notice and choice.

Illinois Supreme Court Finds Federal Law Labor Preempts Union Members' BIPA Claims

Posted March 27, 2023

Can unionized employees sue their employers in court for violations of Illinois' Biometric Information Privacy Act (BIPA)? In a rare victory for BIPA defendants, the Illinois Supreme Court unanimously ruled they cannot.

The plaintiff in *Walton v. Roosevelt University* was an SEIU union member who had worked as a security guard for Roosevelt University in Chicago. His BIPA lawsuit alleged Roosevelt required him and other unionized workers to provide hand-geometry scans, for timekeeping purposes, without their consent.

The Illinois Supreme Court concluded Walton's BIPA claims could not proceed in state court. Namely, because Walton agreed to a collective bargaining agreement between his union and Roosevelt, the Court found his BIPA claims preempted under federal labor law—specifically, Section 301 of the Labor Management Rights Act (LMRA).

The Illinois Supreme Court did not write on a blank slate. In recent years, federal courts have consistently ruled union members' BIPA claims are preempted by the LMRA. By deferring to those federal decisions, the Illinois Supreme Court shut the door on union members seeking to litigate BIPA claims in state court.

PUTTING IT INTO PRACTICE: *Walton* should stop unionized employees from bringing new BIPA claims in state and federal court. *Walton* also forecloses unionized employees from bringing BIPA claims on a class action basis. Companies on the receiving end of a BIPA lawsuit from a current or former union member should always explore a motion to dismiss the lawsuit on preemption grounds.

Illinois High Court Rules "Per-Scan" Damages Can Be Awarded Under BIPA

Posted March 2, 2023

February 2023 was a momentous month for Illinois' Biometric Information Privacy Act (BIPA). Just two weeks after imposing a 5-year time limit for all BIPA claims, the Illinois Supreme Court resolved another pressing issue. In *Cothron v. White Castle System, Inc.*, the Illinois Supreme Court considered whether a BIPA claim accrues every time a company scans or transmits a person's biometric identifier (e.g., fingerprint) without consent. In a closely divided 4-3 ruling, the Court answered "yes."

Cothron greatly increases companies' liability exposure for violations of BIPA's sections 15(b) and 15(d). Now, every unauthorized biometric scan entitles a plaintiff to damages ranging from $1,000 to $5,000. If the Court had ruled BIPA claims only accrue upon the *first* scan, plaintiffs' maximum recoveries would be much lower.

The Court clarified that trial courts are not required to award the maximum damages award in a BIPA case. Rather, trial courts have discretion to determine the appropriate amount. But unfortunately, the Court provided no further guidance or standards for trial courts.

Cothron'spotentially ruinous effect on companies did not seem to trouble the majority. While recognizing companies could face bankruptcy for "per-scan" damages judgments, the Court laid blame at the Illinois legislature and gently encouraged lawmakers to clarify the issue. It remains to be seen whether the Illinois legislature will act.

PUTTING IT INTO PRACTICE: After *Cothron*, BIPA poses an existential threat to companies who collect or transmit Illinois residents' biometric data without consent. Especially in class actions, a company's maximum potential exposure will skyrocket because every unauthorized scan of a fingerprint or faceprint entitles a person to *at least* $1,000. Companies should make sure their biometric procedures fully comply will BIPA to avoid potentially catastrophic damages judgments in class actions.

Illinois High Court Allows Biometric Privacy Claims to Go Back Five Years

Posted February 10, 2023

A plaintiff has her fingerprints forever. But she doesn't have forever to file a lawsuit for improper retention, deletion, collection, or use of her fingerprints. For years, Illinois courts have been perplexed on what statute of limitations applies to different claims under the Illinois Biometric Information Privacy Act ("BIPA"). That left an unanswered question: how long does a plaintiff have to file a BIPA claim before losing it? The Illinois Supreme Court weighed in last week, siding with the plaintiffs' bar. In *Tims v. Black Horse Carriers, Inc.*, that Court held that plaintiffs have five years to file any BIPA claim.

The five-year period comes from a catch-all statute of limitations. That limitations period generally applies to claims brought under laws that do not have their own statute of limitations. Many defendants like Tims instead argued that a one-year statute of limitations applies to all BIPA claims. Disagreeing with the lower appellate court, which found a 1-year period applied to some claims, the Court held that only one statute of limitations should apply to all BIPA claims. That led the Court to choose the longer five year period because it could apply to all BIPA claims, not only some of them.

The recent ruling opens up the number of BIPA claims that may get past early motions to dismiss. Multiple cases that are currently on hold pending the *Tims* decision are likely to move forward in light of this result.

PUTTING IT INTO PRACTICE: The number of BIPA cases filed may increase in light of the Illinois Supreme Court's guidance on the statute of limitations. Other issues, like when a BIPA claim accrues, remain open questions for that court. Companies affected by BIPA should remain vigilant in light of the court's focus on broadly effecting BIPA's policy goals.

CHILDREN'S PRIVACY

CARU Releases Metaverse Guidelines

Posted October 26, 2023

The Children's Advertising Review Unit (CARU) released new guidelines for interacting with children in the metaverse: *Building Guardrails for Child-Directed Advertising & Privacy in the Metaverse*. The guardrails are intended to be "realistic and actionable" ways for companies to comply with privacy laws and engage responsibly with children online.

The guardrails outline how companies can eliminate possible confusion between content and ads in the metaverse. They also guide businesses in how to protect children's personal data. They include recommendations for responsible metaverse experiences for children, and include questions that companies should explore before offering metaverse experiences to children. For example, clearly distinguishing ads from content, transparently disclosing ads and complying with relevant privacy regulations (i.e., the Children's Online Privacy Protection Act (COPPA)).

CARU released these guidelines only a month after the FTC released recommendations for separating ads from content and cautioned against blurred advertising for children.

PUTTING IT INTO PRACTICE: There continues to be close scrutiny on how advertisers interact with children in the digital world. Advertisers operating in the metaverse should keep this in mind; this development is a reminder to review privacy compliance programs, especially if virtually interacting with children.

California Judge Enjoins California Age-Appropriate Design Code Act

Posted September 28, 2023

A California judge recently entered a temporary injunction delaying the California Age-Appropriate Design Code Act. The trade association, NetChoice, requested the injunction.

Before this decision, the law was to go into effect on July 1, 2024. As we wrote previously, the law would require companies providing services likely to be accessed by minors to ensure protecting minors' privacy and data. The California judge said that NetChoice has a good chance of winning its argument that this law violates the First Amendment. California Attorney General, Rob Bonta, doesn't agree with the judge's decision and plans to continue to fight it in court.

PUTTING IT INTO PRACTICE: We will continue to monitor this development, but companies who might be covered should keep in mind the similar -and currently in effect- UK code.

The Beehive State Joins the Buzz Around Minors and Social Media

Posted April 12, 2023

The Utah legislature recently passed SB 152 and HB 311. While these two bills will primarily impact those who are "social media" entities under the law, they may have broader impact when the majority of their requirements take effect, on March 1, 2024.

The bills apply to "social media companies" – defined as companies with more than five million account holders worldwide. Key provisions include:

- SB 152: Starting March 1, 2024 social media companies must (i) verify the age of a Utah resident seeking to maintain or open an account, and (ii) get parental consent before minors under 18 can open or maintain their current account. Existing users who do not verify their age within 14 days of trying to access their account must have their access denied. The social media company must give minors' parents (or guardians) access to all posts, messages, and responses. These companies also cannot display advertising to minors. Minors also will not be able to engage in a variety of interactive activities -like direct messaging- to individuals outside their friend group. The law also requires for data minimization of information in minors' accounts and limits the time of day that minors can access their accounts. Namely prohibiting use between 10:30pm and 6:30am. The bill provides for a private right of action, as well as rulemaking to clarify a variety of points including how to obtain parental consent and verify age.
- HB 311: This bill is focused on "addiction" to social media. Under the law, social media companies may not "use a practice, design or feature" on its platform that it knows or should know would cause a minor to become addicted to the platform. Addiction is defined as use that both indicates "a substantial preoccupation or obsession" with the platform and causes "physical, mental, emotional, developmental or material" harm to the minor. Social media companies will be subject to auditing by the Utah Division of Consumer Protection. They will not be liable for content uploaded by third party account holders. Violations may result in a $250,000 civil penalty per violation. The bill also provides for a private right of action to collect attorney fees and damages.

- These bills are the first of their kind in the US and have received a fair amount of focus. SB 152 in particular may have impact on entities beyond social media companies themselves. For example, the prohibition on displaying ads to minors. And HB 311 may result in modifications in how social media companies design their platforms for all users to avoid allegations of "addiction." We may also see a drop off in account holders in Utah, given the need for all to verify age and the requirement that accounts be cancelled if age is not verified within the bill's time frames.

Putting it into Practice: While California is often seen as a leader in these consumer protection statutes, other states may be following Utah's lead this time. Connecticut, Ohio, and Texas have introduced similar bills to regulate minors' use of social media. As social media companies gear up for the March 1, 2024 deadline, others are reminded that regulators and enforcement agencies both are concerned about children's use of online platforms.

CONSUMER PRIVACY

Connected Devices: Eyes on EU Data Act

Posted December 19, 2023

The European Council recently approved a final version of the EU Data Act. The Act applies to manufacturers of connected devices. Among other things, it gives consumers certain rights about the information those devices collect. The Act is viewed as part of an overall data strategy by the EU, and complements both GDPR and the Data Governance Act.

The requirements will not go into effect until mid-2025. Among other things, under the Act those who create connected products will need to ensure that data collected from these devices is portable for both users and in some cases governments. To accomplish this, the Act requires manufacturers to design products in a way that makes data sharing easy.

PUTTING IT INTO PRACTICE: These requirements are part of a growing interconnected set of requirements in the EU around treatment of data. As companies develop new interconnected products, they will want to keep in mind these upcoming obligations.

Massachusetts Wagers Big on Privacy in Sports Betting

Posted November 15, 2023

The Massachusetts Gaming Commission approved data privacy regulations under the 2022 Massachusetts Sports Wagering Act earlier this fall. While directed to a narrow group of companies, the restrictions around use of artificial intelligence, profiling and breach notification suggest the types of concerns that we may see other regulators focus on in other industries.

The law was passed last year to legalized sports betting in the state. It also placed obligations on how covered entities handle personal information. Entities covered by the law, and thus impacted by these regulations, are those who run physical or virtual sports wagering establishments in or directed towards those in in Massachusetts. Under the law, the gaming commission was given regulatory authority. The regulations from this fall spell out how to meet the protection obligations of the law. Namely:

- **Limit how information is used**. Operators may use and keep patrons' information only to operate their sports wagering platforms. If they wish to use information for other reasons, they must get consent. Consent must be "clear and conspicuous" and not part of another agreement. The rules specifically prohibit relying on acceptance

of terms for this kind of consent. Operators are also prohibited from using actual or predicted behaviors to encourage wagers or to serve marketing. Of particular concern was putting patron information into AI systems to make gaming more addictive.

- **Protect information**. Operators must develop and maintain data privacy and security policies. These policies must address employee training, incident response procedures, and technical and organization measures for protecting information.
- **Notify in the event of a breach**. Operators must notify the Massachusetts Gaming Commission and begin an investigation within 5 days of a *suspected* data breach. A breach is the same as under the state's breach notification law, namely unauthorized acquisition or use of computerized personal information. (That law, as many know, and like most breach notification laws, has a specific definition of personal information.)
- **Limits on data sharing**. Under the regulations, operators can share patrons' information only as necessary to operate the sports wagering establishment or platform and only if there is a written agreement in place with the recipient. That agreement must include, *inter alia*, a promise that the vendor will protect the information and have data security program and incident response procedures in place. Operators must also encrypt or hash information before sharing.
- **Patron rights**. Similar to rights found in state comprehensive laws, patrons have the right of access and correction. The law also provides for the right to have information deleted and to have use limited. These rights need to be communicated online.
- **Promoting responsible gaming:** The law requires sports wagering operators to compile and aggregate patrons' personal information and analyze it for purposes of developing programs to help people with gambling addiction.

PUTTING IT INTO PRACTICE: While applicable only to those sports wagering operators, these requirements highlight concerns that are on the minds of all regulators. This includes restrictions on use of artificial intelligence and concerns about using behaviors and profiling to influence behavior.

California Regulator Drives Inquiry into Vehicle Data

Posted August 15, 2023

The enforcement division of the California Privacy Protection Agency (CPPA) recently announced it intends to review the privacy practices of connected vehicles. The driving force behind the review is the technologies in connected cars that raise privacy concerns. These include location sharing and smartphone integration. Connected cars often also have cameras and web-based entertainment systems. These cars—and the technologies in them—may monitor people both in the car and outside of it. For many Californians, the car is part of their daily routines. Connected vehicles can effectively becoming a constant data generator.

The CPPA, California's independent data protection authority, was created under amendments to the CCPA. It is charged with enforcing the state's privacy law, among other things. This is the agency's first announcement of this kind. Its focus until now has been on rulemaking. The agency is conducting the review under the CCPA, and pointed to the fact that the law grants consumers certain rights. These include the right to delete, right to know, and the right to stop sale or sharing. Presumably the agency's review (and likely subsequent enforcement) will not be for violations of the regulations adopted by the CPPA on March 29, 2023, which as we reported cannot be enforced until 2024.

Key among this data is the vehicle's location. When combined with personal information and/or third-party data or mapping services, location information can unveil intricate details about a person's preferences and habits. CPPA's announcement implies they are looking at both the information collected about people in the connected vehicles and also information captured about other devices near the vehicle. This implies the potential for monitoring not just the driver's information but also that of passengers and individuals nearby.

The CPPA is not the only regulator focusing on connected vehicles. Chinese regulators have expressed concerns, while the European Commission is working on regulations to ensure equitable access to vehicle data.

PUTTING IT INTO PRACTICE: While CPPA's enforcement regime has had a minor setback, the agency continues to move forward with its enforcement plans. Companies should keep an eye out for existing compliance issues that may be on the forefront of CPPA's radar as they begin to show how they will wield their new authority.

The Rough Waters of Website Accessibility

Posted March 20, 2023

Companies are continuing to find it hard to navigate the legal landscape of website accessibility. Plaintiff's lawyers argue that "inaccessible" websites or mobile apps fail to comply with the Americans With Disabilities Act or similar state laws. This despite the absence of standards for website accessibility in these laws. Similarly, while the Department of Justice does not have a regulation setting out detailed website accessibility standards, the Department's position has been that the Americans with Disabilities Act's general nondiscrimination and effective communication provisions apply to web accessibility.

The Department has directed that businesses look to existing technical standards for website accessibility including the Web Content Accessibility Guidelines (WCAG) and the Section 508 Standards, which the federal government uses for its own websites. And despite the absence of formal website accessibility standards, the Department has continued to file enforcement actions against businesses who operate websites that it deems inaccessible.

The laws in question broadly require that places of public accommodation be accessible. But are websites or mobile apps places of public accommodation? Courts are divided. Some hold that **any** website can be a place of public accommodation. Others have not gone this far. This split has made it difficult for companies to know how best to proceed when developing their websites and mobile apps. The following are steps can a business take to mitigate risks in the face of these enforcement and litigation threats:

- *Carefully Negotiate Website Development Agreements:* If you use a third parties to build or maintain your website, require that the vendor ensure the site complies with the WCAG 2.1 AA. Potential costs of ADA website litigation can be high. Thus in addition, carefully negotiate indemnification and limitation of liability provisions.
- *Evaluate Current Accessibility:* Third party testing exists to see if a site complies with WCAG 2.1 AA. Companies can also use free or low cost tools. For example, WAVE (https://wave.webaim.org/) is a free Chrome tool often used by the plaintiff's bar. The tool identifies website access "errors" and can be run on each website page. Setting a schedule of regularly checking site page accessibility can be an important tool in your risk mitigation arsenal.
- *Beware of Relying on Widgets or Overlays*: Many online companies provide for-a-fee widgets or overlays. These purport to make sites fully compliant. Most of these lack human testing and are able to identify a small percentage of compliance issues. These tools may prove of limited value.
- *Remediate:* Once the business understands the areas of non-compliance, it should evaluate the costs of remediation versus redesigning the website from scratch. Businesses will often need to balance risk against budget and practicality. At a minimum, businesses should minimize the number of accessibility errors on each website page to mitigate the risk of a website access lawsuit and to undermine any assertion should litigation ensue that their website's noncompliance constituted intentional discrimination.

PUTTING IT INTO PRACTICE: These four steps can help companies mitigate the risks associated with potentially costly accessibility litigation. From regular accessibility checks to strong contractual controls, companies can take steps today even absent clear legislative direction.

Mobile Apps Beware!: California AG's Current Privacy Sweep

Posted February 13, 2023

The California AG announced an investigative sweep of mobile apps, as we reported in our sister blog. The investigative focus is on companies in the retail, travel and food service industries who may not be complying with the California Consumer Privacy Act (CCPA). As we have written previously, the California law requires entities to provide individuals with a myriad of rights, including as it relates to "sale" of personal information.

The focus of the current sweep should be of interest to entities trying to understand the AG's focus this year (for more on this topic, you can also listen to our recent webinar). In particular, the AG has signaled his concern that these entities are either not respecting opt-out requests or pare not giving consumers the ability to opt out of the sale of their information. The Attorney General is especially looking at opt-out requests sent by third party vendors like Permission Slip.

PUTTING IT INTO PRACTICE: This is not the first year that California has begun the year with CCPA-related privacy sweep. While last year's focus was on loyalty programs, this year companies subject to CCPA should keep in mind that the law applies beyond information collection on websites. The AG has signaled its concern in this recent sweep on mobile app compliance with CCPA.

UK App Code Provides Privacy and Security Compliance Direction

Posted February 9, 2023

The UK's new Code of Practice for App Store Operators and App Developers provides companies with privacy-related resources. It also highlights ICO privacy expectations. Participating in the code is done by voluntarily complying with it (it is not mandatory). The UK Department for Digital, Culture, Media, and Sport, though, is not only working with leading companies to participate in the code, but also is looking at whether current laws should be expanded and/or if code participation should become mandatory.

Compliance under the code follows an eight-step approach. Those include keeping apps' security controls updated, and outlines how companies should handle data breaches (referring developers to the ICO's breach guidance).

Another step is providing privacy information to consumers in an "accessible" way. Privacy-related information companies should provide consumers mirrors requirements of UK GDPR. Among other things, the code specifically calls out explaining what analytics and marketing activities in which the company will engage.

PUTTING IT INTO PRACTICE: Companies launching an app in the UK market can look to the code for insight in applying UK GDPR to apps. Even if a company does not wish to attest to compliance at this time, the code is worth understanding to the extent participation in the code, or the code's compliance approach, become law in the future.

Gaming Operators Latest to See Specific Privacy & Cybersecurity Laws

Posted February 8, 2023

Two states recently passed laws with specific data security requirements for entities that are gaming operators or licensees. These new regulations in Nevada and Massachusetts add to the already complex set of data security laws that exist at the federal and state level. In the US, companies may be subject to certain data security laws because of the *type* of information they collect or because of the industry they are in (financial, healthcare, insurance, telecommunications, etc.). The gaming industry is the latest to add to the mix.

In this latest addition to this complex patchwork, the Nevada Gaming Commission adopted regulations for certain operators at the end of 2022 with the regulations becoming effective January 1, 2023. The rules apply to certain "covered entities" and impose requirements around: (1) risk assessments, (2) incident response, and (3) personnel. The Massachusetts law, aimed at both "operators" and "licensees" impose both general and specific obligations. Among other items, the law sets forth specific requirements for privacy policies, individual rights, automated decision making, and data security. While the Massachusetts rules were published with effective dates of December 2022, comments are invited until February 2023.

PUTTING IT INTO PRACTICE: Gaming operators will want to make sure that they understand these laws and their requirements, including around data security and privacy disclosures. If you are a vendor working with covered entities, you may also want to look at these requirements. Those outside of this industry should take heed, as these two new laws signal the ever-evolving web of privacy and data security laws, including sector-specific requirements.

CROSS-BORDER DATA TRANSFERS

No Need to Mind the Gap – UK Extension is a Data Bridge for US-UK Data Transfers

Posted October 10, 2023

Beginning today, the UK adequacy decision for US data protection measures goes into effect. As a result, UK companies can transfer personal information to entities in the US that are participants in the EU-US Data Privacy Framework (DPF). As part of the decision, the UK Secretary of State will review the ongoing sufficiency of the DPF every four years. The ICO, in supporting the decision, suggested that the UK Secretary of State look at specific factors when reassessing the program. These include the risk to UK data subjects for automated decision making and right to be forgotten.

Not all US companies will necessarily want to participate in the DPF (see more about the process here). If they do not, then UK companies making transfers will need to rely on existing mechanisms, like SCCs coupled with supplemental safeguard measures.

PUTTING IN INTO PRACTICE: This extension was expected, but companies who are considering DPF participation for UK-EU transfers should keep in mind that the UK review of the program is on a different cadence than that in the EU.

Considerations for Participation in the EU-US Data Privacy Framework

Posted September 7, 2023

Now that the EU has adopted its adequacy decision for the EU-US Data Privacy Framework (DPF), many companies are assessing whether participation makes sense. Participation by a US entity is a mechanism -but not the only mechanism- for two parties (one EU and one US) to transfer personal data from the EU to the US. Other transfer methods include Binding Corporate Rules or Standard Contractual Clauses. As we wrote recently, when the EU determined that the program was "adequate," it noted that the safeguards developed by the US for the DPF applied to *all* methods of transfer. In other words, for BCRs or SCCs.

Why, then, might a company want to participate? Especially if this program has a short life span, and ceases to receive EU approval, likes its predecessors (the Safe Harbor and Privacy Shield) programs? Reasons for participation include because the organization finds it is being pushed by EU contractual partners to participate. Or, negotiating hundreds of individual SCCs may be overly burdensome. There is no one-size-fits-all answer to whether participation makes sense. Companies will want to evaluate the program carefully, as participation goes beyond merely signing up on the Department of Commerce website.

As part of the evaluation process, it may be helpful to keep in mind the steps for participation, which include:

1. **Developing or updating individual rights and choice mechanisms**: Program participants will need mechanisms to provide individuals with rights and to make choices. These include, as with US state laws, giving individuals the ability to make rights requests (access, correction and deletion). Participants must also give people the ability to opt-out of marketing, having their information shared with (non-agent) third parties, or used for a materially different purpose. Those collecting and using sensitive information (including, *inter alia*, health and ethnic origin information) must get consent if that information will be disclosed or used for a purpose other than that for which it was collected.
2. **Implementing a complaint handling process and selecting an independent recourse mechanism**: DPF participants will need to put in place a process to handle consumer complaints. Like predecessor programs, they will have to give individuals the ability to lodge complaints with an independent recourse mechanism (third party) or by agreeing to cooperate with the relevant EU data protection authority.
3. **Developing or updating internal policies and procedures**: The program is enforced on the US side by the Federal Trade Commission, under the unfairness and deception prong of the FTC Act. Participants are required to make certain disclosures about their compliance with the program, and the FTC will enforce those by examining whether the company has adhered to them (i.e., are not deceptive claims). Given this, companies will want to ensure they have undergone sufficient diligence to confirm compliance with their representations, and have correct policies and procedures in place to make sure they have ongoing compliance. These policies might include, for example, ones focused on security measures, consumer rights responses, and data integrity and purpose limitations.
4. **Adopting a verification process/adopt appropriate record keeping**: Participants will need a method for verifying that they are complying with the program. This can be with an external verification body, or through self-verification. Part of the DPF's verification requirement is that participants maintain records of how the DPF has been implemented.
5. **Updating privacy policies and related disclosures**: DPF participants must include certain content in their privacy policies. This includes saying that the company is subject to FTC jurisdiction and liability in the event of onward transfers. (Other requirements will likely mirror content already in existing policies: the type of personal information collected and the types of entities to whom information is disclosed). Only after the earlier steps are taken will companies be in a position to update their external disclosures.
6. **Submitting the self-certification**: DPF participants must not only address the items above, but also register with the Department of Commerce, submitting the required information, designating a point of contact, and paying the applicable fees. Those contemplating participation should keep in mind that there is an annual renewal as well.

PUTTING IT INTO PRACTICE: As this list of steps makes clear, participation goes beyond merely modifying a privacy policy and submitting a form. Companies will have many steps to take, including potentially developing internal processes, conducting diligence, adopting new (or modifying existing) policies, implementing record keeping measures, and selecting and working with new (IRM and/or verification) vendors. Keeping these obligations in mind can help as companies are making decisions about whether the DPF is the right program for them.

EU Adopts Adequacy Decision for EU-US Data Privacy Framework

Posted July10, 2023

The EU Commission adopted today an adequacy decision for the EU-US Data Privacy Framework. As we indicated last month, this has been an area closely watched by those transferring data from the EU to the US. The issue has been a contentious one. Concerns in particular have been raised on the EU side regarding US surveillance agencies' ability to access non-US individuals' personal information. These concerns led to the downfall of both of the Framework's predecessors: Safe Harbor and Privacy Shield.

Companies in the US that find themselves receiving European personal information can elect to participate in the new Framework program, operated by the US Department of Commerce. It is not mandatory, and other transfer mechanisms may exist. These include Binding Corporate Rules as well as Standard Contractual Clauses. To participate, among other things companies must publicly confirm that they will adhere to specific privacy obligations ranging from data minimization and retention to limits on data sharing. By making this public commitment, this gives standing for the FTC to bring enforcements under Section V of the FTC Act. The program will be reviewed on an ongoing basis by the EU to ensure it continues to meet "adequate" levels of protection, including the first review in one year.

In determining that the Framework program was "adequate," the EU pointed to several elements of the program. This included that participating companies must give individuals rights similar to those under GDPR (access, correction, deletion). They must also offer a free dispute-resolution mechanism for mishandled information. Additionally, one of the key factors resulting in the program's approval by the EU was the US's establishment -through a White House Executive Order- of safeguards for use of non-US nationals' personal information by US surveillance agencies. Under that order, there are limits on when such agencies can access this information, more oversight on their information collection and use activities, and an independent redress mechanism for individuals to use. Specifically, for this last, individuals can submit complaints to their domestic data protection authority: they do not need to bring the complaint in the US. Those complaints will then be sent by the EDPB to the US, which will have a "Civil Liberties Protection Officer" investigate. The investigator's decisions can be appealed to a newly created "Data Protection Review Court." The EU noted that these safeguards apply to *all* data transfers from the EU to the US "regardless of transfer mechanism used." In other words, the EU indicated, they "facilitate the use of other tools" including standard contractual clauses and binding corporate rules. This should thus help companies who elect to use SCCs or BCRs as a transfer mechanism instead of joining the new Framework program.

PUTTING IT INTO PRACTICE: For those who are interested in learning more about the Framework program, they can visit the Department of Commerce's program site here. The Framework is not the only mechanism for transferring personal data between the EU and US. Given the fate of the prior programs, companies will want to work with their counsel and think carefully about whether this one is a good fit for them. They will also want to keep in mind the various principals to which they will be asked to publicly adhere, and ensure that they have processes and procedures in place to meet them.

EDPB Adopts Binding Corporate Rules Recommendations

Posted July 5, 2023

As those in the privacy world await the outcome of the EU-US privacy framework negotiations, the EDPB was in the news recently for a different mechanism for data transfers: Binding Corporate Rules. Namely, it adopted recommended standard forms for BCR applications by controllers and recommendations for the application process.

As we have written previously, personal information cannot be exported out of European Union Member States unless the recipient is in another Member State or a country with an "adequate" level of protection. There are many exceptions, including execution of Standard Contractual Clauses (with, if necessary, supplemental protection measures). For multinational organizations that make frequent intracompany cross-border transfers, another appealing option has been Binding Corporate Rules. These are created by the company and then reviewed and approved through the local Data Protection Authority. While each DPA has its own system, there are commonalities, which were based on pre-GDPR "Article 29 Working Party" guidance, last updated in 2018.

The EDPB's recommendations replace this prior guidance for BCRs used by controllers -for example large multinational corporations engaging in intracompany trans-border transfers- and outlines what should be contained in a BCR application. The recommendation also includes the form itself. Information to be provided includes a description of the data flows, how the BCRs will be binding on the group of companies to which it applies, and similar items. While some of the content is not new, the level of detail being requested in the application has increased. Also, not surprisingly, there are provisions intended to address the law enforcement access concerns raised by *Schrems II*.

PUTTING IT INTO PRACTICE: The EDPB has indicated that all controllers who are seeking to implement -or who have *already*– implemented Binding Corporate Rules will "have to bring their BCR-C in line with the requirements set out in the recommendations." Multinationals who are seeing to implement BCRs will want to thus familiarize themselves with the new form, as well as the mechanisms developed to address law enforcement access concerns.

Where Do We Stand?: EU to US Data Transfers

Posted June 8, 2023

The process for data transfers from the EU to the US under Standard Contractual Clauses has been back in the news recently, leading many to ask: will the proposed EU-US Data Privacy Framework be approved by the Europeans soon?

A quick recap on the background: the new transfer regime was developed in March to replace the Privacy Shield program. For the program to be an effective basis for transfer, however, it has to not only launched in the US, but also formally adopted by EU Commission. The key concern has been — and what led to the downfall of the two prior programs, Safe Harbor and Privacy Shield — US governmental surveillance of non-US individuals. To address this, Biden issued Executive Order 14086 in October 2022. That order put restrictions in place over potential surveillance activities, but gives US intelligence community until October to update policies and practices to align with the order.

Where are we now?: a draft adequacy decision was proposed in December to begin the review process. However, in February the EDPB raised concerns. Last month the European Parliament echoed the EDPB's concerns, and recommending that the EU Parliament *not* adopt the adequacy decision. The key concerns included:

- The US President can expand the list of national security objectives for which surveillance can be conducted without informing the EU of that expansion.
- Although there are safeguards for bulk collection, there is no provision for prior authorization, something the Parliament reminded was the concern that caused the downfall of the Privacy Shield program.
- The approach towards determining what is "necessary and proportionate" for a US surveillance activity are not in line with the EU approach.
- The order does not address information that surveillance agencies might access through existing laws like the US Patriot Act.
- Additionally, while the order set forth a redress mechanism for individuals, it was not viewed a sufficiently transparent or independent by the EU Parliament. The Parliament recommended this be monitored if the Framework is in fact adopted by the EU Commission.
- In recommending that the EU Commission vote against adopting the adequacy decision and continue negotiating with the US, the EU Parliament noted the October deadline for the US intelligence community. As such, it stated it could not fully assess the effectiveness of the order.

PUTTING IT INTO PRACTICE: While we continue to wait for finalization of the new EU-US Privacy Framework, companies will need to continue to rely on alternate mechanisms for EU-US data transfers, which include supplemental protection measures.

CNIL Weighs in On GDPR Applicability to US Company

Posted February 7, 2023

The French Data Protection Authority capped off 2022 by terminating an investigation into Lusha Systems, Inc.'s compliance with GDPR. CNIL concluded that the law did not apply to the US company's activities. As many know, since GDPR was passed US companies have been concerned about the extent the law applies outside of the EU: it applies not only to those entities with operations in the EU, but also those outside of the region who are either offering goods or services to people in the EU or monitoring individuals in the EU. Here, CNIL concluded that Lusha was not offering goods or services to those in the EU, nor was it monitoring those in the EU.

The European Data Protection Board has issued guidance and examples on the scope of CNIL. These include "monitoring" situations, perhaps the trickiest fact pattern. However, the guidance gives examples of when GDPR *would* apply but not situations where it *would not* apply. The Lusha case is thus helpful to companies as they consider GDPR applicability.

The activities in question surrounded the company's browser extension, which let users append phone numbers and email addresses to contacts on LinkedIn or Salesforce. To accomplish this, Lusha matched LinkedIn and Salesforce user profiles with contact information it had previously obtained from other users' address books. (Specifically, users of its browser extension were prompted to share their address book data, the email addresses and phone numbers of which would go into Lusha's database). Some of those individuals (from the users' address books) resided in the EU.

In concluding that GDPR was inapplicable, CNIL noted that the users of the service were in the US, not the EU, and thus the services were not offered to EU individuals (even if some EU individuals' information was being obtained by the service). With respect to the question of monitoring those in the EU, CNIL concluded that the pulling of contact information was not "monitoring."

PUTTING IT INTO PRACTICE: For US companies with no EU operations, this case is a good reminder that simply because your organization has information about EU individuals does not automatically mean GDPR applies. Instead, an analysis needs to be made of the extent to which you are offering goods or services to people in the EU, *or* are monitoring EU residents.

DATA BREACH

FTC Decision with Global Tel*Link Signals Expectations for Use of Testing Environments

Posted November 29, 2023

The FTC recently announced a settlement with Global Tel*Link, a telecommunications company that contracts with prisons and jails to provide communication services to incarcerated individuals and their families. Those who use their services create accounts with the company and are required to provide not only usernames and passwords but also Social Security numbers and government ID numbers. The company also collects financial account information as well as names and addresses. The company included in its marketing materials promises about security, including that it was the "cornerstone of what we do." The company also made promises about its security in RFPs to prisons and jails.

An August 2020 data breach, according to the FTC, exposed the personal information users' had submitted. This included information of both incarcerated individuals as well as that of their family members. The breach, the FTC alleged, resulted from the company's failure to take appropriate safeguards during a software upgrade. Namely, during the upgrade, the company copied users' personal information from its regular work environment into a test environment that did not include encryption, automated monitoring, a perimeter firewall, or log monitoring. All things that existed in its regular working environment.

The alleged lack of security existed for three days, and during that time almost 650,000 users' information was in the test environment. And, according to the FTC, the company's forensic investigation showed both access to the test environment as well as data exfiltration during that three day window. The company also, the FTC indicated, received consumer complaints saying their information had been misused. However the company made statements to the press that "no medical data, passwords or consumer payment information" was impacted.

The company did notify a subset of individuals (45,000), but as of the date of the settlement, had not notified the remainder of people whose information was in the test environment.

As part of the settlement, GTL has agreed to both implement things that are standard for an FTC settlement (put in place a security program, have the program assessed by a third party) as well as some that are less usual. These include steps that can signal what the FTC might view as "appropriate" security measures, such as:

- Implementing specific security measures that would impact security of test environments. These include security practices for in-house developed applications and having procedures in place to protect personal information when changes to systems to networks occur that might affect risk. (On this latter point the settlement provides for very specific requirements, rather than more general "appropriate measures" that it has called for in past settlements.)
- Not only ensuring that those who were impacted by this incident receive notice (and credit monitoring), but also if the company suffers a breach in the future it has agreed to provide notice within 30 days to impacted individuals and the relevant prisons and/or jails. While these requirements may mirror what exists under state breach notification laws, the company has also agreed to notify the FTC in such cases as well.
- Providing the board (or equivalent) a written report of compliance with its security program at least annually, and within 30 days after on breach that requires notice under breach notification laws. Related to this is assessing compliance with the program annually.
- Having all employees take security awareness training annually. InfoSec personnel are also required to take additional training "sufficient to address relevant security risks." The settlement also calls for developers and engineers to receive appropriate training.

PUTTING IT INTO PRACTICE: The detailed requirements imposed in this settlement not only combine state law requirements around breach notification and data security, but go beyond them as well. Reviewing the details can be helpful in understanding what the FTC expects of companies, not only in normal environments, but others -like test environments- where sensitive data may be housed.

Amended Kochava Complaint Gives Insight into FTC's View of Harm from Data Profiles

Posted November 21, 2023

The FTC's second attempt to pursue the data broker, Kochava, continues to move forward. The amended complaint, which was just unsealed and thus available for the public to review, gives insight into the agency's perspective on the harm that results when companies create profiles with sensitive information, and use that information to target ads to individuals. The amended complaint provides more detail about Kochava's alleged practices; allegations the company strongly disagreed with. (Thus, why it sought -unsuccessfully- to have it sealed.)

The agency's original complaint from August 2022 focused on the company's data selling practices. The complaint alleged Kochava collected geolocation data from hundreds of millions of mobile devices and packaged them into "data feeds" for marketing purposes. Those feeds included personal identifiers like name and address. It also included information about gender identity and ethnicity. The feeds, the FTC alleged, tracked location information that might place people in "sensitive" physical locations. These included reproductive health clinics, domestic abuse shelters, places of worship, and the like. Those feeds, the FTC noted, are time stamped. Meaning that the time the person (mobile device) was at the location can also be tracked.

Notwithstanding these concerns, the case was dismissed in May of this year for failure to state sufficient harm, with leave to amend. The FTC 's amended complaint was filed in June (but just unsealed), and in it, not surprisingly, the FTC has expanded its discussion of harm to consumers.

In the original complaint, the FTC's concerns focused on the potential harm if someone was tracked at a sensitive location, with a potential for discrimination and physical violence. In the amended complaint, the FTC includes harm from the company's alleged collection and use of profiles based on sensitive information gathered from a wide variety of sources. These sources, according to the FTC, include health information from women's reproductive health apps. The profiles it creates, the FTC further alleges, is then sold to third parties. It is then used to market to individuals based on the sensitive information. For example, targeting ads to "new parents/expecting" or "likely Republican voter."

Like the initial complaint, the amended complaint alleges that Kochava had no security processes in place for determining whether to approve a data access request. Nor were there controls in place, according to the FTC, to limit the subsequent use and sale of the data.

PUTTING IT INTO PRACTICE: While this is far from settled, it shows that the FTC is being aggressive in its use of the FTC Act to pursue those who create and use consumer profiles. This effort mirrors others in the data broker space, including California's recent Delete Act, and examination of data brokers by the CFPB.

Texas Amends Data Breach Notification Law, Updates Effective September 1

Posted August 28, 2023

Texas recently enacted an amendment to its data breach notification law. As of September 1, 2023, there are two changes to the requirements when notifying the Texas Attorney General. In Texas, breaches of 250 residents or more must be reported to the Attorney General. Now, as amended, this will need to be done so as soon as practicable, and not later than 30 days from determination of the breach (previously, it was 60 days). Texas joins Colorado, Florida, and Washington in requiring notice within a 30-day time frame. Notification in Texas *must* also be submitted electronically using a form on the AG's website.

PUTTING IT INTO PRACTICE: These changes are a reminder that states continue to update their breach notification laws. Companies should keep in mind the upcoming change in Texas from 60 to 30 days. Additionally, companies may want to otherwise review their incident response plans at the end of the calendar year.

EyeMed Data Breach Multistate Settlement

Posted May 18, 2023

EyeMed recently entered into a settlement with the Attorneys General of Oregon, New Jersey, Florida and Pennsylvania around a 2020 breach of an EyeMed email account that contained the data of more than 2 million individuals. As we previously reported, EyeMed entered into settlement with NYDFS over this breach in October of 2022.

EyeMed has agreed to pay $2.5 million as a part of this new settlement as well as implement an information security program with requirements around the following areas: (1) data collection and retention; (2) cyber security operations center; (3) logging and monitoring; (4) email filtering and phishing solution; (5) access controls; (6) authentication; (7) asset inventory; (8) data loss/exfiltration prevention; (9) encryption; (10) data deletion; (11) risk assessments; and (12) information security program assessment. For two years after the settlement, EyeMed must provide the Attorneys General a certification of compliance as well as additional documents requested to demonstrate compliance.

PUTTING IT INTO PRACTICE: In addition to monetary settlements, in the aftermath of a breach, regulators are focusing on the security in place at the time of the breach. This is a reminder that companies should regularly assess their information security program to ensure it is appropriately designed to protect the security, integrity, and confidentiality of the companies' data.

May 2nd Marks Effective Data of Pennsylvania Breach Law Amendments

Posted May 1, 2023

As we wrote in November, Pennsylvania amended its data breach notification laws last year, and those changes go into effect tomorrow (May 2, 2023). Beginning tomorrow, if a breach of username/email accounts and their respective passwords occurs, companies can provide electronic notification to the impacted individual. That notice will need to tell individuals to change their passwords or take other proactive measures. The law also amends the definition of personal information. It will now include, as of tomorrow, medical and health insurance information.

Putting it Into Practice: These changes are a reminder that states are continuing to update their breach notification laws, and serve as a reminder for companies to regularly review their incident response programs.

Utah Amends Data Breach Law, Creates Cyber Center

Posted April 21, 2023

Utah's breach notification requirements will change on May 3, 2023. The recently amended data breach notification law now requires companies to notify the Attorney General for a breach involving 500 or more state residents. If the breach involves 1,000 or more residents, then notification to each consumer reporting agency is also required.

The obligation to notify a state authority exists in more than half of US jurisdictions, with Utah joining California, Colorado, Delaware, Florida, Illinois, Iowa, Rhode Island and Washington with a 500-individual threshold. The AGs in many of those jurisdictions ask that companies follow specific processes for making such notifications. Utah does not currently list on its website any such process requirements.

At the same time as amending its breach notice law, Utah has also codified a Utah Cyber Center. This entity appears to be the successor to one that had its soft launch in 2018. The Center, along with the Attorney General, will need to be notified in the event that a breach involves more than 500 residents. The law does not provide a point of contact for the Center, however as of this writing it indicated it would like notices to be sent by email (cybercenter@utah.gov), although that process may change in the future.

The Center's responsibilities are broader, however, than merely receiving breach notifications. It is also charged with promoting cybersecurity best practices and "partnering" with "private sector organizations to increase the state's cyber resilience." In addition, it is charged with centralizing governmental entities' cybersecurity efforts. This includes developing -by June 30, 2024- a statewide strategic cybersecurity plan for executive branch and other governmental agencies. It will also share cyber threat intelligence with governmental entities and coordinate cyber responses for governmental agency incidents (on their request). The director of the Center will be Chief Information Security Officer of the existing Utah Division of Technology Services.

PUTTING IT INTO PRACTICE: Utah has joined a growing list of states that require notification to state authorities if an entity suffers a data breach. If, after May 3, an entity suffers a data breach impacting 500 or more Utah residents, it will need to keep in mind these updated notification obligations. We will be monitoring news from Utah for possible changes to the notice mechanics. We will also be monitoring developments from the Center about cybersecurity best practices and how it intends to partner with the private sector on cyber resilience.

DATA BROKER

Data Broker Rulemaking in Texas and Oregon

Posted December 22, 2023

Both Texas and Oregon recently adopted rules that will, among other things, implement a registry required by both states' data broker laws. The Texas law went into effect September 1, 2023, and the Oregon law will go into effect January 1, 2024. Both are similar to laws in Vermont and California.

Texas defines data brokers more broadly than Oregon, namely entities whose "principal source of revenue" comes from collecting or transferring personal information that the entity did not itself collect. However, the requirements under the law apply only to those data brokers who over the last 12 months received 50% or more of their revenue from data broker activity or of 50,000 or more individuals. Under the Texas law, data brokers must, *inter alia*, register with the Texas secretary of state and post a privacy policy on its website saying that it is a data broker. The law called for the Texas secretary of state to create language for this notice, which it has done for both websites and apps. The notice is lengthy, especially in a mobile context.

With respect to the registry, the new Texas rules address the law's requirement that data brokers register and renew annually. Those subject to the law should keep in mind that it requires disclosure not just of contact information, but also disclosing the number of breaches the data broker has suffered, and if the broker knows that it has information about children. These disclosures are no doubt linked to the law's obligations around data security, something lacking in the Oregon law. Namely, in Texas, brokers must have a "comprehensive information security program" that includes training. It also needs to include vendor oversight.

The Oregon registry process is an interim one, given that the law is going into effect in a little over two weeks. Data brokers covered by the Oregon law must submit not only contact information, but also answers to some specific questions. These include whether individuals can opt-out of having their information brokered, and how they can do so.

PUTTING IT INTO PRACTICE: These rulemaking activities are a reminder that data broker activities are in legislators' minds. The obligations under these laws are for specific types of activities, but reflect a broader trend on concerns with sharing and "selling" of personal information, and are a reminder that companies may want to look at their practices even if not "brokers."

In 2024 Oregon Will Join List of States Requiring Data Broker Registration

Posted August 16, 2023

Oregon recently joined Vermont and California as the third state requiring data broker registration before collecting, selling, or licensing "brokered personal data." Several types of entities are exempt from the law. These include those collecting information from their customers, subscribers or users or those in a "similar" relationship or an entity acting as those companies' agents. Also exempt are consumer reporting agencies, financial institutions, and affiliates or nonaffiliated third parties of financial institutions subject to GLBA. The new law takes effect on January 1, 2024.

Provided an exception does not apply, companies will need to figure out if they sell or license information as that term is defined by the law and thus might be viewed as a "data broker." Unfortunately, the law is silent on what constitutes a "sale" of brokered personal data. Licensing means granting access or distributing brokered data to another person for consideration.

Information covered under the law ("brokered personal data") includes, *inter alia*, name, data or place of birth, maiden name of an individual's mother, biometric information, social security or other government-issued identification number. It also includes information that can "reasonably be associated" with the individual.

To the extent that the law applies, the "data broker" must register with the Department of Consumer and Business Services. In addition to paying a fee, they will need to include a declaration that describes whether consumers can opt-out of all or a portion of the data activities, how the consumer can exercise their opt-out choices, and whether an authorized agent can do so on the consumer's behalf. The DCBS will maintain a list of registered brokers on its website. Companies who do not register as required face penalties up to $500 for each day it fails to register. Penalties are capped at $10,000 per calendar year.

PUTTING IT INTO PRACTICE: This new law suggests that legislators may be renewing their focus on companies that sell or license personal information to third parties. While there are many exceptions under the law, this law serves as a reminder to examine information sharing practices.

DATA SECURITY

CNIL Fines Canal+ Over Marketing and Data Security Concerns

Posted November 27, 2023

The French Data Protection Authority announced a €600,000 fine against Groupe Canal+ over concerns with the media company's direct marketing activities. According to the CNIL, the company sent users email marketing without getting consent, in violation of both GDPR and French privacy law. In particular, the CNIL noted, the company sent marketing emails to individuals who had provided their personal information not to Canal+, but instead to one of its partners. When doing so, they were not told by the partner that the information would be share with -and used by- Canal+ for Canal+'s marketing activities. Canal+ should have ensured that the partners had gotten appropriate consent, according to the CNIL.

In addition, the decision against the company cited other alleged violations of GDPR. This included not disclosing in the company's privacy policy its data retention period. (The policy that was shared with users when they created a "MyCanal" account). It also included not giving privacy disclosures when contacting consumers by phone, and not responding to rights requests within a month after receiving them from consumers. It also, the CNIL indicated, did not respond to certain consumers' access requests.

In addition to data privacy concerns, the decision also highlighted data security concerns as well. According to the CNIL the company did not use appropriate security measures when storing employee passwords. It also failed to notify the CNIL of subscriber data that resulted in that data being viewable to others for five hours.

Putting it into Practice: This case is a reminder to review marketing consents, even when information is being collected by a third party. Companies may also want to review their rights requests and breach notification procedures.

SEC Gives Finality on Cybersecurity Disclosures for Public Companies

Posted September 28, 2023

The SEC has now finalized its much anticipated rules for public companies' cybersecurity disclosures. The final rules, published this month, require disclosure of certain cybersecurity incidents much sooner than under many other breach notification regimes. Additionally, the final rules require new periodic disclosures about a company's processes to assess, identify, and manage material cybersecurity risks and about the roles of management and the board of directors in managing or overseeing those cybersecurity risks. These new requirements vary from the SEC's prior (2018) guidance, and unlike in the past, are now codified under the Securities Exchange Act of 1934 and the Securities Act of 1933.

Under the new rule, a public company that suffers a "material cybersecurity incident" will have to file a Form 8-K disclosing the incident within four business days after the company's materiality determination. Material means it is substantially likely that an investor would consider impact of the incident important in making an investment decision, or if it alters the total mix of available information. In making this determination, companies should consider the total impact of the incident, including both immediate and long-term effects on finances, brand perception, customer relationships, and the like. The SEC acknowledges that evaluating whether an incident is material may take time, but it makes clear that companies should make that determination "without unreasonable delay."

The SEC further explains that, in the new Item 1.05 of the Form 8-K, the company must disclose the nature, scope, timing, and impact, or reasonable likely impact, of the incident. This includes reporting on the financial and operational impact of an incident. Additionally, to the extent any of the information required in Item 1.05 is not available at the time of initial reporting, companies are required to file an amendment to the Form 8-K containing such required information within four business days after the information becomes available. Though this final rule went into effect on September 5, 2023, the SEC has given most public company registrants until December 18, 2023 to start complying with the rule (smaller reporting companies—companies with revenues or public floats under certain thresholds—will not have to start complying with the incident disclosure requirements until June 15, 2024).

The final rules also amend Regulation S-K, adding a new "Item 106" to companies' annual 10-K filings. Beginning with fiscal years ending on or after December 15, 2023, public companies must add information about how they assess, identify, and manage their cybersecurity risks to their annual 10-K filing, including management's role in assessing and managing material cybersecurity risks and the board of directors' role in overseeing such cybersecurity risks. They must also disclose any cybersecurity incidents that materially affect or are likely to materially affect the company.

PUTTING IT INTO PRACTICE: December is not far away. Companies can begin now by reviewing their internal cybersecurity programs and incident response plans to address the four-day requirement and to ensure they have the necessary cybersecurity risk assessment and cybersecurity governance processes in place to include in their upcoming 10-K disclosures.

Iowa Joins Growing List to Offer Potential Safe Harbor for Companies With Security Programs

Posted August 10, 2023

Iowa recently became the fifth state to offer businesses a safe harbor if they have a written cybersecurity program. Others are Connecticut (October 1, 2021), Ohio (effective November 2, 2018), Oregon (effective January 1, 2020), and Utah (effective March 5, 2021). Like these, as of July 1, 2023, businesses that have a written cybersecurity program and suffer a breach may have an affirmative defense in Iowa against tort claims for inadequate security measures.

To take advantage of the safe harbor, the company must have a written cybersecurity program that contains certain elements. The program must, *inter alia*:

- Evaluate and mitigate anticipated risks on a continual basis
- Be of an appropriate scope and scale, measured by it costing "no less than [the company's] most recently calculated maximum probable loss value"
- Assess -at least annually- the potential maximum probable loss from a breach
- In the event of a breach, provide that the company will tell impacted parties what steps they can take "to reduce any damages"

These elements mirror those expected under other state safe harbor laws, but are more detailed than we have seen in the past. Program that reasonably conform to an industry recognized cybersecurity framework will be deemed to have a qualifying program.[1] These industry programs include the NIST Cybersecurity Framework, FedRAMP and ISO/IEC 2700. Businesses regulated by -and adhering to- several well-known laws will also be viewed as having a sufficient program. These include both HIPAA And GLBA.

[1] 554G.3(1).

PUTTING IT INTO PRACTICE: Iowa's safe harbor law picks up from similar provisions last passed by a state in 2021 (Connecticut). As the cost of breach-related lawsuits continues to rise, these provisions can offer some comfort to companies. We will be watching to see if other states begin incorporating similar provisions in their breach notice laws.

Cybersecurity Labeling Program to Increase Transparency of IoT Device Security

Posted August 3, 2023

In response to a constantly-evolving cyber threat landscape, the Biden Administration recently announced the launch of a new cybersecurity labeling program – the U.S. Cyber Trust Mark program – in an effort to enhance transparency and protection against cyber threats in the growing Internet of Things ("IoT") device space.

This program is the first of its kind in the cybersecurity sector and builds upon the National Institute of Standards and Technology's ("NIST") recent efforts to develop criteria for such a program as called for in Executive Order 14028, *Improving the Nation's Cybersecurity*. The labeling program currently is voluntary for IoT device manufacturers, but aims to create incentives for manufacturers to meet higher cybersecurity standards. Several major companies have already committed to participating in this program, as noted in the White House announcement.

The U.S. Cyber Trust Mark will appear on the packaging of eligible devices as a picture of a shield with a QR code that can be scanned to link users to a national registry of certified devices, which will contain up-to-date security information about the device.

This program proposal is described in a Notice of Proposed Rulemaking ("NPRM") and, if adopted by the FCC, will be opened for a public comment period on the proposal. The FCC anticipates that this program could be implemented by late 2024. Once implemented, the Cybersecurity and Infrastructure Security Agency ("CISA") will work with the FCC to encourage major U.S. retailers to prioritize products bearing the U.S. Cyber Trust Mark Label in the marketplace.

For more information on the U.S. Cyber Trust Mark, see our recent article on Sheppard Mullin's Government Contracts Law Blog.

PUTTING IT INTO PRACTICE: While this program is still in its preliminary stages, consumers and manufacturers can expect to see it move forward and provide momentum for similar labeling initiatives from other Federal agencies. Companies that manufacture smart devices may consider taking a detailed look at the security posture of their IoT products and consider participating in the program or other data security initiatives. The Sheppard Mullin team will continue to track updates to this program, as well as other Federal cybersecurity initiatives.

NIST Seeks Input on Standards for Protecting Sensitive Government Information

Posted June 15, 2023

The National Institute of Standards and Technology is updating the security standards that govern the protection of sensitive government information. NIST recently released an initial public draft for comment. The document will be the third version of its existing standard (NIST SP 800-171), *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The comment period closes July 14, 2023.

NIST SP 800-171 applies to entities that handle or store government data in their systems under government projects. It forms the baseline for data security requirements those entities must meet. Included in the standard are best practices for protection of sensitive information in company systems.

As we wrote in our sister blog, this proposed third version includes new and revised requirements and removes some outdated requirements. Some examples of new requirements include requiring organizations to:

- Develop and implement methods to mitigate supply chain risks;
- Establish a process for identifying or addressing weaknesses in the supply chain;
- Provide incident response training to users;
- Document an inventory of system components;
- Limit the number of external network connections to the system;
- Route internal network communications to external networks through an authenticated proxy server;
- Develop system and component configurations for individuals traveling to high-risk areas;
- Implement spam protection mechanisms at designated locations within the system to detect and act on unsolicited messages.

NIST anticipates releasing one more draft before publishing the final version in early 2024.

PUTTING IT INTO PRACTICE: The changes NIST has made to this standard mirror what we are seeing in other industries and reflect growing focus on data security. Those interested can make comments before the deadline to 800-171comments@list.nist.gov. We will be continuing to track this development and monitor for the final version.

New York AG Releases Guide for Business Data Security

Posted May 22, 2023

New York Attorney General Letitia James recently published a guide to help companies in preparing their data security programs and responding to data security incidents. The security program recommendations are paired with highlights from recent investigations by the Attorney General that provide valuable insights into what the Attorney General views as data security pitfalls that should be remedied.

The guide contains nine items the AG recommends including in data security programs. These include security measures like use of multifactor authentication and complex passwords, encryption of sensitive data, and deletion of old or unused accounts. It also includes policy advice like maintaining a data storage map so companies know where sensitive data is located, and proper auditing of vendor information security practices. Importantly, two of the nine recommendations focus on responding to a data security incident, which makes clear that incident response is an essential part of a well-rounded data security program.

Putting it into Practice: The guide puts companies on notice of some of the key factors the NY Attorney General's office looks for in their data breach investigations. By including practical examples, the AG signals a clear list of features that should be addressed in every data security program.

Graduation Goods Settlement: A Good Reminder of AGs' Data Security Priorities

Posted February 1, 2023

The New York and Pennsylvania AGs settlement with Herff Jones from late last year provides guidance to businesses about expected security measures as we enter into 2023. The case arose after Herff Jones, producer and seller of graduation goods, suffered a breach resulting in the theft and sale of customer payment card information.

The AGs alleged the breach of consumers' payment card information resulted from the company's failure to use reasonable data security measures. According to the AGs, the company also did not comply with the Payment Card Industry Data Security Standards, a contractual obligation placed by credit card companies on those entities who accept credit card payments.

Under the settlement, Herff Jones has agreed not only to pay $100,000 to each AG but also to implement a comprehensive written information security program within 180 days from the date of the settlement. The security procedures agreed upon illustrate the expectations these AGs -and likely others- have of companies' security programs. Namely, Herff Jones has agreed to:

- **Implement and perform annual information security risk assessments** that conform to standards issued by information security organizations such as NIST, ISO 27005, and CIS RAM.
- **Implement certain minimum reasonable information security safeguards** designed to safeguard and protect personal information. These include installing only approved software and using software patch management program with automated, standardized patch management distribution tools to deploy, verify, and track patches. Also included are a penetration-testing program designed to identify, assess, and remediate security vulnerabilities and segmented card data environment from other areas of the company's IT infrastructure.
- **Reasonable measures to detect and respond to security incidents**, such as log correlation and alerting, file and data integrity monitoring, intrusion detection and prevention tools, and a documented incident response plan.
- **Access controls**, such as multi-factor authentication, one-time passcodes, location-specific requirements, and other access enhancements.
- **Designate a qualified individual** to being charge of program oversight who will, among other things, advise senior leadership on risks and remediation strategies.
- **Annually conduct cybersecurity awareness training** for employees with key responsibilities for information security.
- **Comply with the PCI data security standards**.
- As part of the settlement, within one year of the date of the settlement agreement and then biennially for 5 years thereafter, the company is required to have a qualified and independent third-party evaluate and test the effectiveness of their information security program.

PUTTING IT INTO PRACTICE: Portions of the expectations set out by these two AGs mirror those in other settlements in 2022, including by the FTC and the NYDFS. These include comprehensive risk assessments and security programs, certain minimum technical and administrative safeguards, and qualified personnel designated to handle information security.

FINANCIAL PRIVACY

Impact of FTC Safeguard Rules Amendment on Breach Notification Timing

Posted November 20, 2023

The FTC recently amended the Safeguards Rule to make non-banking institutions such as mortgage brokers, motor vehicle dealers, and payday lenders notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach involving the information of at least 500 consumers. The FTC plans to provide an online form that will be used to report certain information, including the type of information involved in the security event and the number of consumers affected or potentially affected. The FTC's Safeguards Rule also requires non-banks to develop, implement, and maintain a comprehensive security program to keep their customers' information safe.

As reported by our sister blog here, in October 2021, the FTC announced it had finalized changes to the Safeguards Rule to strengthen the data security safeguards that financial institutions are required to put in place to protect their customers' financial information.

PUTTING IT INTO PRACTICE: Companies collecting sensitive consumer data should be reminded that they have a responsibility to protect such data, as well as be transparent if that information has been compromised. Non-banks may wish to develop steps into their regular data incident response planning for reporting to the FTC the types of data breaches and other security events as described in the amendment.

NY Enhances Financial Cybersecurity Regulations

Posted November 16, 2023

New York recently announced amendments to the State Department of Financial Services' cybersecurity regulations. The changes further solidify the state's already comprehensive cybersecurity regulatory regime. The amendments were both announced by Gov. Hochul and became effective on November 1, 2023. They apply to DFS regulated entities and aim to strengthen provisions around cyber governance, risk mitigation, incident notification, and training.

New obligations under the amendments include:

- Senior leadership is now explicitly required to exercise oversight of an entity's cybersecurity risk management.
- CISOs must make timely reports to an entity's senior leadership on material cybersecurity issues, including on cybersecurity events and changes to the entity's cybersecurity program.
- Previously required cybersecurity risk assessments must now be conducted annually, or whenever there is a material change to the covered entity's cyber risk.
- Entities must now conduct annual cybersecurity awareness training that includes training on how to address social engineering.
- Incident response plans must now include business continuity and disaster recovery plans. These plans must also be tested annually.
- Entities must notify DFS within 24 hours after making an extortion payment (i.e. a ransomware payment) and provide a detailed explanation of the reasons for making the payment within 30 days.

The amendments also created additional obligations for larger "Class A companies." These are companies with a two-year average of (1) at least $20 million in gross revenue (including instate revenue from affiliates) and; (2) 2000 employees or $1 billion in total annual revenue (including all affiliate revenue). Class A companies must design and conduct independent cybersecurity program audits, implement a privileged access management solution that includes specific password requirements, and deploy an endpoint detection and response solution that includes logging and security event alerting.

PUTTING IT INTO PRACTICE: These updated regulations continue to demonstrate that New York State remains hyper-focused on cybersecurity. Regulated entities should review the new regulations carefully and take care to ensure they update their policies and procedures to comply with the new requirements.

CFPB Director Elevates Priorities for Data Privacy & Repeat Offenders

Posted April 17, 2023

On April 4, CFPB Director Rohit Chopra delivered remarks at the International Association of Privacy Professionals' Global Policy Summit on the importance of reigning in repeat violators of consumer finance and privacy laws. According to the Director, the CFPB is to enhance penalties against repeat offenders of consumer protection laws. Such penalties could involve a broader range of agency remedies, including naming executives in enforcement actions and placing meaningful limitations on future business practices, in addition to simple fines.

Notably, Director Chopra stated that the CFPB intends to focus on enforcement in the context of violations of consumer data protection laws, whether by small firms, tech conglomerates, or companies situates in the middle. Director Chopra highlighted a number of privacy-related priorities that include:

- Addressing the potential risks associated with tech companies moving into the digital payments market;
- The safety and soundness of digital currencies; and
- The use of "dark patterns" allegedly designed to manipulate consumers into buying products and/or sharing their personal information.

PUTTING IT INTO PRACTICE: Director Chopra's remarks underscore recent agency enforcement actions against repeat offenders (see previous posts from our sister blog here and here). The CFPB and other agencies are focused on identifying noncompliance with consent orders and remain intent on enforcing substantial penalties against companies that they deem to be repeat offenders. Accordingly, companies that are subject to ongoing consent orders, whether with the CFPB or other agencies, should confirm and document their compliance with such consent orders or else risk facing enhanced penalties, especially where such consent orders relate to alleged violations of consumer privacy law.

72 hours: The NCUA's New Cyber Incident Reporting Requirement

Posted March 16, 2023

Three days. Starting September 1, 2023, that is all federally insured credit unions will have to report cyber incidents.

The rule, approved on February 16, 2023, broadly defines cyber incident to include any incident that jeopardizes an information system or the information stored in one. Reportable incidents however are defined by a slightly less broad, but perhaps more complex, three-part definition that also requires a report when a credit union has a "reasonable belief" it has been the victim of a cyber attack:

- Part one requires a report if the incident causes a substantial loss to an information system. This includes through the exposure of data, disruption of vital services, or as a result of a serious impact to the safety and resiliency of a system.
- Part two requires a report in the event of an incident that causes a disruption to business operations, vital services, or to an information system.
- Part three requires a report if a third-party informs a credit union that credit union data or business operations have been compromised. This portion of the rule only applies to third-parties that have a relationship with the credit union.

Procedurally, the report must be provided to the credit union's designated NCUA's point of contact no later than 72 hours after it experiences or reasonably believes it has experienced a reportable cyber incident. In the case of third-party notification, the 72 hour period begins to run from the time of the third-party notification. A credit union need not fully assess the incident before making its report.

PUTTING IT INTO PRACTICE: This rule is another example of a regulator trying to move organizations towards a faster reporting deadline. Federally insured credit unions should organize their incident response plans to respond in kind.

CFPB Starts Year Seeking Comments on Proposals to Give Consumers Enhanced Control of Financial Data

Posted January 9, 2023

Recently, the CFPB released an outline of proposed measures related to the Bureau's Dodd-Frank Section 1033 rulemaking efforts that would allow consumers to take control of their personal financial data and determine which third parties could have access to such data. The CFPB is seeking comments on the rulemaking, by January 25, 2023.

Data aggregation companies have been pursuing such a rule for years, primarily in the face of opposition by banks and other financial institutions concerned about data security and liability related to allowing third-party access to customers' online accounts. The outline discusses proposed regulations that would require covered financial institutions to make consumer financial data available directly to a consumer and to any third parties authorized by the consumer. In a high-level summary of the proposed regulations, the CFPB discusses the regulatory provisions it is considering proposing, including the following:

- **The types of information to be made available to third parties:**
- periodic statement information for settled transactions and deposits
- information regarding prior transactions and deposits that have not yet settled
- other information about prior transactions not typically shown on periodic statements or portals
- online banking transactions that the consumer has set up but that have not yet occurred
- account identity information.
- **How and when information would need to be made available.** The Bureau is considering ways to define the methods and the circumstances in which a financial institution would need to make information available with respect to both direct access and third-party access.
- **Third party obligations.** The CFPB is considering proposals under which authorized third parties would have to limit their collection, use, and retention of consumer information to what is reasonably necessary to provide the product or service the consumer has requested.
- **Implementation period.** The Bureau is seeking feedback on timeframes to ensure consumers are able to benefit from a final rule, while also considering implementation factors for data providers and third parties.

The CFPB proposals have parallels to many recent state privacy laws in California, Virginia, Colorado, Utah, and Connecticut that have focused on data access rights, data minimization, and third-party obligations. One meaningful difference from the state regimes is that the CFPB's outline does not exempt data or entities subject to the Gramm-Leach-Bliley Act (GLBA). In fact, companies subject to GLBA are one of the primary targets of these regulations.

PUTTING IT INTO PRACTICE: Data sharing protocols that have been in place at banks for nearly two decades under GLBA (e.g., notice-and-opt-out requirements) are likely to require significant updates under the new rules, in-line with some of the state privacy laws currently that give consumers more control of how data is shared.

GOVERNMENT PRIVACY

Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Five- Further Adoption of FedRAMP & StateRamp

Posted January 25, 2023

To conclude our series of cybersecurity areas to focus on in 2023 for those who do business with the Federal government, we look at the FedRAMP and StateRAMP developments from 2022. For the rest of this series, see our prior articles (Part One, Part Two, Part Three, and Part Four).

FedRAMP Authorization –The Federal Risk and Authorization Management Program (FedRAMP) Authorization Act was signed into law as part of the FY23 National Defense Authorization Act. The Act officially codified FedRAMP as the definitive standardized security assessment and authorization program for federal procurement of cloud products and services. To encourage further agency adoption of FedRAMP, the Act includes a "Presumption of Adequacy" which states that a FedRAMP authorization package is presumed adequate for any agency authorization. This allows an agency to use a FedRAMP authorized offering without having to conduct any additional review. FedRAMP is also directed to establish a means for the automation of security assessments and reviews. These measures should further reduce barriers for agency adoption of cloud services and products.

The Act subjects the FedRAMP program to additional rulemaking requirements – any proposed FedRAMP guidance or directives that may have an impact on cloud service providers must undergo a public comment period. Additionally, the Act also calls for the creation of two advisory boards that will provide additional guidance to the program: the FedRAMP Board, consisting of federal stakeholders, and the Federal Secure Cloud Advisory Committee, comprised of federal and industry stakeholders.

FedRAMP, Revision 5 Baselines – In early 2022, FedRAMP was in the process of updating its standards to better align with NIST SP 800-53, Revision 5 standards. FedRAMP planned on releasing a draft of the new FedRAMP Revision 5 baseline standards for public comment, but has been notably silent since spring 2022. In Fall 2022, FedRAMP sought additional public comment on updating the Authorization Boundary Guidance. You can read our article about the rulemaking for the Authorization Boundary Guidance here.

StateRAMP – Modeled after the FedRAMP program, the State Risk and Authorization Management Program (StateRAMP) provides a common standard and model for states and local governments to verify that cloud products and services have appropriate security controls in place. In 2022, Arkansas, Colorado, Maine, Nebraska, North Dakota, Vermont, and West Virginia joined StateRAMP as participating government members, bringing the number of StateRAMP participating organizations to 23. The National Association of State Procurement Officials (NASPO) announced the addition of StateRAMP as a strategic partner to "help its members achieve success as public procurement leaders in their states" through the development of educational content and resources for state governments.

PUTTING IT INTO PRACTICE: What to expect in 2023: We expect that FedRAMP and StateRAMP programs will continue to gain traction as adoption of these programs becomes more widespread. We continue to eagerly await the release of the FedRAMP, Revision 5 baselines and any updates to the Authorization Boundary Guidance.

Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Four-Federal Acquisition Regulation (FAR) Updates

Posted January 24, 2023

The federal government has continued its efforts to fulfill the requirements set forth in Executive Order 14028, *Improving the Nation's Cybersecurity*. For companies that do business with the Federal government, beyond looking at the other issues raised in this series of posts (see here, here and here), these efforts will be important to keep in mind in 2023. There are three efforts underway by the FAR Council to amend the Federal Acquisition Regulations (FAR) related to the Executive Order (in addition to the Secure Software efforts discussed in Part Three).

- **Cyber Threat and Incident Reporting and Information Sharing** – new provisions will require information technology and operational technology service providers to collect and preserve information related to cybersecurity incidents on federal information systems and report relevant information to the federal government. These requirements may impose a tight timeline similar to the 72-hour incident reporting requirement currently in the DFARS. OMB received a proposed FAR rule in December 2022; if approved we may see proposed language this year.
- **Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems** – the federal government currently is undergoing an effort to standardize cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems. It is unclear how or if this clause would impact ongoing federal efforts to adopt the Controlled Unclassified Information (CUI) Program managed by National Archives Records Administration (NARA), which is also pending at OMB. These requirements may be similar to the DoD CUI requirements reflected in the DFARS. OMB received a proposed FAR rule in December 2022; if approved we may see proposed language this year.
- **Establishing FAR Part 40** – this is an effort to amend the FAR to create a new FAR part, Part 40, which will be the single, consolidated location for cybersecurity supply chain risk management requirements. It is unclear at this point which FAR clauses will be included in this section. OMB listed this proposed FAR measure in the "Final Rule Stage" and tentatively anticipates it will be finalized this spring.

PUTTING IT INTO PRACTICE: What to expect in 2023: We continue to monitor for updates to the FAR. However, contractors and suppliers can begin preparing for additional requirements for safeguarding controlled unclassified information and cybersecurity incident reporting by reviewing current requirements in the DFARS and related guidance.

Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Three-Secure Software Development Attestation Requirements

Posted January 23, 2023

Today we continue our series (see here and here) with the Office of Management and Budget's September 2022 memorandum requiring federal agencies to only use software from software producers that attest compliance with secure software development guidance issued by the NIST. The new requirements will apply to any third-party software that is used on government information systems or that otherwise "affects" government information. You can read our article about the guidance here.

The FAR Council is currently drafting a proposed FAR rule addressing Supply Chain Software Security to integrate these requirements into federal contracts.

PUTTING IT INTO PRACTICE: What to expect in 2023: OMB's guidance provided a timeline for agency adoption of these requirements and when requirements will be communicated to software producers. We expect agencies will begin communicating requirements in early 2023 and begin collecting attestation letters for critical software this summer. Software producers should evaluate their software against the NIST guidance. For federal contractors and software resellers, the impact and scope of these requirements remains unclear, but we anticipate additional guidance in 2023.

Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Two-NIST SP 800-171, Revision 3

Posted January 19, 2023

In this second in our series, we look at the long awaited update to NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," which is expected to be released in late spring 2023. NIST SP 800-171 forms the backbone for contractor security requirements in Department of Defense regulations and the CMMC program. It remains unclear if this update will impact the rollout of the CMMC program.

The National Institute of Standards and Technology (NIST) sought feedback in July 2022 on improvements to NIST SP 800-171 and the related CUI series of publications. It released an analysis of the public feedback in November 2022. According to NIST, the update will align requirements with NIST SP 800-53, Revision 5 and include an overlay of CUI security requirements to NIST SP 800-53.

PUTTING IT INTO PRACTICE: What to Expect in 2023: We expect to see further efforts to adopt a government-wide regulation protecting Controlled Unclassified Information, based on NIST SP 800-171, in the Federal Acquisition Regulations (FAR). Contractors subject to DoD regulations should continue to monitor for updates to the NIST CUI series and ensure ongoing compliance with these standards.

Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part One-CMMC Developments

Posted January 18, 2023

In this second in our series, we look at the long awaited update to NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," which is expected to be released in late spring 2023. NIST SP 800-171 forms the backbone for contractor security requirements in Department of Defense regulations and the CMMC program. It remains unclear if this update will impact the rollout of the CMMC program.

The National Institute of Standards and Technology (NIST) sought feedback in July 2022 on improvements to NIST SP 800-171 and the related CUI series of publications. It released an analysis of the public feedback in November 2022. According to NIST, the update will align requirements with NIST SP 800-53, Revision 5 and include an overlay of CUI security requirements to NIST SP 800-53.

PUTTING IT INTO PRACTICE: What to Expect in 2023: We expect to see further efforts to adopt a government-wide regulation protecting Controlled Unclassified Information, based on NIST SP 800-171, in the Federal Acquisition Regulations (FAR). Contractors subject to DoD regulations should continue to monitor for updates to the NIST CUI series and ensure ongoing compliance with these standards.

HEALTHCARE PRIVACY

CCPA Amendments Extend Protections to Reproductive Health and Citizenship Status

Posted October 27, 2023

Governor Newsom recently signed two amendments to the CCPA strengthening protections for certain data types. The changes go into effect January 1, 2024.

One of the amendments, AB-947, extends the definition of "sensitive personal information" to include citizenship and immigration status. Current categories of sensitive personal information include precise geolocation, racial or ethnic original, religious beliefs, and genetic data. Citizenship and immigration status are already considered sensitive data under privacy laws in Connecticut and Virginia. Collecting sensitive personal information in California triggers certain notice, use, and opt-out rights.

CCPA currently allows businesses to cooperate with law enforcement and government agencies by providing personal information that is requested pursuant to official investigations. Now, AB 1194 specifically carves out reproductive health data. This means that information related to "accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services" need not be provided in an official investigation. It does not limit a business's obligations to preserve information in a civil proceeding or where required by law. These amendments were prompted by heightened concerns involving government access to records of individuals seeking reproductive healthcare following the *Dobbs* decision at the Supreme Court. This follows trend with other types of California amendments strengthening reproductive privacy protections. It also follows other states and FTC's heightened concerns about information involving a person's health that might not be covered by HIPAA.

PUTTING IT INTO PRACTICE: Businesses should refresh their data mapping exercises to identify where they may collect personal information related to citizenship, immigration status and reproductive health. For citizenship or immigration status information, the CCPA's sensitive personal information requirements should be adopted.

Regulators Send Warning Letter to Hospitals and Telehealth Providers About Tracking Technology Use

Posted July 24, 2023

The FTC and OCR at HHS are continuing to scrutinize the use of tracking technologies that may reveal information about a person's health or health status. Both agencies recently sent a letter to a reported 130 hospitals and telehealth providers warning about the use of tracking technologies and the risks they pose. This follows on the heels of other statements, guidance, and enforcement actions from these regulators about these tools over the past two years.

Last year, OCR highlighted its concerns about the improper disclosure of protected health information through the use of tracking technologies in a bulletin. While there are certain considerations for organizations regulated by HIPAA when it comes to the use of cookies and other tracking tools, companies outside of HIPAA have their own set of requirements to keep in mind. This includes the FTC's Health Breach Notification Rule (HBNR) (currently under review to amend) and unfair and deceptive practice allegations under Section 5 of the FTC Act. There may be other considerations under state "comprehensive" privacy laws as well.

The FTC first foreshadowed how these considerations apply to non-HIPAA "health information" in 2021 in a case with a popular fertility tracking app. There, a company was inadvertently disclosing information about fertility status via tools used to track analytics events (not marketing). Ultimately, depending on how a company configures the use of a tracking technology on its site and/or apps, the disclosure of "health" information without a consumer's authorization may violate the FTC Act and the HBNR. Companies regulated by HIPAA are not subject to the HBNR, but could still face FTC Act violations. Additional published resources (here and here) and the recent string of cases against digital health companies this year has further cemented that this remains a key priority for the FTC.

PUTTING IT INTO PRACTICE: This warning letter adds nothing substantively new to the conversation about the use of tracking technologies on sites and apps that collect data revealing information about a person's health. However, it undoubtedly signals a clear and unequivocal warning to companies to carefully audit the use of tracking technologies (even if for analytics and not marketing) that may convey information about a person's health and take steps to remediate. The disclosure of personal health information without the data subject's authorization may violate HIPAA, Section 5 of FTC Act, the

HBNR and/or the entity's privacy notice. While the letter serves as a notice to companies to the extent they are using tracking technologies, it also serves as a reminder of potential civil penalties for using these tools in a way that contradicts agency guidance. The notice also represents another example of the FTC's strategy to bring joint enforcement actions with other agencies (both state and federal) and to seek civil penalties in light of the the Supreme Court's *AMG Capital* decision (which curbed the FTC's ability to seek certain monetary relief).

FTC Looks to Update Health Breach Notification Rule, Targeting Digital Health Industry

Posted June 26, 2023

The FTC recently proposed amendments to the Health Breach Notification Rule (HBNR). This is on trend with its aggressive interest over the last couple of years in health data not covered by HIPAA.

Generally, in its current state, the rule requires vendors of "personal health records" and related entities not covered by HIPAA to notify consumers, the FTC, and the media of a breach of unsecured identifiable health information. While the HBNR had long been a dormant arrow in the Commission's quiver, it resurfaced in 2021 when the FTC released a somewhat controversial position statement about the scope of the rule and its applicability. Since then, the FTC has continued to take interest in health data not covered by HIPAA, including several enforcement actions this year. The proposed rule seeks to codify some of the positions taken in the Agency's position statement. Specifically, the proposed rule seeks to:

- **Expanded scope of entities**. The changes would revise several definitions to clarify the rule's application to health apps and similar technologies not covered by HIPAA. More entities will be subject to this rule through the addition of two terms – "health care provider" and "health care services or supplies" which includes any online service that provides health-related services or tools to track diseases, health conditions, medications, diet, sexual health, and more.
- **Revised definition of breach**. A reportable breach under the Proposed Rule includes not just data breaches, but *any* disclosure that is not authorized by a consumer.
- **Clarifications about drawing health information from multiple sources.** The PHR definition applies to products with the ability to obtain data from multiple sources. The proposal would clarify that this includes applications that have the technical capacity to draw information from multiple sources, even if a consumer only uses one of those sources when using an app.
- **Additional notification options**. The Proposed Rule would permit notification to impacted consumers, with their consent, by text, in-app messaging, or electronic banner in an application.
- **Changes to content requirements for notifications**. In addition to the existing content requirements, the Proposed Rule would require a description of the potential harm that could result from the breach, contact information of any third parties that acquired the information at issue, and what the entity is doing to protect affected individuals.

PUTTING IT INTO PRACTICE: In light of the FTC's recent string of HBNR enforcement actions, developers of health and wellness apps and devices should assess whether HBNR applies and ensure that any sharing of information would not constitute an unauthorized disclosure. Comments on the proposed rule will be accepted until August 8, 2023.

My Health My Data Act: Consent Requirements

Posted May 3, 2023

In this third post in our ongoing series, we examine the scope of the consent requirements under the recently enacted My Health My Data Act. (Visit here for information about the scope of the law and here for information about consumer rights). The Act imposes consent requirements on a wide range of common processing activities.

What is "consent"?

Consent under the law must be affirmative, freely given, specific, and informed. For consent to be valid, it cannot be obtained by a consumer (1) accepting a general terms of use or similar agreement, (2) hovering over, muting, pausing, or closing a piece of content, or (3) agreeing where such agreement was obtained though deceptive design.

When is consent required?

Generally, the Act requires consent for any processing of consumer health data beyond what is necessary to provide a consumer-requested product or service. A separate consent is required for any "sharing" of consumer health data beyond what is necessary to provide a consumer-requested product or service. An "authorization" (a higher level of consent) is required for any disclosure of data that would be considered a "sale" of consumer health data under the Act. Any consent must be separate from other consents. Like CCPA, "sell" is defined broadly to mean exchange of consumer health data for monetary or other valuable consideration. Given the breadth of what constitutes a sale, the requirement could be interpreted as a complete prohibition on targeted advertising using any consumer health data.

What is an authorization?

While an authorization is a concept familiar to HIPAA-regulated entities, it is not a concept in most consumer privacy laws. Under this law, an authorization is a lengthy document that contains a long list of specific information and statements that must be signed and dated by the consumer. A copy of the signed authorization must be provided to the consumer and both the seller and the buyer of the data must retain a copy of the authorization for 6 years. Authorizations will expire after one year.

Putting it into practice: The heightened and broad scope of consent requirements under this law is likely to have the effect of chilling certain processing activities altogether. Organizations should carefully evaluate their activities and consider how it would obtain consent for any beyond what is necessary to provide the product or service. Companies will also need to keep in mind how to manage requests withdrawing consent.

My Health My Data Act: Consumer Rights

Posted May 2, 2023

In this second post in our ongoing series, we examine the scope of rights given to consumers under the recently enacted My Health My Data Act. (Visit here for information on the scope of the law). The law provides consumers several rights, all of which are in other privacy laws. However, the requirements associated with some of these rights create some unique challenges.

Under this law, consumers have a right of access, a right to delete, a right to withdraw consent, and a right to not be discriminated against for exercising their rights.

- **Right to access**. This gives consumers the right to confirm whether a regulated entity is collecting, sharing, or selling consumer health data about them. It also gives them a right to access such data. It goes further than other privacy laws by also giving consumers a right to receive a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data *and* an active email address or other online mechanism for contacting these third parties.

- **Right to delete**. Most privacy laws (except for HIPAA) create a right to delete. However unlike other laws, this Act is missing common exceptions to the right to delete. For example, an exception for when data may be required to defend against legal claims or to comply with legal obligations. There is also a passthrough obligation to this right. If a deletion right is exercised, regulated entities must also notify all affiliates, processors, and other third parties with whom the data was shared. The recipient must also delete the data. The deletion requirement also applies to data archives and backups, though there is a 6 month deadline to complete.
- **Right to withdraw consent**. The Act gives consumers the right to withdraw consent for the "collection and sharing" of consumer health data. Because the Act requires consent for processing beyond what is necessary to provide the requested product or service there could be a wide range of data subject to withdrawal.
- **Right of non-discrimination**. The Act also provides that regulated entities "may not unlawfully discriminate against a consumer for exercising any rights" under the Act. Unlike the CCPA non-discrimination right, however, this provision does not specify any details about what kind of discriminatory practices are prohibited.
- The procedure aspects for responding to rights requests borrow from other privacy laws. Specifically, organizations must have a secure and reliable means for consumers to submit requests and need to authenticate the consumer making the request. Companies are prohibited from charging a fee for up to two requests annually. Responses should be provided within 45 days (which can be extended another 45 days). Companies must also offer an appeal process denied requests.

PUTTING IT INTO PRACTICE: While companies subject to other privacy laws will be familiar with the type of consumer rights and procedural requirements, there are several notable differences in handling rights requests under this Act. These challenges, along with the law's private right of action, will increase risk for companies that receive requests. In our next post we will examine the obstacles created by the broad consent requirements.

My Health My Data Act: Scope of the Law

Posted May 1, 2023

On April 27, 2023, the state of Washington enacted a landmark privacy law aimed at protecting the privacy of health data *not* covered by HIPAA. While the 2023 legislative season has been busy for state "comprehensive" privacy laws, this law is likely to have the most impact on businesses. The My Health My Data Act covers a very wide range of entities, consumers, and data, as we describe below. And, it contains a private right of action. With the law coming into effect in the first half of 2024, organizations will want to take steps now to understand the scope of this law and its onerous obligations.

What Entities are Covered by the Act?

The law applies to "regulated entities" as defined by the Act. The definition is sufficiently broad that it will apply to most non-governmental entities – including non-profits. A "regulated entity" is any entity that (1) conducts business in Washington, *or* produces or provides products or services targeted to consumers in Washington, and (2) alone, or jointly with others, determines the purpose and meanings of collecting, processing, sharing, or selling of consumer health data.

The Act also defines "small businesses." However, "small businesses" are a subset of regulated entities and the only difference in the Act is that for *some* provisions, there is a different effective date for small businesses. As we discuss below, there are a number of exclusions in the Act, primarily for data covered by other enumerated privacy laws.

What Consumers are Covered by the Act?

"Consumer" means (1) a natural person who is a Washington resident; *or* (2) a natural person whose consumer health data is *collected* in Washington. The definition excludes employees and B2B data (unlike CCPA). While the first prong seems to set a geographic boundary on the scope of consumers covered, the second prong creates a surprising

broader scope. The second prong could be interpreted to mean that personal data of individuals with no connection to Washington are captured by the law if the data is "collected" in Washington. "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner.

What Data is Covered by the Act?

The law applies to "consumer health data." Given the broad scope of the definition, it is easier to first think about what data is *not* included in the Act.

There are exceptions for data that is subject to certain enumerated privacy laws such as HIPAA, GLBA, FCRA, FERPA, and existing Washington state laws related to health care and insurance. The exception covers nearly all health information processed by a HIPAA covered entity or a business associate processing the data on behalf of a covered entity. Data that is not covered by HIPAA, but that originates from and is maintained by a covered entity or business associate and intermingled with HIPAA-covered data is excluded.

The law also excludes employee and B2B information (since those persons are excluded from the definition of consumers). There is also an exception for data used for certain peer-reviewed research in the public interest. Deidentified information (as defined in the Act) and "publicly available" information are also excluded.
With the lens of what data is not in scope, we turn to the actual definition of "consumer health data." This is defined as any personal information that is "linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." The definition goes on to enumerate a list of data types that are included within "physical or mental health status," though the list is non-exclusive. The list includes data that identifies a consumer seeking health care services and any information that is derived or extrapolated from non-health information.

PUTTING IT INTO PRACTICE: The enactment of this law fits within the growing trend of increased focused around health information and the privacy laws that govern it. Given the sweeping scope of this law, companies should carefully evaluate to what extent the law may apply. We may see some companies geo-blocking consumers from Washington and avoiding processing data in Washington as a way to limit potential exposure under the Act. In the coming days we will discuss other aspects of the law, including the consumer rights provisions and consent requirements.

HHS Release Cybersecurity Guide

Posted March 29, 2023

The US Department of Health and Human Services recently updated its guide to help the private and public healthcare sectors develop cybersecurity protocols that address NIST's Framework for Improving Critical Infrastructure Cybersecurity. The guide is a toolkit, with information and resources intended to help companies implement cybersecurity programs in the health care space. While the aim of this guidance is to help companies implement NIST's protocols for protecting US critical infrastructure, the recommendations contained in the guide mirror other agencies' security recommendations (for example those we have written about from the Department of Labor and the FDA).

Included in the guide are recommendations on implementing NIST's seven-step cybersecurity framework (prioritize – orient – create a current profile – risk assessment – target profile – gap identification – action plan). Within the guide are items specific to health care providers, including conduct an enterprise wide inventory of the creation, reception, maintenance, and transmission of electronic protected health information (ePHI) and doing a business impact analysis on systems that create, receive, maintain, and transmit ePHI. The guide also contains information about external resources available to assist in cybersecurity efforts (with a list of many tools developed for the health care industry, like the Health Care and Public Health Risk Identification and Site Criticality Toolkit).

PUTTING IT INTO PRACTICE: While this guide is intended as a resource rather than a compliance roadmap, it is a reminder that HHS is increasing its focus on cybersecurity.

US STATE COMPREHENSIVE PRIVACY LAWS

Closing Out 2023 with Utah's Privacy Law

Posted December 26, 2023

This year has been active on the state "comprehensive" privacy law front. Seven states passed new laws in 2023 (Delaware, Iowa, Indiana, Tennessee, Montana, Florida, and Oregon). These states joined California, Connecticut, Colorado, and Virginia with laws already in effect. Soon, Utah will join the "active" law list when its privacy law comes into effect on December 31.

For companies complying with the laws already in effect, little additional steps need be taken for Utah. That said, with each new law going into effect, companies would be well-served to review key components of the privacy program to help ensure that existing programs and processes are reflective of the then-requirements. This includes:

- **Confirming Applicability**. Each time a law goes into effect, companies should re-assess which of the US laws apply (or not) to it. These laws primarily apply based on revenue and/or volume of personal information processed – two factors that may have changed since last evaluated. Our blog post here helps summarize the thresholds and criteria for when a law may apply or not.
- **Review Notice Obligations**. Best practice is to review a privacy policy at least annually, or during any new data collection activity. As part of this process, it would also help to double-check that the current privacy policy checks the boxes of the state content requirements (as we summarize here).
- **Choice and Rights**. Like a privacy policy, the process for handling individual rights may also require some elements of continual evaluation and improvement. Assessing how current practices are mapping to the statutory requirements may shed light on the need for additional updates or modifications.
- **Vendor Contracts**. By now, many are familiar with updating standard privacy and cybersecurity contractual terms due to changing legal requirements. As part of overall house-keeping companies should verify that its templates similarly adhere to state requirements.

PUTTING IT INTO PRACTICE: Even if your organization is not subject to Utah's privacy law, now is a good time to access how compliance with state privacy laws is going. And, while Utah's law was generally viewed as more "business friendly" when passed, Utah is signaling itself to be a state with more interest in matters involving privacy and cyber, which may impact the enforcement level of this law. For example, Utah created a "Cyber Center" and enacted a law aimed and social media and minors.

California Releases Automated Decision Rules in Draft

Posted December 20, 2023

The CPPA, the California regulatory body charged with enforcing CCPA, recently released draft regulations for use of automated decisionmaking technology. The draft comes under the law's requirements for the agency to issue regulations on the topic. Under the law, automated decisionmaking technology is discussed in relation to profiling. Profiling is defined as "any form of automated processing of personal information" to analyze or predict people's work performance, health, personal preferences, and the like. However, what constitutes "automated decisionmaking technology" is not defined.

CCPA calls for rules to give consumers the ability to opt out of use of these technologies, and to access information about how the tools are used to make decisions about them. The rules have fairly onerous obligations on those who use these technologies. As such, the definition of them -and the times when they are being used- is particularly important. Of concern for many is how broad the current definition is, namely, any system, software or process that helps in human decision making.

As proposed, the rules include the following obligations:

- **Give consumers a "pre-use notice."** This notice would need to include, among other things, an explanation in plain language of how, *specifically*, the business will use these technologies. It also needs to outline how consumers can exercise their opt-out rights.
- **Give consumers the ability to opt out of certain uses of the technologies.** These include when they would be used to produce legal or similarly significant effects. It also includes times when a consumer is profiled while acting in their capacity as an employee, contractor, or job applicant. And, when profiling a consumer in a public place or for those known to be under 16. It also includes when trying to train automated decisionmaking technology.
- **Give consumers information about how these technologies are being used to make decisions about them**. For example, businesses must provide a direct notice to consumers if they make a decision using the technologies that results in the denial of goods or services. Businesses must also provide an explanation for the denial and information about the right to file a complaint with regulators.
- **Implement processes for handling information of minors between the ages of 13 and 16 and children under 13**. These include, for example, provide opt in consent for using such children's information for behavioral advertising purposes.

The draft is not final, and received criticism at the CPPA's recent public board meeting. There, the agency indicated that the intent was to facilitate public participation and board discussion. This draft follows other new draft regulations from the agency, including on risk assessments and cybersecurity audits.

PUTTING IT INTO PRACTICE: The regulations are not yet final. However, businesses can start preparing for the regulations by inventorying the various tools and technologies, including HR tools, that they use to facilitate human decision making.

California's "Delete Act" Significantly Expands Requirements for Data Brokers

Posted October 12, 2023

California recently passed a groundbreaking new law aimed at further regulating the data broker industry. California is already one of only three states (along with Oregon and Vermont) that require data brokers—businesses that collect and sell personal information from consumers with whom the business does not have a direct relationship—to meet certain registration requirements.

Under the new law, the regulation of data brokers—including the registration requirements—falls within the purview of the California Privacy Protection Agency (CPPA) and requires data brokers to comply with expanded disclosure and record keeping requirements. Notably, the law also requires the CPPA to make an "accessible deletion mechanism" available to consumers at no cost by January 1, 2026. The tool is intended to act as a single "delete button," allowing consumers to request the deletion of all of their personal information held by registered data brokers within the state.

PUTTING IT INTO PRACTICE: Businesses considered "data brokers" should carefully review the new and expanded requirements and develop a compliance plan, as certain aspects of the law (e.g., the enhanced registry requirements) go into effect as soon as January 31, 2024.

The Comprehensive Privacy Law Deluge: Impact on Loyalty Programs

Posted October 2, 2023

Among the various requirements under US state comprehensive privacy laws, those that relate to loyalty programs may be some of the most confusing. Only three states — California, Colorado and Florida — regulate these programs. How they do this varies, and the level of detail contained in the laws also varies. In California and Florida, the laws' impact on loyalty programs is in how they define "financial incentives." These are times when a company "pays" a consumer for their personal information. This might occur with a straight cash payment. More common though, is optimized pricing or providing a higher quality of services in exchange for getting personal information. For those who offer loyalty programs, depending on how they are operated, they may viewed as be financial incentives under these laws. Colorado's comprehensive privacy law, on the other hand, imposes obligations on companies that operate "bona fide loyalty programs." These are defined as programs where information is processed solely to provide the program's benefits. Benefits must be -like in California- better pricing or quality of services.

What is required if companies engage in these activities?

Notice: Businesses that offer such incentives must provide accessible notice that contain many provisions. Combining the requirements across the three states, the notice must, among other things, clearly explain the material terms of what is being offered, namely what price or service difference is offered (CA, CO, FL). The notice must also give instructions about how to opt-in to the program and how to withdraw from the program (CA, CO, FL). It should also tell people if withdrawing consent will affect participation in the program and if withdrawal of consent will result in program removal, the notice must explain why (CO). It must also explain how the price or service is related to the consumer's data and how the business arrived at that estimate (CA). Finally, it should describe how exercising consumer rights may impact participation in such a program (CO). This notice should be provided at the point of program registration, either directly or in the form of a link to a *specific* section of a privacy notice or a separate notice containing these terms (CA, CO).

Record keeping: California requires that companies keep records of how they calculate the value of consumer's data. The calculation can utilize a variety of metrics if the calculation is reasonable and conducted in good faith.

Withdrawing consumers: In Colorado, if consumers exercise rights (like the right to have their information deleted) such that participation in the program is impossible, a business can withdraw the consumer from the program. The business has 24 hours before discontinuing the loyalty program benefit or membership to let the consumer know. If a consumer requests that their information be deleted and the Loyalty Program does not require the deleted information for participation, though, then consumers should be allowed to stay enrolled. In California, a request to delete from a loyalty program participant would likely need to be examined under the exception to provide a service requested by the consumer or within the context of the ongoing relationship with the consumer.

Opt out signals: Connecticut, Delaware, Montana, and Oregon also briefly mention loyalty programs. Namely, surrounding their requirements on respecting opt-out preference signals. In other words, a signal sent by a platform or technology on behalf of a consumer that communicates the consumer's choice to opt out of sale or sharing. If the signal interferes with consumer's ability to participate in the program, the business should notify the consumer.[1]

PUTTING IT INTO PRACTICE: With all of these laws, companies should keep in mind that they'll first need to determine if the law is applicable to their business (remember some states have higher thresholds than others) and when the laws will take effect. If your business offers perks, discounts, or other incentives to consumers in California and Colorado, then keep those states' requirements in mind, including notice and record keeping.

What Do the CPPA's Draft Regulations on Risk Assessments and Cybersecurity Audits Mean for Companies?

Posted September 14, 2023

The CPPA, the California regulatory body charged with enforcing CCPA, has now issued draft regulations on risk assessments and cybersecurity audits. The draft was released ahead of a public board meeting to discuss those topics (among other things).

As we have written previously, while the CPPA issued regulations to address certain parts of the CPRA amendments to the CCPA, it had not yet drafted all needed regulations. Missing were regulations to address cybersecurity audits, risk assessments, and automated decision-making technology.[1] The CPPA, in releasing these regulations in draft, emphasize their preliminary nature. Its intent, it indicated, was to facilitate public participation. Formal rulemaking has yet to begin.

Although these two are in draft form, they provide companies with an understanding of what the CPPA expects for both risk assessments and cyber audits.

- **Examples of when to conduct a risk assessment**: Under CCPA, companies must conduct a risk assessment if they process consumers' personal information in such a way that it presents significant risk to consumers' privacy or security.[2] As proposed, the draft regulations indicate that a "significant risk" is presented when selling or sharing personal information, processing sensitive information, using technology to monitor consumer behavior, and using automated decision-making technology. The regulations also give specific examples. For example, a business that offers a personal-budgeting application that collects income information that also serves targeted ads for payday loans. This is sharing, under the draft, that would merit a risk assessment.
- **Risk assessment contents:** While CCPA calls for conducting a risk assessment, it does not indicate what content to capture in that assessment. The draft regulations outline content to include, such as, *inter alia*, explaining what is being collected, how it is being used, and the "processing context." Also to include is why the processing is needed, the benefits to the business and consumer, and negative impacts on the consumer. Also to assess are the safeguards the company will put in place to address those negative impacts.
- **Submitting the risk assessment to government authorities:** CCPA specifies that businesses submit risk assessments to the CPPA on a "regular basis." The draft regulations propose an annual submission schedule, and add that they would be submitted to on AG request.
- **Vendor contracts**: While CCPA already provides detailed provisions that must be part of vendor contracts, the draft regulations add one more. Namely, requiring that vendors assist businesses with completing risk assessments (something covered in other states, but not California). This may be another set of obligations for businesses to comply with.
- **Examples of when to conduct a cybersecurity audit**: CCPA mandates that companies must do annual cybersecurity audits if their activities present a "significant risk" to consumer privacy and security. The law indicates already that to assess risk, companies should consider their size and complexity and the nature and scope of processing activities. The draft regulations provide for more detail. To determine if an audit is needed, the regulations outline different monetary, employee, and consumer thresholds. The draft regulations also clarify that the audit can be done by an internal or external team.
- **Cybersecurity audit contents**: CCPA may require an audit, but it doesn't provide much detail in terms of what should be covered. The regulations give more detail. This includes identifying gaps and weaknesses, listing previously-identified gaps and weaknesses, and identifying corrections made. Audits under the regulations would also need to identify a person responsible for completing the audit and qualifications to do so.
- **Audit result submissions**: Under CCPA, those entities that have to conduct a cyber audit must do so annually, but there are no obligations to submit the audit to government authorities. Under the draft regulations, businesses must submit a notice of compliance to the CPPA. (The audit itself does not need to be submitted.) The notice

would be a written certification of compliance -or non-compliance- covering the audit's 12-month period. If the business was not compliant, it needs to identify the areas of noncompliance and either a remediation timeline or confirmation that remediation is complete.

- **Vendor contracts**: CCPA provides detailed provisions for content to include in contracts with vendors who are collecting or processing information on the company's behalf (among other things). The draft regulations contemplate adding provisions to the existing CCPA vendor contract requirements. Namely, requiring that vendors assist businesses with completing cybersecurity audits. This may be another set of obligations for businesses to comply with.

PUTTING IT INTO PRACTICE: While rulemaking in this area is far from complete this draft is an indication of what to expect with final regulations. These drafts do not even represent the beginning of formal rulemaking. The drafts are intended to facilitate public conversations. There is no formal process for submitting comments to these drafts at this time. We will continue to monitor the CPPA's rulemaking activities.

FOOTNOTES
[1] 1798.185(a)(15).
[2] 1798.185(15)

The "First State" Officially Becomes the Thirteenth State with a Comprehensive Data Privacy Law

Posted September 13, 2023

After some delay, Delaware's governor has at last signed into law the thirteenth state comprehensive privacy law. This is the seventh law passed in 2023, joining Iowa, Indiana, Tennessee, Montana, Florida, and Oregon. The law takes effect on January 1, 2025. The bill was passed by Delaware's congress at the end of June and was sent to the governor's office for signature on June 30, 2023. He did not sign it, though, until this week.

Like other states, Delaware's law does not contain a private right of action. The Delaware Department of Justice has sole enforcement power. The law provides a 60-day cure period for violations until December 31, 2025. If a violation is not cured, the Department of Justice may bring an enforcement proceeding under state UDAAP laws. Since Delaware already has an existing online privacy law (though less stringent than this law), entities should consider both in their compliance plans.

Key provisions include:

- **Applicability**. Delaware's privacy law will apply to consumer information and not to employees. The law contains thresholds different to other states. Like Montana, Delaware has lower thresholds. It will apply to businesses that either (1) process personal data of at least 35,000 Delawareans or (2) process personal data of 10,000 state residents *and* receive 20% of gross revenue from sale of personal data. Like California and Oregon, there is no entity-wide exemption for covered entities or business associates under HIPAA. Like Colorado and Oregon, Delaware does not exempt non-profits (except for those dedicated to preventing insurance crime).
- **Privacy notice content**. Under the Delaware law, businesses will need to include the same kind of content in their privacy policies as currently required under other laws. Privacy notices should state what categories of data are being processed and the purpose of processing. The notice must also state whether data is sold or shared. Also required is an explanation of consumer's rights, how to exercise those rights and how to appeal a decision. Like California, Colorado, Connecticut, Montana, and Oregon, Delaware businesses must provide in their privacy notice an email or other online mechanism that allows consumers to contact the business.

- **Consumer rights.** Delaware consumers will have similar consumer rights as other states. This includes the right to access, correct, delete, and port personal information. Delaware will also allow consumers to designate an authorized agent to act on the consumer's behalf. Timing for processing rights is similar to other states: 45 days to respond, with a 45-day extension possible. Like a handful of other states, businesses will need to comply with universal online opt-out mechanisms. The Delaware Department of Justice may publish or reference a list of mechanisms who will have presumptive authority to make such opt-out requests.
- **Targeted advertising, sale, profiling, and sensitive information.** Like other states, Delawareans under the new law will need to be given notice of, and the ability to opt out of, targeted advertising, the sale of their data, and profiling. Businesses will need to perform data protection assessments if they engage in any of those activities. Importantly, only businesses that control or process data for *100,000 consumers* must conduct any needed data protection assessments. This is a higher threshold than the applicability for the rest of the law which impacts businesses that control or process the data of 35,000 Delaware consumers. For sensitive information, consent must be obtained before processing. (This is the same as Colorado, Connecticut, Indiana, Montana, Oregon, Tennessee, Texas, and Virginia). The definition of sensitive information parallels other states**. It also, though, includes** "pregnancy" as a mental or physical health condition and (like Oregon) "transgender/non-binary status."
- **Vendors. Vendor contracts for data processing require familiar provisions.** The agreements must provide instruction on how to process information and what type of information will be processed. Vendor contracts will also require data confidentiality and allow companies to assess vendors' compliance (vendors must cooperate with those assessments).

PUTTING IT INTO PRACTICE: By now, many of these state privacy laws may be feeling familiar. However, privacy remains a space where "one-size-fits-all" policies still won't hit the mark. Companies should continue to take a flexible approach to their privacy program in order to customize where necessary. As more states follow suit, differences will become harder to accommodate with one uniform policy or practice.

The Comprehensive Privacy Law Deluge: Record-Keeping and Related Requirements

Posted September 11, 2023

It's been a busy summer for US state privacy laws, and companies now need to keep track of a growing list of requirements from these laws. These include many we have written about in the past, including notice, vendor contract provisions, and offering consumers rights and choices. The laws also impose certain record keeping requirements, which we discuss here.

But first, as a reminder, the laws have rolling effective dates. Only California, Virginia, Colorado, Connecticut are in effect. The others go into effect as follows:

- **December 31, 2023:** Utah
- **July 1, 2024:** Florida, Oregon, and Texas
- **October 1, 2024:** Montana
- **January 1, 2025**: Delaware and Iowa
- **July 1, 2025**: Tennessee
- **January 1, 2026**: Indiana

The laws impose record keeping requirements on companies to whom the laws apply (for more about the laws' applicability read our prior post). These requirements overlap in many respects. They include:

- **Rights requests:** Records of rights requests must be kept for 24 months (CA, CO), and in readable and secure format. (CO). Each record must include the date and nature of the consumer request and include any business responses or denials (CA, CO).
- **Deletion requests:** Companies must also keep records of deletion requests and the minimum amount of data necessary to ensure that the consumer's personal data remains deleted and not used for any other purpose (CA, CO, CT, DE, FL, IN, MT, OR, TN, TX, VA).
- **Metrics:** Companies must compile annual metrics for the number of consumer requests and opt-out requests they've received. (CA) As part of this, companies must track how many requests were processed or denied, and whether this was done in whole or in part (CA).
- **Data limitation:** Information kept for record-keeping purposes should not be used for any other purpose (CA, CO).
- **Assessments:** If engaging in targeted advertising, selling data, engaging in profiling, or processing sensitive data, companies must conduct data protection assessments under all states' laws except those of Iowa and Utah. We discuss these requirements in more detail in our recent webinar. (And keep in mind that California is still working on regulations for these assessments.) Companies should keep in mind that these assessments also carry record keeping requirements. Namely:
- Document every DPA conducted (CA, CO, CT, DE, FL, IN, MT, OR, TN, TX, VA).
- DPAs must be kept for three (CO) or five years (OR)

PUTTING IT INTO PRACTICE: As the summer comes to a close, now is a good time to revisit your privacy programs. Keeping in mind the various requirements under the laws is getting more complex. Having a scalable program that addresses record keeping and other requirements can make compliance easier.

Texas' SCOPE Act Puts Focus on Social Media and Minors

Posted September 5, 2023

Texas has joined Arkansas and Utah as the third state to impose requirements on social media accounts for those under 18. Namely, with the Securing Children Online through Parental Empowerment Act ("SCOPE Act"), Texas will place requirements on "digital service providers." The law goes into effect September 1, 2024. It does not provide for a private right of action. Instead, enforcement will be by the Texas attorney general.

Under the law, a digital service provider is not only a "website, application, software, or program" but also an entity that determines the "purpose and means of processing" users' personal information. Unlike the Utah law, there is no user or monetary threshold. The law does have some exemptions. Notably for most, sites that generate content rather than serving as a platform for *others* to post content and user content (like comments and chat) are incidental, are exempt. Exemptions also exist for small businesses, higher education institutions, and entities subject to HIPAA or GLBA.

If a company is a covered digital service provider, it must:

- **Conduct age verification**: When registering for an account, digital service providers must ask users their age. If a user indicates that they are under 18, they cannot be allowed to "age up." The provider must then follow the laws' information limitation, content restrictions, and parental controls requirements.

- **Limit information collected from minors**: Providers can only collect information that is reasonably necessary to provide the digital services. Additionally, minors' geolocation information cannot be shared or disclosed.
- **Content restrictions:** Providers will need to put in place a strategy to limit minors' access to content that can be harmful to them. By way of example, this includes information about suicide or bullying content. The provider's strategy must include, among other things, keeping a list of harmful material and filtering it from minors. Content filtering will need to include both technical measures and human-review. Relatedly, service providers must make commercially reasonable efforts to stop third party advertisers from targeting minors with ads for products and services that are "unlawful for a minor" in the state of Texas.
- **Parental involvement**: Digital service providers must give parents the ability to "participate" in their children's accounts. To do this, the provider must first verify the person as the parent. Once verified, providers will need to allow parents the ability to supervise the account. This includes accessing and controlling their children's account settings. Parents also need to be able to limit how long their children use the service and restrict children's ability to make purchases.[1] Like Arkansas' law (but unlike Utah) the SCOPE Act is silent on whether parents must be provided with access to a minor's content and messages.

PUTTING IT INTO PRACTICE: While this law has narrow applicability, it signals a trend at a state level to regulate social media consumption by minors. We anticipate that this trend will continue in other states.

FOOTNOTES
[1] Sec. 509.054(b).

State Comprehensive Privacy Laws – Beaver State Makes a Dozen

Posted July 21, 2023

Oregon's governor has now signed into law the state's comprehensive privacy law. Meaning, there are now 12 states with these laws, six of which were passed just this year (others passed in 2023 were Iowa, Indiana, Tennessee, Montana, and Florida). Oregon's law will go into effect on July 1, 2024, with limited parts not effective until January 1, 2026.

Like other states, there is no private right of action. Instead, the Oregon Attorney General is to enforce the law. Companies will have a 30-day cure period, which cure period sunsets on January 1, 2026. The law provides for civil penalties of up to $7,500.

Key provisions include:

- **Applicability**. Like all states except California, the law covers consumer information. It does not apply to employee or job applicant information. The law contains a long list of exemptions, as in other states. Notably, like California, personal information processed under HIPAA is exempt. On the other hand, like other states, financial institutions more broadly are exempt as well. The law contains thresholds similar to other states. Namely, it is applicable to businesses that either (1) process personal data of at least 100,000 Oregonians or (2) process personal data of 25,000 state residents *and* receive 25% of gross revenue from sale of personal information.
- **Privacy notice content**. Under the Oregon law, businesses will need to include the same kind of content in their privacy policies as currently required under other laws. This includes listing what categories of data being processed and the purpose of processing. Policies also need to include what is sold or shared and explain rights and how to exercise them. Business that either serve target advertising or profiling (that creates consumer risk) must disclose this in the privacy notice and give consumers a way to opt-out.
- **Consumer rights.** Oregon consumers will have similar consumer rights as other states beginning July 1, 2024. This includes the right to access, correct, delete, and port personal information. Oregon consumers can also request

a list of the *specific* third parties to whom the business has disclosed their information**.** That said, the company does not *have* to give this information. Timing for processing rights is similar to other states: 45 days to respond, with a 45-day extension possible. Beginning January 1, 2026, companies will also be required to respect opt-out preference signals (similar to the requirement in California, Colorado, Connecticut, and Montana).

- **Targeted advertising, sale, profiling, and sensitive information.** Like other states, can opt out of targeted advertising, the sale of their data, and profiling. Businesses must perform data protection assessments if they engage in targeted advertising or profiling that creates risks to consumers.[1] They must keep data protection assessment records for five years. For sensitive information, consent must be obtained before processing. (This is the same as Colorado, Connecticut, Indiana, Montana, Tennessee, Texas, and Virginia). The definition of sensitive information mirrors other states (race and religious beliefs, etc.). It also, though, includes "status as a victim of crime" and "transgender/non-binary status."
- **Vendors.** As under other states' laws, Oregon will require contracts with vendors who process consumer personal data. Those agreements must include provisions that will sound similar to those familiar with other comprehensive privacy laws. They include telling the vendor how to use information and what information will be processed. The contracts will also need to require data confidentiality and provide companies with the ability to assess vendors' compliance (vendors must cooperate with those assessments).

PUTTING IT INTO PRACTICE: This latest privacy state "comprehensive" privacy law suggests that other states may not be far behind. In light of this, companies may want to take an adaptive approach to their privacy program. Included in this would be how to easily assess if the laws apply; and updating consumer notices, ways of offering choices and rights, assessing obligations if profiling, as well as updating vendor contracts.

Impact of the Last Minute CCPA Enforcement Delay

Posted July 10, 2023

A California court recently issued a ruling delaying the CPPA's ability to enforce the most recent CCPA regulations until March 29, 2024. This does not delay enforcement of the CCPA statute or existing regulations.

What happened?

The CPRA -which went into effect January 1, 2023- modified California's existing privacy law: CCPA. The CPRA amendment required the California regulatory authority (the CPPA) to adopt final regulations on a set of issues by July 1, 2022. (Other issues had a longer time frame.) The regulations due on July 1 were not adopted on time: they were only adopted March 29, 2023. Concerned about the lack of time to understand and implement the requirements in the regulations, the California Chamber of Commerce recently sought an injunction banning the enforcement of those regulations. They argued that enforcement should not begin until 12 months after the adoption of the regulations. The court agreed, noting that under the statute as amended, the date set for enforcement was drafted using non-mandatory language ("**shall not** commence until July 1, 2023" (emphasis added)). Meaning that it did not *have* to begin on that date. But the date by which regulations were to be adopted was mandatory ("the timeline for adopting final regulations . . . **shall** be July 1, 2022" (emphasis added)). Read together, the court found, the intent was that the regulations were to be enforced 12 months after their adoption. In other words, CPRA essentially called for a 12 month grace period between the date of the regulations and the date of enforcement. As such, the court held, the enforcement date of the regulation should be pushed back one year from when the regulations were issued to March 29, 2024.

What does this mean?

The CPRA amendment to CCPA became effective January 1, 2023. For now, even though the new requirements are in effect, the CPPA cannot under this order bring enforcements except for violations of the prior regulations or

the statute. The ruling does not impact the substance of the CPRA amendments to the CCPA. As a reminder, the regulations that have been adopted do not cover all of the CCPA (as amended)'s requirements. Looking forward, the CPPA still needs to adopt regulations for automatic decision making, risk assessments and cybersecurity audits. It will be holding an open hearing to discuss these and other issues on July 14.

PUTTING IT INTO PRACTICE: Companies can use this additional time to evaluate their CPRA regulation compliance efforts and build a sustainable privacy program agile to adapt to the flurry of other state laws that have been passed.

The Comprehensive Privacy Law Deluge: Approaching Notice Obligations

Posted July 6, 2023

When thinking about privacy notice obligations, companies often -incorrectly- leap to the wording in their privacy policies. The new comprehensive state privacy laws are a reminder that notice obligations are a bit broader than mere privacy policies. To the extent that these laws apply to your organization (see our prior applicability post) there are some notice-related obligations to keep in mind.

For many companies, the biggest "change" is that these laws contain obligations to provide individuals with notice (a privacy policy) not just online -as existed under prior state online privacy laws (California, Delaware and Nevada)- but at any point that personal information is being collected. In other words, in offline or by phone. Some, like California, contain details about how to provide offline notice. Previously, other than state laws requiring privacy notices, there were only sector or activity-specific laws that contained the requirement. Companies nevertheless had them because of FTC guidance and expectation. Companies also had them to mitigate and minimize risk that consumers might expect information was treated in a certain way. The privacy policy was a tool to explain the company's actual practices.

In terms of content, for entities that already comply with GDPR or CCPA, the requirements are not significantly different. Thus if your organization has already updated its privacy policy to address CPRA requirements, little additional content will be needed to address the newer state laws. At a high level, content required is as follows (refer to our effective date post for timelines, which may impact when an organization decides to amend its policy to address these laws):

	CA	CO	CT	FL	IA	IN	MT	TN	TX	UT	VA
Categories of personal information and purposes of processing	x	x	x	x	x	x	x	x	x	x	x
If sensitive information will be processed	x	x		x					x		
If information will be shared and categories of those third parties	x	x	x	x	x	x	x	x	x	x	x
Consumers' rights, and how to exercise them	x	x	x	x	x	x	x	x	x	x	x
How to appeal a decision	x	x	x	x	x	x	x	x	x		x
How to opt out of certain processing	x	x									
Date policy was last updated (CalOPPA also requires effective date)	x	x									
Contact information for questions or concerns	x	x	x				x				

This list is not exhaustive, and many states have specific -and fairly complex- requirements about what these notices look like and content to include in the categories listed above.

PUTTING IT INTO PRACTICE: As we move past Colorado and Connecticut's effective dates, presumably organizations have already reviewed and updated their privacy policies. However as more and more states put "comprehensive" privacy laws in place there will be a need to continue to review those statements. Internal procedures for regular review of privacy policies can be a helpful mechanism to ensure the document not only keeps up with the regulatory requirements, but also remains factually accurate.

The Comprehensive Privacy Law Deluge: Updating Vendor Contracts

Posted June 27, 2023

Of the many worries on privacy compliance teams' lists as we face the onslaught of state "general" privacy laws are the impacts they have on vendor contracts. Fortunately for those who have already had to deal with contracts with vendors (service providers, processors) in California or EU's GDPR, the impact should be fairly minimal.

In Colorado, Connecticut, Montana, Tennessee, Texas, Utah and Virginia, contracts are required with entities who process or collect information for the business. What do these laws, collectively, require be in the contracts? The following is a quick reminder:

- Instruct on how data is to be processed, and the nature and purpose of the processing. (In California, that processing will be limited to the specific purpose listed in the contract if the entity is a "service provider." In Colorado, Connecticut, Montana, Texas, Tennessee, Utah and Virginia, that processing will be limited to the specific purpose listed in the contract if the entity is a "processor"). (CA, CO, CT, IN, MT, TN, TX, UT, VA)
- Indicate the type of personal data to be processed and duration of the processing. (CA, CO, CT, IN, MT, TN, TX, UT, VA)
- Obligate confidentiality and that information be returned upon termination. (CA, CO, CT, IN, MT, TN, TX, UT, VA)
- Obligate appropriate technical and organizational measures to protect the data. (CA, CO, CT, IN, MT, TN, TX, UT, VA)
- Give proof of ongoing legal compliance. (And in California, compliance specifically with CCPA). (CA, CO, CT, IN, MT, TN, TX, UT, VA)
- Cooperate with assessments and audits. (CA, CO, CT, IN, MT, TX, UT, VA)
- Obtain written permission before engaging subcontractors (CO, CT, IA).

PUTTING IT INTO PRACTICE: As we quickly approach July 1, and companies are thinking about the effective dates of Colorado and Connecticut, now is a good time to review contracts and assess if they need to be updated for future state laws.

The Comprehensive Privacy Law Deluge: What to Do About "Profiling"

Posted June 26, 2023

With a little less than a week before the next US state "comprehensive" privacy laws (Colorado and Connecticut) go into effect, many are reviewing existing practices. One that keeps coming up is the concept of "profiling." As a reminder, we now have 11 states with comprehensive privacy laws: California, Colorado, Connecticut, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah, and Virginia.

Profiling has a very specific definition under these states' laws (with the exception of Indiana and Utah), following similar themes:

State	Definition	Opt-Out Required
California	automated processing of personal information…to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.	x [regulations on mechanism pending]
Colorado, Connecticut	automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.	x
Florida, Indiana, Montana	solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, [health records, Indiana] personal preferences, interests, reliability, behavior, location, or movements.	x
Tennessee, Texas	solely automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.	x
Virginia	automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.	x

The states regulate profiling if it produces a legal or similarly significant effect. Additionally, if a company is engaging in profiling in California, Colorado, Connecticut, Florida, Indiana, Montana, Tennessee, Texas and Virginia then an individual needs to be able to opt out of that activity (Iowa and Utah do not contain specific provisions about profiling in their laws).

In addition to providing choices around profiling, under many state laws a risk assessment must be conducted, Namely, in Colorado, Connecticut, Florida, Indiana, Montana, Tennessee, Texas and Virginia, if there is a risk of:

- Unfair or deceptive treatment
- Financial, physical or reputational injury
- Physical or other intrusion upon the solitude or seclusion
- Other substantial injury to consumer

Colorado, under its regulations, outlines specific steps that a company must take for a risk assessment. This includes engaging in a "genuine, thoughtful analysis" of the processing activity. The assessment must also involve all stakeholders. The assessment itself must, *inter alia* (1) summarize the processing activity, (2) list categories of personal information to be processed, (3) the context of processing activity, (4) nature of processing, (5) sources of information, and (6) names of recipients.

PUTTING IT INTO PRACTICE: If your organization is engaging in profiling that will have a "significant legal or similar impact" on individuals, keep in mind the choice and assessment obligations under the comprehensive privacy laws. Colorado's regulations provide detail that can be helpful in determining how to conduct a data protection assessment.

The Lone Star State Joins the Privacy Law Deluge: Another Governor Signs

Posted June 19, 2023

Texas has now become the 11th state, following Florida, to have a "comprehensive" privacy law. HB 4 was signed by the governor on June 18, 2023. This caps off a busy spring for state lawmakers not only in Texas, but Florida, Iowa, Indiana, Tennessee, and Montana. The law goes into effect on July 1, 2024 (the ability for agents to submit rights requests is not effective until January 1, 2025 however). For a round-up of state laws' effective dates, visit here.

Like other states, there is no private right of action. The Texas AG is required under the law to maintain an online portal where consumers can lodge complaints. Companies will have 30 days to cure potential violations (provided they meet certain requirements, like providing supporting documentation showing the violation was cured). The law provides for civil penalties of up to $7,500 per violation.

Key provisions include:

- **Applicability.** The law will apply to those who do business in Texas (or sell products/services to Texans). Like others, it covers consumer information but exempts health care providers, financial institutions, and several others. There are no thresholds under the law, but "small businesses" have fewer obligations. Namely, they may not sell sensitive personal information without first getting consent. Sensitive information includes not only racial or ethnic information, mental diagnosis and biometric information, but also children's information and precise geolocation information.
- **Data minimization.** Like Colorado, Connecticut, and Montana, businesses will need to limit their collection of personal data to what is adequate, relevant, and reasonably necessary for the purposes it was collected.
- **Consumer rights.** Texans will have the right to access, correct, and delete information, rights that exist under other state laws. The law also gives a right of data portability. Like California, consumers in Texas must have two or more methods for submitting rights requests. Also like most other states, companies will need to respond to these requests within 45 days, with an additional 45 day extension available.
- **Targeted advertising, selling and profiling.** Like other states, consumers will need to be able to opt-out of targeted advertising, sale of personal data, and profiling. Also, if a company is going to engage in profiling, sale of personal data, or targeted advertising in a way that could create risks to consumer rights a data protection assessment must be conducted. "Sale" is defined similarly to California, Connecticut, Colorado, Florida, Montana: it includes both monetary consideration and "other valuable consideration."
- **Privacy notice content**. Privacy notices will not likely need to change much. The law will require that they outline the categories of data being processed, the purpose, categories of data being sold or shared, and provide consumers with information about exercising their consumer rights. Like California, Texas will also requires a clear, conspicuous statement if the company sells sensitive or biometric data. The language to use is proscribed, namely: "we may sell your sensitive personal data" or "we may sell your biometric personal data."

- **Sensitive data**. Before processing sensitive data, companies must obtain consumer consent (as in Colorado, Connecticut, Montana, and Virginia).

PUTTING IT INTO PRACTICE: This latest US state law is (another!) reminder for companies to review their information collection and use practices, as well as their third party contracts. Having a scalable privacy program will make dealing with these laws easier, as they continue to go into effect over the coming months and years.

The Comprehensive Privacy Law Deluge: Approaching Choice and Rights

Posted June 14, 2023

Companies may want to review their consumer rights processes as we approach July 1. This is the date of enforcement for those parts of CCPA modified by CPRA. It is also the effective date of two more state privacy laws: Colorado and Connecticut. Neither law is substantively much different from California and Virginia, but if an entity was not subject to those laws it may be subject to those in these two additional states. Let's recap the requirements around choice and individual rights:

- Companies in all four states need to give consumers the ability to opt-out of the sale of personal information, targeted advertising and profiling that produces a "legal or similarly significant" impact. (California also imposes requirements for opting out of the "sharing" of personal information).
- In California, consumers must be given the opportunity to opt out of the processing of sensitive information. (Consent (an opt-in) is needed in Virginia, Colorado (with some exceptions) and Connecticut).
- Consumers must be given the right to access, correct and have information deleted in all four states.
    - In all, certain exceptions apply, like if it involves a disproportionate effort (California), is manifestly unfounded, excessive or repetitive (California, Colorado, Connecticut, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah, Virginia), or technically infeasible or impossible (California, Colorado, Iowa, Montana, Utah).
    - Similar requirements -and exceptions- will apply in future jurisdictions as well (however Utah and Iowa will not give a correction right, and Indiana's correction right is limited to that which the person gave the company).
    - Companies have 45 days to respond to rights requests in all states (except Iowa, where it will be 90 days and Florida, where it will be 60 days), with all allowing companies to extend that time frame by 45 days if "reasonably necessary" (Florida's extension, however, will be 15 days).
    - Additionally, from a process standpoint, all states contemplate verifying consumer identities as part of the rights granting process.
    - Consumers can exercise rights twice within a 12 month period in California, Florida, Iowa, Tennessee, Texas, and Virginia, but only once in Colorado, Connecticut, Indiana, Montana, and Utah.

PUTTING IT INTO PRACTICE: As we approach the July 1 effective date for Colorado and Connecticut's privacy laws, now may be an appropriate time to review your current rights response practices, especially if you already receive a high number of requests.

Another Governor Signs: Florida Privacy Law Will be Effective July 2024

Posted June 12, 2023

Florida has become the latest state to enact a comprehensive privacy law this year when SB 262 was signed by Governor DeSantis last week. It combines some new, and some familiar, provisions. It has also passed a child privacy law, similar to parts of California's Age Appropriate Design Act, going into effect July 1, 2024.

The Florida Digital Bill of Rights Law

Entities that will be covered by this law are very limited. The law will apply only to those who earn $1 billion in global gross annual revenues *and* either (1) receive 50% of gross annual revenue from the sale of online ads, (2) operate cloud-connected smart speakers with virtual assistants, *or* (3) have an app store or digital distribution platform that has at least 250,000 apps available for download.

Like other states, the Florida law applies to consumer information, and provides many exemptions. This includes financial institutions subject to GLBA, HIPAA covered entities and business associates, non-profits, and higher education institutions. Aside from entity exemptions, there are also *data* exemptions. For example, information collected as part of human subject research.

Violations carry high possible penalties: $50,000 per violation. The AG has discretion on whether to offer companies a 45 cure period. The AG must adopt rules about authenticated consumer requests, enforcement, data security, and authorized agents. The law has no private right of action.

The requirements for the limited number of companies to whom this Florida law applies are similar to those in other states. This includes giving consumers rights of access, correction and deletion. Consumers can also opt out of targeted advertising and profiling that could create significant legal impacts. An opt-in is required for processing sensitive information. The law provides for data minimization and content requirements in privacy notices.

Given the narrow scope of companies to which the law applies, it does have some unique features not seen elsewhere. These include, among other things:

1. Allowing consumers to opt out of the collection of personal data from voice recognition or facial recognition technology features.
2. Controllers that operate a search engine must publish an up-to-date plain language description of how search results are ranked, including the prioritization or de-prioritization of political partisanship or political ideology in search results.
3. Companies must establish data retention schedules and, in the absence of a schedule, must dispose of consumer data two years after the last interaction.

Florida's New Children's Privacy Law for Social Media Platforms

As part of the bill, Florida also passed a new law that will apply to operators of social media platforms who have platforms that are accessed by Florida children. These companies will have restrictions similar to California's Age Appropriate Design Act. (But by contrast, the California law applies more broadly than just to social media platforms and includes those who provide online products, services or features to children.) This Florida law also follows Utah laws from earlier this year (which go into effect in March 2024). Those, as we have written, apply to social media companies with more than five million account holders worldwide and are thus narrower in scope than the new Florida law.

Restrictions under Florida's law include not processing children's data if substantial harm will result. Social media platforms also cannot profile a child unless necessary, and will not be able to use a child's information for any reason other than the stated purpose of collecting the information.

As in California, children are defined as those under 18. Violations carry high possible penalties ($50,000 per violation), but companies have a 45 cure period. The law provides for potential rulemaking, and has no private right of action.

PUTTING IT INTO PRACTICE: Florida has now joined the growing number of states with comprehensive privacy laws (currently, ten in total), although its requirements will likely not apply to most entities. It also joins California in targeting legislation towards social media platforms, something we may see in more states in the coming months.

The Comprehensive US Privacy Law Deluge: Which US Privacy Laws Apply to Your Company?

Posted May 30, 2023

The US has what appears to be a never-ending list of comprehensive privacy laws, but do they all apply to your organization? Not necessarily.

Let's recap. Since we last wrote at the beginning of the month about preparing for these laws, some things have changed. Eight comprehensive privacy laws have now been passed (California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Utah, and Virginia) and one more is expected to pass soon (Florida). Two are already in effect (California and Virginia) and two will go into effect on July 1, 2023 (Colorado and Connecticut).

Which of these laws should your organization worry about? First, as a baseline, your organization must be doing business in that state. Second, only California applies beyond consumers (to employees and employees of third parties). Third, many have revenue triggers: California ($25 million), Florida ($1 billion), Tennessee ($25 million), and Utah ($25 million). The latter three apply these amounts as a baseline before the law applies. Finally, the laws apply only if the company processes information about a certain number of individuals in the state (175,000 in Tennessee; 100,000 in California, Colorado, Indiana, Utah and Virginia; 50,000 in Montana) or sell information about certain threshold number of individuals (or engage in another covered activity, in particular Florida). The applicability triggers for each state are outlined below:

State	Covered Individuals	Threshold, Revenue	Threshold, Number of residents
California	Consumers Employees 3rd parties' employees	gross annual revenues above $25 million *or*	100,000 consumer information bought, sold, or shared *or* 50%+ of annual revenue from selling personal information
Colorado	Consumers	n/a	100,000 consumer information processed *or* 25,000 residents' information processed or derives revenue and gets discount on the price of goods or services from the sale of personal data
Connecticut	Consumers	n/a	100,000 consumer information processed *or* 25,000 consumers' information processed and 25%+ of annual revenue from selling personal information
Florida	Consumers	$1 billion in gross revenue *and*	50% of revenues from online advertisement sales *or* operate a consumer smart speaker or voice command service with cloud-based, voice-activated virtual assistance *or* operate an app store with at least 250,000 apps

State	Covered Individuals	Threshold, Revenue	Threshold, Number of residents
Indiana	Consumers	n/a	100,000 consumer information processed *or* 25,000 consumers' information processed and 50%+ of annual revenue from selling personal information
Iowa	Consumers	n/a	100,000 consumer information processed *or* 25,000 consumers' information processed and 50%+ of annual revenue from selling personal information
Montana	Consumers	n/a	50,000 consumers' information processed *or* 25,000 consumers' information processed and 25%+ of annual revenue from selling personal information
Tennessee	Consumers	$25 million+ in gross annual revenues *and*	175,000 residents information processed *or* 25,000 processed annually and 50%+ of gross revenue from sale of personal information
Utah	Consumers	$25 million+ in gross annual revenues *and*	100,000 consumer information processed *or* 25,000 processed annually and 50%+ of gross revenue from sale of personal information
Virginia	Consumers	n/a	100,000 consumer information processed *or* 25,000 processed annually and 50%+ of gross revenue from sale of personal information

Even if your organization meets these thresholds, the law may still not apply, or not in all cases. All laws except California exempt entities that are in regulated industries like health care and financial services. California, on the other hand, exempts only the *information* that is subject to the regulations of these industries (i.e., GLBA, HIPAA). Outlined below are (some of) the many exemptions and states in which they exist:

Exemption	CA	CO	CT	FL	IN	IA	MT	TN	UT	VA
Health care companies		x	x	x	x	x	x	x	x	x
Financial services entities		x	x	x	x	x	x	x	x	x
State or government agencies			x	x	x		x	x	x	x

Native tribes									x	
Non profits	x		x	x	x	x	x	x	x	x
Higher education institutions	x	x	x	x	x	x	x	x	x	x
Public utilities		x			x					
Air carriers		x							x	
HIPAA-regulated information	x	x	x	x	x	x	x	x	x	x
GLBA-regulated information	x	x	x	x	x	x	x	x	x	x
FERPA-regulated information		x	x	x	x	x	x	x	x	x
Drivers Privacy Protection Act-regulated information	x	x	x	x	x	x	x	x	x	x
Farm Credit Act-regulated information	x		x	x	x	x	x	x	x	x
Information maintained for employment records		x								
Information collected when a third party benefit provider	x		x	x	x	x	x	x		x

PUTTING IT INTO PRACTICE: As you review the upcoming law's requirements, it is helpful to keep in mind their applicability thresholds – and their exceptions. While we may see more states pass similar comprehensive laws in the coming months, their applicability thresholds may be a similar patchwork.

Montana Governor Signs Big Sky's Privacy Law

Posted May 23, 2023

Montana now joins a growing list of states to have a comprehensive privacy law. The law was signed by the governor on May 19, 2023 and will go into effect October 24, 2024. This is before some Iowa (effective January 1, 2025) and Indiana (effective January 1, 2026), which pre-dated it in passage.

The law will apply to those that do business in Montana and either: (1) control or process personal data of at least 50,000 state residents; or (2) derive over 25% of gross revenue from the sale of personal data *and* control or process personal data of 25,000 or more state residents. As with other laws (outside of California), Montana has a long list of exemptions, including entities covered by HIPAA or GLBA. It also does not cover employee information. Key provisions include:

- **Notice**. Like other state laws, a company must tell consumers the categories of data it processes, the purpose, categories of data being sold or shared, and provide consumers with information about exercising their consumer rights.
- **Consumer Rights.** Montana provides for similar rights that we've seen under other state privacy laws. Namely rights of access, correction, deletion, and portability. Like the new Tennessee law, companies need only provide portability to information the consumer provided. Consumers can have agents make rights requests on their behalf. Companies must respond to these rights requests within 45 days (extendable by 45 days). Companies also have to let consumers opt out of sale of personal data, targeted advertising and profiling. "Sale" includes "other valuable consideration" and not just a monetary exchange (as is the case in California, Connecticut, and Tennessee). Montana will also require that companies recognize opt-out preference signals (mirroring California, Colorado, and Connecticut).

- **Sensitive Personal Data.** Businesses in Montana must obtain consent before processing consumer's sensitive information, just like they do in Colorado, Connecticut, and Virginia. Sensitive information is defined as data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, citizenship or immigration status. It also includes genetic or biometric data, precise geolocation information, and information about children.
- **Contracts**. Like most other states, Montana will require contractual obligations that ensure privacy and technical safeguards are in place to protect consumer information.
- **Enforcement**. There is no private right of action under the law or specific statutory damages. Before the attorney general can initiate an action, it must give companies written notice and 60 days to cure the violation. This cure period will sunsets April 1, 2026 (the sunsetting provision is similar to that of Colorado, but unlike Indiana, where the cure period does not sunset).

PUTTING IT INTO PRACTICE: Companies now have another state's law to add to their list for provision of privacy rights and to address from a contractual standpoint. The threshold for applicability is lower in Montana than others, something to keep in mind prior to the October 2024 effective date.

Another Governor Signs: Tennessee Volunteers to Join the Privacy Patchwork

Posted May 15, 2023

The Tennessee governor has signed Tennessee's comprehensive privacy law, which as we have indicated will go into effect July 1, 2025. As initially proposed, the law would have been effective July 1, 2024, and would have required companies have a written privacy program compliant with NIST's privacy framework. That obligation -which is unlike that which exists in any other state's general privacy law- has been toned down in the final version signed by the governor.

Tennessee, like other states, has no right of action for violations of the law, but does provide statutory penalties of up to $7,500 per violation. Before initiating an enforcement action, the attorney general must first give companies written notice and 60 days to cure the violation. Tennessee's law for the most part merely expands existing comprehensive law obligations onto their states' citizens. There are two notable exceptions:

- **NIST – An Affirmative Defense**. Companies who violate the Tennessee law will have an affirmative defense if they have a "written privacy policy" that "reasonably conforms" with the NIST privacy framework or if they otherwise have documented policies and procedures "designed to safeguard consumer privacy." While a written privacy program is no longer required under the law as finally signed, it mirrors other states in requiring that companies have "reasonable" administrative and technical practices to protect the "confidentiality, integrity and accessibility" of personal information (47-18-3204(a)(3)).
- **Applicability:** The law has higher thresholds than many of the other states. First, it applies only to those who do business in the state and have revenues of over $25,000,000. In addition, for the law to apply, companies *must also* either (1) control or process information of 175,000 or more state residents during a calendar year *or* (2) control or process personal information of 25,000 or more state residents and get over 50% of gross revenue from the sale of personal information. As with other states, the law does not apply to those regulated by HIPAA or GLBA. It also does not apply to non-profit entities or "institutions of higher education," among other exceptions.

Tennessee's law otherwise fairly closely mirrors that in other states. Namely:

- **Notice**. As in other states, companies will need a privacy policy that outline the categories of data being processed, the purpose, categories of data being sold or shared, and provide consumers with information about exercising their consumer rights.

- **Consumer Rights.** Tennessee will require, like others, that companies give state residents rights of access, correction, deletion, and portability (within 45 days, extendable by 45 additional days). Companies need only provide portability to information the consumer provided. As is the case elsewhere, companies also have to let consumers opt out of sale, targeted advertising and profiling (the last of which if it has "legal or other similarly significant" effects). Tennessee has a broad impact assessment requirement, applying to entities that engage not only in selling or profiling, but also targeted advertising. Tennessee follows California and Connecticut, with "sale" including both a monetary exchange, as well as an exchange of personal data for "other valuable consideration." Disclosures to affiliates or as part of a sale or merger are expressly excluded from the definition of sale.
- **Data Minimization**. Like Colorado and Connecticut, companies will need to limit their collection and processing to information that is reasonably necessary and proportionate to the purpose for which it was collected.
- **Sensitive Personal Data.** Businesses in Tennessee -as with Colorado, Connecticut and Virginia- must obtain consent before processing consumer's sensitive information. Sensitive data includes not only elements like race, ethnicity, religion, sexual orientation, or medical diagnoses, but also biometric information and precise geolocation.
- **Contracts**. As we reported for Indiana, TIPA will require contractual obligations that are very similar to other US state comprehensive privacy laws.

PUTTING IT INTO PRACTICE: While mostly following other states, Tennessee's privacy program provisions serve as a reminder to think about documenting and ensuring compliance with privacy laws more generally. While many may find that -even when the law does go into effect in 2025- they do not meet its thresholds, it is possible that other states may begin to mirror these new provisions.

Preparing for the US Comprehensive Privacy Law Deluge

Posted May 11, 2023

With January well in the rear view mirror, companies are setting their privacy compliance sights on the next two laws to come into effect on July 1, 2023: Colorado and Connecticut. Knowing, of course, that Utah (December 31, 2023) is not far behind. To say nothing of five more on the horizon, in order of effective date:

1. Montana, anticipated to be passed into law soon, and effective October 1, 2024;
2. Florida, anticipated to be passed soon, and effective July 1, 2024;
3. Iowa already passed and effective January 1, 2025;
4. Tennessee, anticipated to be passed into law soon, and effective July 1, 2025; and
5. Indiana, already passed, and effective January 1, 2026.

Those who have previously assessed their organization's compliance with California, Virginia, or GDPR will find that these laws do not significantly add to the mix of obligations. Nevertheless, tracking the differences in applicability, notice/choice/rights obligations, contractual clauses, to say nothing of their varying approaches to sensitive data, sales, and financial incentives can be headache inducing. To help minimize stress (and confusion!) we will be posting articles in the coming weeks outlining the core similarities and differences between these different laws. In the meantime, the following table summarizes where we are at today:

State	Passed?	Effective Date
California	Yes	January 1, 2020 (updated by CPRA, January 1, 2023)
Virginia	Yes	January 1, 2023

Colorado	Yes	July 1, 2023
Connecticut	Yes	July 1, 2023
Montana	Pending	October 1, 2024
Florida	Pending	July 1, 2024
Utah	Yes	December 31, 2023
Iowa	Yes	January 1, 2025
Tennessee	Pending	July 1, 2025
Indiana	Yes	January 1, 2026

PUTTING IT INTO PRACTICE: Companies operating in the US now have a growing patchwork of privacy laws to contend with. Not only do they need to keep track of obligations under activity (email, texting), industry (financial services, healthcare) or type of individual (children, employees) privacy laws, but they also have a growing list of "GDPR-lite" laws to contend with. Developing a "substance" specific framework that groups together obligations by type (notice, choice, rights) can be a helpful approach when contending with this growing landscape of laws.

Governor Signs: Hoosier State Adds to the US Privacy Patchwork

Posted May 3, 2023

Indiana has now become the seventh US state to enact a comprehensive privacy law after Senate Bill 5 ("SB5") was signed by the governor on May 1, 2023. The new law will go into effect January 1, 2026, and is almost identical to recent comprehensive privacy laws in other states.

The law will apply to those that do business in Indiana and either: (1) control or process personal data of at least 100,000 Hoosiers; or (2) derive over 50% of gross revenue from the sale of personal data and control or process personal data of 25,000 or more Hoosiers. Like most other states, it contains an exemption for entities covered by HIPAA or GLBA, and applies only to consumer (and not employee) information). Key provisions include:

- **Notice**. The impact of the Indiana law on business's privacy notices should be minimal. Like other state laws, the policy must outline the categories of data being processed, the purpose, categories of data being sold or shared, and provide consumers with information about exercising their consumer rights. It is this last category that will prompt privacy policy modifications, in particular for those companies that have indicated in their policies that rights can be exercised only by individuals in the jurisdictions where currently legally required.
- **Consumer Rights.** Once in effect, Indiana consumers will have rights of access, correct, deletion, and portability. They can also opt out of the sale of their personal data. The right to correct only extends to personal data that the consumer has previously provided to the business. Businesses will have 45 days to respond to rights requests.
- **Consumer Opt-Outs.** SB5 follows Iowa, Virginia, Utah, and defines "sale" as the exchange of personal data for "monetary consideration" rather than the broader definition of California[1] and Connecticut[2] which includes "monetary or other valuable consideration". Like other states, consumers can also opt-out of targeted advertising, as well as profiling that could produce legal or other similarly significant effects. Those who profile must do a data impact assessment. Indiana will not require that companies recognize universal opt-out mechanisms (similar to Iowa, Utah, and Virginia).

- **Sensitive Personal Data.** Like Colorado, Connecticut and Virginia, a business must obtain consumer consent before processing sensitive information, rather than -as in California- give consumers the ability to opt-out.
- **Contracts**. Companies who use third party data processors/contractors will need to have contracts in place, just as in other states. The requirements under this new Indiana law are almost identical to those in place in Virginia.
- As with other states, there is no private right of action under the law. Before the attorney general can initiate an action, it must give companies written notice and 30 days to cure the violation (this right does not "sunset," unlike in Colorado, where the 60 day cure period will be sunsetting in January 2025). The Indiana law provides for statutory civil penalties of up to $7,500 for each violation.

PUTTING IT INTO PRACTICE: Companies will need to add January 2026 to their US state privacy law roadmap. While the Indiana law does not add substantively to the list of requirements, it does mean that companies will need to keep track of another state when determining its notice and choice practices, among other things.

Iowa Becomes Sixth State with Comprehensive Privacy Law

Posted April 11, 2023

With the governor signing SF 262 into law last week, Iowa became the sixth US state with a comprehensive privacy law. The law goes into effect January 1, 2025. It applicability is similar to other states' laws. It applies to companies that do business in Iowa and either: (1) control or process personal data of at least 100,000 Iowans; or (2) derive over 50% of gross revenue from the sale of personal data and control or process personal data of 25,000 or more Iowans. These thresholds are calculated annually.

Key provisions include:

- **Privacy Policy.** Similar to the other state privacy laws, businesses must provide privacy notices to consumers. Policies must include specific provisions about personal data processing activities.
- **Data subject rights.** As with other states, Iowa residents will have rights of access, deletion, and portability. They can also opt out of the sale of their personal data. Like Utah, though, Iowa's law does not give right of correction.
- **A Limited Definition of Sale.** Iowa follows the more limited definition of "sale" under the Virginia and Utah laws. Sale includes only exchanges of personal data for "monetary consideration."
- **Longer Time Period for Responding to Consumer Rights Requests.** Businesses have the longest time frame under the Iowa law to respond to rights requests. They have 90 days to respond (unlike the initial 45 days granted by the other state privacy laws). That time frame can be extended by an additional 45 days.
- **Processing of Sensitive Personal Data.** Similar to Utah, Iowa's law requires that businesses provide notice and the ability to opt out of the processing of sensitive personal data.
- **Contracts with Processors.** As with other states, businesses must enter into contracts with their personal data processors that contain certain required provisions.
- **90 Day Cure Period/No Private Right of Action.** Businesses will have 90 days to cure alleged violations of the law before the state attorney general can bring an enforcement action. The law does not give a private right of action. Instead, following the 90 day cure period, the attorney general can bring an action and seek civil penalties of up to $7,500 for each violation.

PUTTING IT INTO PRACTICE: Iowa's new law, while not substantially different from that of other states, does have some unique features. Companies will have until January 2025 to expand their rights provisions to Iowa residents and otherwise update their practices. This includes privacy policy and contractual updates as well as any consumer rights tools and workflows.

Colorado Privacy Law Regulations Finalized: Time to Review Information Practices

Posted March 28, 2023

Colorado's Privacy Act regulations have now been finalized, in advance of the law's July 1 effective date. As we have written previously, the Colorado privacy law applies to companies that conduct business in the state and either (1) control or process personal data of 100,000 Colorado consumers during a calendar year, *or* (2) derive revenue or receive a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of at least 25,000 Colorado consumers. The law mirrors in many ways the comprehensive privacy laws of other states.

Additionally, among its many requirements, the law holds that by July 1, 2024, consumers must be able to opt-out of targeted advertising or the sale of information through a universal opt-out mechanism. The Attorney General was to promulgate and adopt rules relating to the law's opt-out mechanisms by July 1, 2023. Those rules were to establish technical opt-out specifications. Draft regulations addressing this were released in December, and have now been finalized.

As indicated in the draft in December, and continued in the finalized version, the Colorado AG will release a list of Universal Opt-Out Mechanisms that meet the requirements of the regulations by January 1, 2024. Additional mechanisms may be added after that time, and companies will have six months from when they are added to the list to respect signals from the new mechanism. As we indicated in December, the regulations contain more requirements than simply issues relating to opt-out mechanisms. Among the many details are more information about:

- **Notices:** The regulations clarify that privacy notices (as required under 6-1-1308) should be in "plain language" and avoid "technical or legal jargon." They should also be accessible to those with disabilities, following standards like W3C guidelines and be straightforward and accurate.
- **Rights Requests**: For rights requests (under 6-1-1306), the regulations clarify that the mechanism does not need to be specific to Colorado, but should indicate which rights are being made available by the company to Colorado residents. The regulations further clarify that the only information that should be collected as part of the process is what the company needs to process the consumer's request. The regulations also significantly build on the law's access right details, mirroring in many ways the process that exists in California. This includes a requirement that companies give people "specific pieces" of personal information, including information created by the company (marketing profiles, inferences, etc.). The company does not need, however, to give financial account, medical information, or other similar sensitive information. The regulations also provide that records of rights requests be maintained for at least 24 months.
- **Data Minimization**: The law contains restrictions on the amount of information companies can collect (namely 6-1-1308's requirement that it be limited to that which is reasonably necessary for the purpose for which the company is processing data). The regulations build on this by requiring that companies review annually if they need to maintain biometric identifiers. This assessment should be documented in writing. The regulations also specify that companies should not collect information except that which it lists in its privacy policy.
- **Consent**: Under the Colorado Privacy Law, consent is needed in some specific situations, including to (a) process sensitive information and (b) process information about a child. Consent can be obtained before July 1, 2023 as long as it meets with the regulations' requirements. Consent must be provided through a clear, affirmative action, be freely given and specific. The regulations provide more detail about what this means. For example, they specify that a pre-checked box or "blanket acceptance of general terms and conditions" are not sufficient. Similarly, if consent is being sought for multiple things and those items are "not reasonably necessary to or compatible with one another" then people must be able to provide separate consents.

PUTTING IT INTO PRACTICE: Now that the Colorado regulations have been finalized, companies subject to the law can more easily move forward with their compliance activities. This includes review of privacy policies, targeted advertising activities, rights request processing, data minimization, consent reviews, and more.

CPRA Update: Moving Toward Finalization

Posted February 23, 2023

The California Privacy Protection Agency (CPPA) Board recently met and unanimously voted to finalize the proposed final CPRA regulations. This approved version was first released in January and updated those released in November 2022. Along with the proposed final CPRA regulations, the CPPA published a draft final statement of reasons and appendices containing responses to the comments received during the public comment periods.

The proposed final regulations do not contain substantive changes. Now, businesses have confirmation of what text to use in finalizing implementation plans. As we previously noted, the regulations provide an option for a discretionary enforcement delay. The CPPA Board also addressed its next order of business: pre-rulemaking activities on cybersecurity audits, risk assessments, and automated decision-making.

The CPRA regulations now begin the final rule making process. They will be sent to the California Office of Administrative Law for review and approval. The Office of Administrative Law FAQs state that the final regulations will take effect sometime in April 2023 at the earliest. This is ahead of CPRA enforcement beginning July 1, 2023.

PUTTING IT INTO PRACTICE: While this process is not over, this is a welcome sign for businesses who have awaited clarity and finalization. Companies should continue to monitor for changes or delays in the process. Companies may also want to look through the draft invitation for preliminary comments on the other forthcoming regulations about different topics.

Movement on CPRA Regulations Expected

Posted January 30, 2023

On Friday, February 3, the CPPA is scheduled to meet about current and forthcoming CPRA regulations. The Board had previously signaled that it expected to finalize the draft regulations in late January or early February 2023. The agenda confirms that the CPRA regulations will be discussed, including "possible adoption" or "modification" of the text.

Also of interest on the agenda is discussion of rulemaking activities for new rules on risk assessments, cybersecurity audits, and automated decision-making. These topics are of great interest to companies, particularly US-only companies who may not be currently subject to any laws that contemplate these types of requirements.

PUTTING IT INTO PRACTICE: With CPRA's effective date of January 1, most companies have been implementing the regulations as currently drafted. However, finalization of the rules will bring welcomed "closure" to companies as they continue to operationalize CPRA compliance. Companies should also keep a close eye on the forthcoming regulations on the other topics as these will likely drive the need for additional actions.

PUTTING IT INTO PRACTICE: Companies operating in the US now have four comprehensive state privacy laws to keep on their radar for 2023. These are in addition to the myriad (and changing) state privacy laws that govern specific activities and types of information (biometric laws, telephone marketing laws, and more). The continued passage of these laws is a reminder of the importance of having a nimble privacy program that can readily adapt to the changing legislative landscape.

2023 CONTRIBUTING AUTHORS

Liisa Thomas
Partner, Team Leader, Privacy and Cyber Security Practice
lmthomas@sheppardmullin.com
312.499.6335

Townsend Bourne
Partner
tbourne@sheppardmullin.com
202.747.2184

David Poell
Partner
dpoell@sheppardmullin.com
312.499.6349

Wynter Deagle
Partner
wdeagle@sheppardmullin.com
858.720.8947

Kari Rollins
Partner
krollins@sheppardmullin.com
212.634.3077

Hayley Grunvald
Partner
hgrunvald@sheppardmullin.com
858.720.7410

Moorari Shah
Partner
mshah@sheppardmullin.com
714.424.8264

Carolyn Metnick
Partner
cmetnick@sheppardmullin.com
312.499.6315

A.J. Dhaliwal
Special Counsel
adhaliwal@sheppardmullin.com
202.747.2323

Matt Benz
Associate
mbenz@sheppardmullin.com
312.499.6359

Dane Brody Chanove
Associate
dbrodychanove@sheppardmullin.com
858.876.3546

Lillia Damalouji
Associate
ldamalouji@sheppardmullin.com
202.747.2307

Anne-Marie Dao
Associate
adao@sheppardmullin.com
858.720.8963

Snehal Desai
Associate
sdesai@sheppardmullin.com
415.774.2960

Charles Glover
Associate
cglover@sheppardmullin.com
212.896.0679

Julia Kadish
Associate
jkadish@sheppardmullin.com
312.499.63340

Elfin Noce
Associate
enoce@sheppardmullin.com
202.747.2196

Alyssa Sones
Associate
asones@sheppardmullin.com
424.288.5305

Skylar Stoudt
Associate
sstoudt@sheppardmullin.com
202.747.1864

Michael Sutton
Associate
msutton@sheppardmullin.com
469.391.7455

Brittany Walter
Associate
bwalter@sheppardmullin.com
858.876.3525

Sam Cournoyer
Law Clerk
scournoyer@sheppardmullin.com
212.896.0608

Kathryn Smith
Cybersecurity & Privacy Fellow
kasmith@sheppardmullin.com
312.499.6355

SheppardMullin

Brussels | Century City | Chicago | Dallas | Houston | London | Los Angeles | New York | Orange County
San Diego (Downtown) | San Diego (Del Mar) | San Francisco | Seoul | Shanghai | Silicon Valley |Washington, D.C.

www.sheppardmullin.com