SheppardMullin

EYE ON PRIVACY: 2024 YEAR IN REVIEW

These articles appeared in the “Eye On Privacy” Blog in 2024
(www.eyeonprivacy.com)

Sheppard Mullin's 2024 Eye on Privacy Year in Review

These articles appeared in the "Eye On Privacy" Blog in 2024 (www.eyeonprivacy.com)

It is hard to believe that another year is upon us! As we have done in years past (including 2023, 2022, 2021, 2020, 2019 and 2018), we have created a comprehensive resource of all our www.eyeonprivacy.com posts from 2024. As you move forward with your privacy program and risk management for 2025, we hope that this compilation of developments from 2024 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, 2024 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

'All Hands on Deck' – White House Continues to Call on Agencies for AI National Security Plan

Posted December 16, 2024

In the waning months of the current administration, the White House issued a memo setting forth actions focused on national security as directed in the AI Executive Order from last year. As a reminder, the order -while directed to government agencies- also had impacts on how businesses use of artificial intelligence.

The national security memo builds on last year's order, and of potential interest for businesses, calls on agencies including the Department of Defense, to assess potential risks to the US private sector's AI competitive advantage. The memo also tasks the National Science Foundation with piloting programs to support AI development, and the Department of Energy and others to coordinate the support of AI-enabled infrastructure.

On the security front, the memo outlines the role for NIST as the government's "primary point of contact" with the private sector's AI developers. The memo tasks NIST with developing testing standards to ensure the safety, security and trustworthiness of AI models. Among other things, NIST is to look at the ability for AI models to impersonate people and ways to stop malicious use of AI models as well as risk management processes through the AI development lifecycle.

PUTTING IT INTO PRACTICE: As the year draws to a close and we anticipate a new administration in Washington, we do not anticipate any slow down in the involvement of agencies on AI development, although the focus of some initiatives may change. The role of NIST as a conduit and developer of standards for the development of AI models will also likely continue.

The Privacy and Data Security Impact of California's Recent AI Bills

Posted October 29, 2024

The dust is beginning to settle from the raft of AI-related bills Governor Newsom signed last month in California. (See for example, our post about neural data.) Most of the provisions will not go into effect for another few months. Before they do, it is worth examining the impact they will have on companies' privacy and data security practices. Most, as we outline below, may not change fundamental practice, but instead serve as a reminder to take into account privacy and data security considerations when assessing and implementing AI tools:

- **AI Definition(s):** AB 2885 establishes a legal definition of artificial intelligence across California laws. AI is defined as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments." In addition, Newsom signed an amendment to CCPA (AB 1008) which clarifies that consumers' "personal information" may exist in AI systems that output personal information. The change to CCPA is effective January 1, 2025.
- **Health Care Services Disclosures**: Similar to Utah's law earlier this year, AB 3030 will put disclosure requirements on health facilities, clinics, physician's offices, or offices of a group practice. Beginning January 1, 2025, if these entities use GenAI to create patient-facing communication, they must take certain steps. These include both (1) a disclaimer that indicates to the patient that a communication was generated by GenAI, and (2) clear instructions describing how a patient may contact a human health care provider, employee, or other appropriate person.
- **AI and Entertainment**: California will join Tennessee on January 1, 2025 in regulating "digital replicas" of voices and likenesses. First, AB 2602 holds contracts to be unenforceable if an employer uses a computer-generated "digital replica" of a performer's voice or likeness in lieu of the performer's in person performance. Second, AB 1836 gives beneficiaries of a deceased celebrity a cause of action to recover damages for the unauthorized use of AI-created digital replicas.

- **AI and Robocalls**: AB 2905 amends California's current automatic dialing-announcing laws. It requires telling call recipients if the prerecorded message uses an AI-generated voice.
- **Transparency**: Beginning January 1, 2026, GenAI developers will need to give certain notices to consumers as provided for in AB 2013. This includes telling people the sources of GenAI data, how the data is used, the number of data points, and a description of the types of data points within datasets. Notice must also include whether there is any personal information within the datasets and list other protected information in the datasets. A similar requirement goes into effect on the same day. The law (AB 942) requires that AI system providers offer a free tool that lets the public determine whether content was generated or modified by AI. Among other things, they must also clearly and conspicuously disclose that content was generated by AI.

PUTTING IT INTO PRACTICE: These recent laws are a reminder to companies to consider privacy and data security compliance when adopting AI tools. We anticipate similar developments from other states. Having an adaptable approach will be key as companies identify and adopt new uses of GenAI.

NYDFS Speaks Out on AI and its Cybersecurity Risks

Posted October 24, 2024

The New York Department of Financial Services ("NYDFS") recently published guidance on managing cyber risks related to AI for the financial services and insurance industry. Though the circular letter does not introduce any per se "new" obligations, the guidance speaks to the Agency's expectations for addressing AI within its existing cybersecurity regulations.

The letter identifies specific AI-related cybersecurity threats, such as AI-enabled social engineering. AI may also enhance typical cybersecurity attacks by amplifying the potency, scale, and speed of an attack. The letter also notes that AI modules may leverage large volumes of non-public information and become a target of an attack. Additionally, reliance on third party providers and vendors for AI-tools introduces supply chain vulnerabilities.

To mitigate these risks, NYDFS advises regulated companies to consider the specific risks related to AI when conducting comprehensive risk assessments. These assessments should consider not only the organization's own use of AI, but also any AI technologies used by a third party service provider. Based on findings of the risk assessments, policies, procedures, and incident response plans may need to be updated to sufficiently address these AI-related risks. NYDFS also highlights the need for cybersecurity training for all personnel (including senior executives) that includes awareness around AI-related threats and response strategies.

PUTTING IT INTO PRACTICE: This latest thinking from NYDFS adds to the growing patchwork of regulatory guidance about specific considerations related to AI (here, the cybersecurity risks). Other guidance has largely focused on other types of harm from AI such as bias and discrimination. It also serves as a reminder for companies that might not use AI themselves to be aware of the potential risks of engaging third parties who do and implement proper mitigating measures.

Illinois Updates Employment Law to Address Artificial Intelligence

Posted August 26, 2024

Illinois recently updated its employment law, the Illinois Human Rights Act to prohibit discriminatory uses of AI. Artificial intelligence as defined by the amendment will cover generative artificial intelligence, not just traditional AI. The amendments are set to take effect on January 1, 2026.

AI is defined to include outputs that can simulate human-produced content, including short answers, essays, diagrams, art, videos and songs. Employers will be prohibited from using AI in a discriminatory way in the employment context. This includes in recruitment, hiring, promotions, and discipline. Discrimination is that which is based on protected classes or use of zip codes "as a proxy for protected classes."

Companies also will need to give employees notice if they are using AI for employment purposes. These include as noted above, for recruitment, hiring, promotion, and discipline. The Illinois Department of Human Rights charged with adopting regulations for, among other things, notice timing and process.

PUTTING IT INTO PRACTICE: This law joins others that seek to regulate company's use of artificial intelligence, including in Colorado and New York City. As companies develop their AI policies, this new law is a reminder to think now about procedures and mechanisms for avoiding discrimination when using the tools.

AI Summer Roundup: EU and Colorado Celebrate Summer with AI Legislation

Posted August 13, 2024

As we enter the end of the summer, the AI regulatory steam is not slowing down. Colorado is now the first US state to have a comprehensive AI law (going into effect February 1, 2026), and the EU published its sweeping AI law in July (with rolling applicability between February 2025 and August 2026).

Both the Colorado and EU laws apply to entities that make AI systems, as well as those that use them. The EU law will also apply to entities who import and distribute such systems into EU Member States. Both laws define AI systems to include all types of AI, not only generative AI, and specifically regulate "high-risk" AI systems (with some exceptions). I.e., those that make consequential decisions about things like education, employment, and housing. Both contain exemptions, like calculators that use AI, or AI used for certain research purposes.

As a reminder, for those watching AI law developments, you know that in the US there is also NYC 's employment-related AI law, which went into effect July 5, 2023 and regulates use of AI in making employment decisions. Utah has an AI law as well. It requires disclosures to individuals when they interact with AI, and went into effect May 1, 2024. Finally, Tennessee's AI law focuses on individuals' rights against deepfakes, and went into effect July 1, 2024.

What should companies keep in mind as we anticipate Colorado's and the EU's more comprehensive AI laws? Especially if future similar laws are passed? Here are some top-of mind concerns, both for those who develop the systems, as well as those who deploy them:

- **Avoid algorithmic discrimination**. Both Colorado and the EU will specifically require that companies take steps to mitigate bias and algorithmic discrimination. For Colorado, discrimination means treating people differently based on characteristics like age, race, gender, or religion. For the EU, discrimination means not avoiding a foreseeable risk that impacts the health, safety, or fundamental rights of an individual. The EU law requires that both developers and deployers implement quality and risk management systems that address and mitigate foreseeable risks like algorithmic discrimination. Colorado's law also imposes a duty on developers and deployers to avoid algorithmic discrimination.

- **Be transparent**. Like the law in Utah, both AI laws will require disclosures to individuals when they are interacting with a consumer-facing AI system – unless such an interaction would be "obvious" to a reasonable person. This notice is required regardless of whether the system is high-risk or not. Companies will also need to give Colorado residents notice of their right to opt-out and how to do so. In the EU, companies will need to disclose AI systems that produce deepfakes or process biometric data or emotion recognition.
- **Developers should give sufficient information to those who deploy high-risk AI systems.** In the EU, those who develop high-risk AI systems also need to provide clear details to those who will use them (i.e., "deployers") about how they work, along with detailed use instructions. The instructions should include, among other things, information about known or foreseeable risks and the high-risk AI systems' technical capabilities. Colorado has similar requirements for developers of high-risk AI systems.
- **Have risk management systems in place**. Those who deploy AI systems in Colorado will need to adopt a "reasonable" risk management program like NIST's recently-updated AI Risk Management Framework, ISO/IEC 42001, or a comparable framework. Businesses in the EU that use high-risk AI systems will also need to establish and maintain risk management systems. These risk-management systems will need to adopt the most appropriate measures in light of the state of the art in AI.
- **Conduct impact assessments.** Those who deploy high-risk AI systems will need to conduct an annual impact assessment under both laws. Companies should keep in mind, though, that these kinds of assessments may already be needed under both GDPR and those US state laws (California, Colorado, Connecticut, Delaware, Florida, Indiana, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, and Virginia) that require impact assessment when a business engages in, among other things, high-risk profiling.
- **Keep in mind related laws' requirements.** Before these laws go into effect, companies should remember obligations under GDPR (for the EU) and US state laws (as noted above), as well as unfair and deceptive trade practices laws. Both EU regulators and the FTC have cautioned that they will enforce many of the same concepts from these upcoming laws under those regulatory regimes.

A violation of Colorado's law constitutes an unfair trade practice. The Colorado AG office has exclusive enforcement power. Under the EU law, the AI Office and member state authorities will share enforcement power.

PUTTING IT INTO PRACTICE: While there is still time before these two laws go into effect, it would be prudent to begin preparing now. Not only will 2025 and 2026 be here before we know it, but some taking these requirements into account can address current regulatory concerns and scrutiny brought under GDPR, US state laws, and concepts of unfair and deceptive trade practices.

Tennessee's ELVIS Act Incorporates AI Considerations into Right of Publicity Protections

Posted May 24, 2024

Tennessee recently amended its 1984 right of publicity statute with passage of the ELVIS Act. The existing law already protected individuals' rights in their image and likeness. As amended, the statute will specifically call out voice as another protected element. It will become the first right of publicity statute to address copying someone's likeness or voice with AI technologies in two ways.

First, beginning July 1, 2024, the law will prohibit distributing software, tools and algorithms whose "primary purpose" is reproducing someone's likeness or voice. The law previously prohibited infringing on someone's likeness, but as amended will also prohibit publishing, transmitting or otherwise making available someone's likeness or voice without the individual's authorization.

Second, the amended version of the law also includes within its protection someone's "voice," which includes broadly a "sound attributable to" a person. This could be their actual voice, or a simulated version of it.

The law was previously known as the Personal Rights Protection Act, but will be known as the Ensuring Likeness, Voice and Image Security (ELVIS) Act of 2024. Not surprisingly, for the Elvis's home state, the rights survive someone's death, and can be enforced by their heirs.

PUTTING IT INTO PRACTICE: This law may have been aimed at protecting celebrities from AI-generated versions of their voice and likeness. However, its protections extend to all individuals, and as such companies who are using AI will want to keep its restrictions in mind.

Utah's New AI Disclosure Requirements Effective May 1

Posted April 26, 2024

The Utah legislature has been busy, with another law effective May 1. This one is "privacy adjacent" but worth keeping in mind. The law, the Artificial Intelligence Policy Act, was signed into law in March. Among other things, it will require companies to respond "clearly and conspicuously" to an individual who asks if they are interacting with artificial intelligence and the communications are made in connection with laws regulated by the Utah department of commerce. (This includes the Utah Privacy Act, the state's sales practices law, its telephone solicitation laws, and many others.)

Artificial intelligence is defined in the law as an artificial system that is trained on data, that interacts with someone through text, audio or visual means, and creates output that is "similar" to a human, without human oversight. The law's disclosure requirement is a reactive one. The disclosure needs to happen only if "asked or prompted" by the individual.

There is one caveat to this reactive provision. Businesses who are in "regulated" occupations must make a prominent disclosure that they are using AI in the provision of those services. Regulated occupations include any licensed by the Utah Division of Professional Licensing. This includes many health care professions, as well as court reporting, athletic trainers, plumbers, electricians, and more.

The reactive nature of the law is unlike a California "chatbot" law. That law prohibits misleading people into thinking they are "interacting online" with a human if in fact they are interacting with an "artificial identity." The law provides an affirmative defense to have a clear and conspicuous disclosure that the tool is a bot. A bot is defined as an online account where actions are not those of a person (so encompassing more than generative AI, but also automated replies). In other words, the law requires disclosing the nature of the "artificial identity" prior to someone interacting with it. It is narrower than the Utah law, however, as it relates only to when someone is interacting with the bot to "incentivize" a sale (or to get someone to vote).

PUTTING IT INTO PRACTICE: Companies who may be subject to this law (apart from any who provide services in "regulated occupations") may want to test any GenAI tools they are using to interface with the public. How do those tools respond if someone asks "are you AI," "is this a bot," "are you human" and the like? For those who are in regulated occupations, remember that the disclosure obligations are affirmative to the extent that the law applies.

FTC Seeks Comments on AI Impersonation Rules

Posted March 20, 2024

Earlier this month, accompanying an update to a rule prohibiting the impersonation of businesses and governments, the FTC sought comments on extending the rule to prohibit impersonation of individuals. The agency indicated that it is considering expanding the rule as the result of rising complaints around "impersonation fraud," especially those generated by AI. Comments are due by April 30, 2024.

As proposed, the rule would prohibit "materially and falsely" posing as another individual both expressly or by implication. Similarly prohibited would be false endorsements. Importantly for businesses seeking to develop products or platforms that incorporate AI, the rule would also prohibit providing goods or services that would be used to engage in these practices. FTC chair Lina Khan, along with two other commissioners, emphasized the importance of "extending liability to any actor that provides the 'means and instrumentalities' to commit an impersonation scam" in an accompanying statement to the proposed rule.

PUTTING IT INTO PRACTICE: It took almost two years to amend the rule to address impersonation of business and governments. While it is possible that the proposed amendment will take just as long, this proposal signals the FTC's concerns not only with those engaging in AI-created "deepfakes," but also with companies that create products and services that make them possible. Even absent a rule amendment, it is possible that the FTC may bring action under its current Section V authority.

FTC Sends Stern Reminder to AI Companies

Posted January 12, 2024

While the US does not have some specific AI-focused law a host of regulators have been providing their thoughts about AI. Noticeable traction on the topic began in 2020. With the explosion of ChatGPT in 2023, commentary (and scrutiny) has been picking up steam.

Unsurprisingly, the FTC is in the mix sharing its thoughts through various blogs and investigations. Its blogs have focused on specific aspects of AI – use of AI, claims about AI, voice cloning, and now, companies that develop AI. In its latest guidance, the FTC reminds companies that develop AI models of their obligations around privacy commitments made to their users and customers. The take-aways and underlying points in this post are not new. The FTC has long reminded (and enforced) companies that the statements made about how information will be collected, used, shared, protected, etc. must be upheld. That said, this guidance puts those concepts into the context of a growing area of companies – model-as-a-service companies.

Model-as-a-service companies are those companies that develop and host AI models that are made available to other businesses and users via an API. According to the FTC, these companies should be cautious about commitments around data use found not only in privacy policies, but terms of service and other promotional materials. The FTC also cautions that material omissions may be just as problematic – e.g., those statements that would affect whether customers buy a particular product.

PUTTING IT INTO PRACTICE: Companies developing any kind of machine learning, natural language processing, or other AI solutions and capabilities for business customers or individual users should take a close look at its statements around data use. Are any claims about how information is being used overstated? Is there anything material missing in product disclosures and terms that would impact whether a person would buy this service? These types of assessments are key for ongoing compliance. The FTC will continue to scrutinize these types of statements and may require deletion of the developed model and algorithm if a company runs afoul of the law.

BIOMETRICS, TRACKING AND WIRETAP

EDPB Provides Insight for Use of Tracking Tools

Posted November 1, 2024

The EDPB released guidance last month to help companies understand their obligations when using newer tracking tools. These include pixels, URL tracking, IP-tracking, and the like. First, some background: an EU law that predates GDPR (Directive 2002/58/EC or the Cookie Directive), impacted how companies could interact with users on their computers. That directive was updated in 2009 (Directive 2009/136/EC or the ePrivacy Directive). Under the ePrivacy Directive, among other things, companies cannot "store" or "access" someone's "terminal equipment" without consent. (There are some exceptions to the consent requirement.) In this recent guidance, the EDPB provided direction on when and whether passive tracking technologies were storing or accessing information on a users' computer (or other device) such that the ePrivacy Directive requirements would apply.

In the guide, the EDPB reminded companies that the ePrivacy Directive requirements apply when the technology collects *any* information (not just personal information). Additionally, that in-scope equipment can be that owned or simply used by an individual. The equipment may also not be a computer, but could be a connected (IoT) device. And, that "access" can occur through technologies that place software on someone's computer (APIs, JavaScript) or instructing protocols (SDKs, tracking pixels). Finally, that "storage" might be temporary, but will still be in scope for the ePrivacy Directive.

With these in mind, the EDPB outlined what it viewed as newer technologies that are in-scope for the ePrivacy Directive. This updates the list from the 2014 Working Party guidance (which included digital fingerprinting). The list provided in this new guidance included tracking pixels, when they are sent to the user's computer and then return to the sender with specific information. It also included IP-only tracking, if the IP address "originates from the" user's computer. The list the EDPB provided was not exhaustive, it stressed.

PUTTING IT INTO PRACTICE: This guide is a reminder that new technologies can be viewed as in-scope for older laws. While this guidance is helpful, it does not outline the times when there might be an exception to the consent requirement. Something that the EDPB specifically called out. Privacy practitioners reviewing proposed tracking tools may find helpful the way that the EDPB analyzed these tools to determine whether or not the ePrivacy Directive would be viewed as applying.

Promising Decision in Wiretapping Case, Win for Businesses

Posted September 26, 2024

Those tracking CIPA litigation are familiar with the recent decision holding in favor of a company whose site had an online chat operated by a vendor. The court in that case held (1) that the company had not violated the California Invasion of Privacy Act (CIPA), and (2) that its chat was not unauthorized "wiretapping." This ruling came as welcome news to companies who offer online chat features, especially those who face—or fear—similar lawsuits.

The case, *Gutierrez v. Converse Inc.*, 2024 WL 3511648 (C.D. Cal. July 12, 2024), followed a similar pattern and set of claims as others have faced. The plaintiff alleged that she used a third-party enabled chat function on Converse's website and that the chat providers stored the chat conversation on third-party servers without her consent. Thus, her attorneys argued, the chat provider aided and abetted "wiretapping" under Section 631(a) of the CIPA.

The court granted the motion for summary judgment on grounds that the chat provider did not engage in wiretapping as a matter of law. Specifically, the court held that Section 631(a) only applies to telephones and did not include smart phones where the plaintiff uses an internet connection to access the chat. Additionally, the statute requires that the chat provider "willfully and without consent" read or attempts to read or learn the contents of a communication. The court held that the plaintiff did not meet this standard because the message was encrypted in transit and password-

protected on the chat provider's servers. The court held that the "mere possibility" that the chat provider *could* read a message was not enough to establish a genuine issue of material fact. There was no CIPA violation, so Converse could not have aided and abetted a non-existent violation.

PUTTING IT INTO PRACTICE: Although this decision is a promising one for companies who operate online chat features, it is still helpful to provide notice if recording chats. Additional disclosures should be included if the chat functionality is run or hosted by a third party. While there can be other defenses available to businesses facing one of the chatbot suits, these notice steps can help.

It's Official – BIPA's "Per-Scan" Damages Are Out; Electronic Signatures Are In

Posted August 12, 2024

If you heard a collective sigh of relief last week, it was probably businesses reacting as Illinois Governor Pritzker finally signed Senate Bill 2979, officially reforming BIPA for the first time since 2008. As a reminder, SB 2979 was passed back in May, but has been awaiting the Governor's signature.

This development is significant for two reasons. First, the new law prohibits the recovery of "per-scan" damages. This means that if a business collects or discloses an individual's biometric data without consent, then that business is only liable for one BIPA violation as to that individual. In 2023, the Illinois Supreme Court's decision in *Cothron v. White Castle Systems* decided that violations were accrued on a "per-scan" basis, leading to an outpouring of claims. This law effectively overrules that decision. Second, the bill permits businesses to fulfill the "written release" requirement for consent via "electronic signature." This will make it easier for businesses to collect – and individuals to provide – consent for the collection and retention of biometric information.

PUTTING IT INTO PRACTICE: These amendments became effective on August 2, 2024. Businesses that anticipated costly litigation from a "per-scan" BIPA demand may have cause for relief. However, the prohibition on "per-scan" damages may not apply retroactively to pending BIPA actions. Additionally, businesses can reconfigure their consent flows to enable electronic signatures.

Websites Beware!: FTC Joins Other Regulators in Scrutinizing Alleged Dark Patterns

Posted July 24, 2024

In its ongoing concern with "dark patterns," the FTC recently announced results of two reviews of sites and apps purportedly engaging in the practice. As a reminder, the FTC views as "dark patterns" practices or web designs that "get consumers to part with their money or data" using deceptive or manipulative means. Both of the recent reports were completed by global consortiums of regulators of which the FTC is a member.

The first report, done by ICPEN, or the International Consumer Protection and Enforcement Network, looked at 642 global subscription services sites and apps. The report found nearly 76% contained at least one alleged dark pattern while 67% used more than one. Most typical was the inability to turn off subscription autorenewals. This was followed by a lack of information about how to cancel a subscription during enrollment or before an autorenewal.

The second report was done by GPEN, or the Global Privacy Enforcement Network. That report looked across industries, at 1,010 sites' and apps' privacy-related practices. According to the report, an alleged 97% had a practice GPEN viewed as a dark pattern. Counted as a purported dark pattern were privacy policies that were "excessively" long, had technical jargon, or confusing language.

PUTTING IT INTO PRACTICE: These reports signal some of the practices that the FTC and others may consider a dark pattern, in violation of Section V of the FTC Act. This is a reminder for companies to look at their online information collection practices, as well as disclosures (like privacy policies), to avoid potential deception and manipulation allegations.

BIPA Reform Watch – Illinois Legislature Eliminates "Per-Scan" Damages

Posted May 22, 2024

For the first time since 2008, BIPA reform is in the air. On May 16, 2024, the Illinois House of Representatives overwhelmingly approved Senate Bill 2979, which paves the way for final passage to Governor J.B. Pritzker's desk.

Most significantly, the new bill overrules the Illinois Supreme Court's 2023 decision in *Cothron v. White Castle Systems*. In *Cothron*, the Illinois Supreme Court held that BIPA plaintiffs could recover liquidated damages of $1,000 (or $5,000) for each unconsented scan of their biometric identifier (e.g., fingerprint, facial scan, etc.). But Senate Bill 2979 prohibits recovery of per-scan damages. If the bill becomes law, a private entity that collects a person's biometric data or discloses it without consent can only be found liable for *one* BIPA violation as to that person. *See* S.B. 2979, amending 740 ILCS 14/20. Illinois General Assembly – Full Text of SB2979 (ilga.gov) Upon passage of the amendments to BIPA's damages provision, *Cothron* will be a dead letter.

The new bill also makes it easier for entities to establish written consent. Specifically, the bill expands BIPA's definition of "written release" to include an "electronic signature"—defined as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." Expressly allowing for consent via electronic signatures will make it easier for companies to obtain and secure records of individuals' consents.

PUTTING IT INTO PRACTICE: Until Gov. Pritzker signs Senate Bill 2979, it is not the law of Illinois. If he does (as expected), the amendments will take effect *immediately*, meaning that per-scan damages will not be available in any pending BIPA lawsuit.

CHILDREN'S PRIVACY

UK and US Issue Joint Statement on Children's Privacy

Posted November 11, 2024

The United Kingdom and the United States released a joint statement last month outlining plans focused on children's online privacy. As indicated in the statement, they intend to engage national institutions and other organizations to support this work. They will also be forming a joint online safety working group.

The statement focused on smartphones and social media use. This aligns with recent laws passed in the US that have tried to place limits minors' interactions with social media. There have been similar efforts in the UK. In the statement, both countries called for increased transparency from online platforms. This would take shape as accessible terms of service and online safety practices. Additionally, the statement proposes several protective measures that online platforms could implement including:

- Preventing the promotion of harmful content
- Better reporting on content moderation
- Strong default privacy settings
- Limits on targeted advertising

PUTTING IT INTO PRACTICE: This statement is a reminder that children's use of social media is a top concern for regulators and lawmakers.

#StatusUpdate on Social Media, Apps, and Children's Privacy

Posted November 6, 2024

Regulations impacting children's use of social media continues to be a space in motion the past few months. There have been developments at both the state level, as well as with the FTC. And there is no sign of slowing down. In this article we give a roundup of some recent developments worth keeping in mind.

First, at a state level Florida's social media and minors law, HB 3, is facing its first challenge. The law, which was passed in March was to go into effect date of January 1, 2025. Among other things, it would have prohibited children 13 and under from creating social media accounts. Additionally, it would have required parental consent for 14- and 15-year-olds to join these sites. The recently-filed complaint mirrors challenges other states have faced for their similar laws. It alleges that the HB 3 is unconstitutional on First Amendment grounds. A Federal judge blocked Utah's revamped social media law which was challenged for the same reasons. Similar social media laws in Texas, Arkansas, and Ohio, were also struck down after First Amendment challenges.

The FTC has also come off a busy summer of children's privacy. Last month the agency announced a virtual workshop on digital platform features aimed at keeping minors online longer and coming back more frequently. It also recently posted a stipulated order for injunction against NGL Labs. The FTC had alleged that NGL's anonymous messaging app violated child privacy laws, including COPPA. According to the FTC, NGL did not get parental consent from users under the age of 13. Among other accusations, the FTC stated that NGL also kept children's data for longer than necessary. The resulting order banned NGL from offering their app to anyone under 18. Additionally, NGL was ordered to pay $5 million in fines.

PUTTING IT INTO PRACTICE: For companies offering online platforms for children, these developments are a reminder that there is heavy regulatory and enforcement scrutiny on these platforms. While there has been success in pushing back on many of the recent laws, the FTC does not seem to be pausing in its review under both COPPA and unfairness/deception under Section V of the FTC Act.

California: Age-Appropriate Design Code Act Partially Blocked, New Social Media Law Signed

Posted September 25, 2024

California has been active in the kids space. First, the Ninth Circuit's recently ruled on the California's Age-Appropriate Design Code Act. Second, the governor has just signed a new law aimed at social media sites.

The Ninth Circuit ruling may cause some confusion about what parts of the law are effective, and what are not. As a reminder, the Act mirrors the UK's Age Appropriate Design Code. As we have written previously, it was intended to regulate companies that offer online services to children. A temporary injunction delaying the law's July 1, 2024 effective date was entered last year. The Ninth Circuit has affirmed part of that injunction, but not all of it. What does this mean for businesses who offer online services to children?

What Has Been Enjoined?

Under the law, companies would have been required to conduct data protection impact assessments documenting an eight-factor assessment of potential risk of harm to children for their online services offered to children. The court held that this report "compelled speech" and thus was subject to First Amendment scrutiny. And under that scrutiny, the Ninth Circuit ruled that there could have been a less restrictive way to accomplish protecting children than requiring a DPIA.

What Is Unclear?

The case was remanded to the district court for further ruling. In particular, because the law does not have a severability provision. Meaning that if part of it -here the DPIA provision- cannot be severed from the rest of the law, the remainder of the law, or parts of it, would not similarly be invalid. The Ninth Circuit ruled that the district court will need to assess this, in particular those provisions of the law that grammatically were tied to the DPIA requirement. This included the following requirements in the law:

- That the company estimate children's age with a level of certainty "appropriate to the risks" from the company's data management practices.
- That the company configure privacy-by-default unless a different setting "is in the best interests of children."
- That the company provide information about privacy in language "suited to the age of the children likely to access" the service.

What Was Not Contested?

Not all of the provisions of the law were contested. Those that were not contested included:

- Collecting precise location information only if it is strictly necessary and other restrictions are followed.
- Not engaging in "dark patterns" to encourage children into sharing more information than necessary for the service.
- Using information collected to estimate age for any purpose other than estimating age.

What Else Is Happening With Kids?

Since the decision, Governor Newsom signed a new law aimed at social media sites that are "addictive" to children. The law, "Protecting Our Kids from Social Media Addiction Act" will go into effect January 1, 2027. It will prohibit providing "addictive feeds" to minors. It also gives parents certain rights. These include letting parents decide whether kids see messages chronologically, or based on the sites' algorithms. Parents will also have the ability to stop kids' access during the school day and at night. The California law is similar to one in New York, which we wrote about recently and will be effective after AG rulemaking.

PUTTING IT INTO PRACTICE: As we await further rulings on the Age Appropriate Design Act, companies that offer online services to children should keep in mind the law's non-DPIA requirements, other similar laws, and the likelihood that the California AG will move forward with the fight to keep the law on the books and to enforce it.

Regulators On Both Sides of the Pond Seek Input on Children's Privacy

Posted September 6, 2024

The New York Attorney General's office and the UK Information Commissioner's Office were busy last month when it came to children's privacy. Both sought input from the public about regulating children's online privacy, including on social media.

New York

In New York, the AG office released notices of proposed rulemaking for the New York Child Data Protection Act (effective June 20, 2025) and the Stop Addictive Feeds Exploitation (SAFE) for Kids Act (effective 180 days after rulemaking is complete). In the notice, the AG office is seeking comments to rules for these two laws by the end of this month.

The New York Child Data Protection Act places restrictions on businesses that collect personal information from teens and requires "privacy protection by default." The law includes obligations not only on information collection and use for children under 13, but also for those from 13 to 18. For those under 13, companies must comply with COPPA. The SAFE for Kids Act, on the other hand, governs "addictive social media" patterns on websites and apps for kids under 18.

United Kingdom

Across the pond, the UK ICO has signaled that it will be looking closely at social media platforms' compliance with its UK Age Appropriate Design Code. The Code outlines for companies how to adhere to UK GDPR when offering digital services to children. Similar to New York, the ICO is also asking for public comments, with a deadline of October 11, 2024. It has asked for input how children's data is used by recommender systems and developments in the use of age assurance systems to identify children under 13.

By way of background, the Code calls on companies to adopt privacy-friendly default settings when offering services to children. In April of this year the ICO issued a compliance strategy that offered suggestions for these privacy-friendly defaults. This includes not defaulting to geo-tracking or profiling children. As a further development, late this summer, the ICO reviewed account sign-up flows for over 30 platforms and had concerns with many for not adhering to the Code.

PUTTING IT INTO PRACTICE: We expect to see more developments in children's privacy through the end of the year, especially in social media space. These two requests for comments are a reminder that regulators expect companies to default to "privacy friendly" settings when interacting with children online.

CARU Settles With KidGeni AI Platform Over Alleged Privacy Violations

Posted August 16, 2024

The Children's Advertising Review Unit recently settled with KidGeni – a generative art platform intended for children- for allegedly violating both CARU's guidelines and COPPA. According to CARU, which is a self-regulatory organization that audits the privacy practices of companies in the child space, KidGeni collected personal information without first getting parental consent. CARU began its investigation in the company's functionality in August 2023. As part of its investigation, it reached out to the company to clarify how the site obtained prior parental consent for its children's platform as required under both COPPA and CARU's guidelines.

CARU concluded that COPPA and the CARU guidelines applied because KidGeni was directed to children under 13. In reaching this conclusion, it looked at the site's visual content and child-oriented activities, as well as representations made by the company. CARU then assessed whether KidGeni collected personal information. It found in many situations that KidGeni did so, including when children (1) signed up for an account, (2) signed up for newsletters, (3) inputted prompts into the AI tool without an account, (4) shared information with friends or on social media. Personal information was also collected, CARU noted, through third party tracking tools on the site. Personal information collected in these instances included name, email addresses, and in the case of free-form submissions (inputs into the AI tool, for example) photos and stories that might contain personal information.

Because KidGeni was directed to children and collected personal information, CARU argued that the company had an obligation to follow both COPPA and CARU's guidelines. That included providing an accurate privacy policy, getting parental consent, and having a process in place for parents to limit how their children's information was used. As for the first, the site originally did not have a privacy policy, as required under COPPA and CARU guidelines. After receiving CARU's inquiry, KidGeni posted what CARU alleged was an "incomplete and insufficient" privacy policy, as among other things, the privacy policy failed to disclose that KidGeni collected and shared personal information with third parties, like open-source AI training technologies. As for the second, KidGeni did not as noted above get prior parental consent. It also, CARU found, did not have parental control processes in place.

Although indicating that it did not agree with CARU, KidGeni agreed to take corrective action. That included getting parental consent before using user data to train AI models. Companies who do not cooperate with CARU are referred by that self-regulatory body to the Federal Trade Commission, which has authority to enforce COPPA.

PUTTING IT INTO PRACTICE: This case is one of the first brought against an operator of AI tools directed to children. It serves as a reminder for companies creating these platforms to think about child-specific privacy requirements, especially when child-submitted information might be used by an AI model. Items to consider include providing adequate to notice about information collected and getting parental consent before collecting personal information from children online.

New York Law Seeks to Regulate Addictive Social Media Feeds

Posted July 19, 2024

New York's governor recently signed the Stop Addictive Feeds Exploitation (SAFE) for Kids Act. Although signed, the law will not be effective until after the New York Attorney General creates implementing regulations. The law is aimed at protecting children under 18 from social media companies' "addictive feeds." Addictive feeds are defined to include platforms and services that recommend content based on information from the user's activity or device. Among other things, the law will:

- Require social media companies to obtain parental consent before serving addictive feeds to minors under 18
- Prevent social media companies from pushing notification to minors between 12 AM and 6 AM, unless otherwise approved by a parent
- Allow parents to limit access to social media
- Prohibits companies from discriminating against users who do not opt-in to addictive feeds or late-night notifications

PUTTING IT INTO PRACTICE: This law is similar to others we have seen in other states, and reflects legislators ongoing concerns about the harms that social media has on young users. We expect to see more in the coming months.

Mother May I? Florida and Utah Recently Passed Regulations for Minor Use of Social Media Platforms

Posted April 23, 2024

Florida recently passed a new law and Utah recently repealed and replaced its previously enjoined law with two new bills (available here and here), which regulate minors' access to social media platforms. The laws highlight states' continued efforts to protect minors in the social media realm.

Florida's law goes into effect on January 1, 2025. It will prohibit social media companies from allowing children 13 and under on their platforms: children under this age cannot create social media accounts. It also requires parental consent for account creation by minors who are 14 or 15. Social media companies will also need to delete existing accounts for children under 14 and implement age verification for pornographic or explicit websites. The law allows the Department of Legal Affairs to enforce it with civil penalties up to $50,000 per violation. Florida house speaker, Paul Renner, touted the law as one that is unlike other state laws that were previously challenged on First Amendment grounds. Renner claimed that Florida's law addresses potentially harmful features, rather than content itself.

Utah's Social Media Regulation Act, which was challenged based on a potential violation of First Amendment rights, has been replaced by two bills, SB 194 and HB 464. Both take effect on October 1, 2024. Both laws apply to "social media companies" operating social media services primarily used by account holders to interact socially. SB 194

contains most of the law's general provisions, while HB 464 includes a private right of action for adverse mental health outcomes that arise "in whole or in part" from a minor's excess use of social media. The definition of a social media service does not include email, cloud storage, or document viewing, sharing, or collaboration services. The laws generally apply to Utah residents who are under 18. As a reminder, California, Ohio, Arkansas and Texas have tried to pass similar laws that aim to either boost online safety or restrict minors' social media access. Such laws have also received constitutional pushback (see holdings for California, Ohio, Arkansas and Texas, which is pending before the U.S. Supreme Court).

Unlike the prior Social Media Regulation Act, the new Utah bills require companies to implement an age assurance system to determine if users are minors. Parental consent is not required for creating or accessing accounts, but only for certain functionalities. Minors' accounts need to have default settings limiting visibility, data collection, direct messaging, and certain engagement features. Minors can designate supervisors to set usage limits, schedule breaks, and access account information.

PUTTING IT INTO PRACTICE: Since prior state laws have been constitutionally challenged, we will likely see more states passing laws attempting to regulate social media platforms' interactions with minors.

COMMUNICATIONS PRIVACY

FCC's One-To-One Consent Rule Takes Effect in January

Posted December 19, 2024

For those who send marketing texts, keep in mind the FCC one-to-one consent rule update. It has been getting some publicity, and takes effect January 27, 2025. As most are aware, TCPA requires getting consent before sending certain automated texts. For automated marketing texts, prior express written (i.e. signed) consent is needed.

Under the updated TCPA rule, the FCC has expressly indicated that business's cannot rely on a third party's consent. According to the FCC, this will close a "lead generator loophole." As amended, the rule now indicates that a consent to send an automated marketing text can authorize "no more than one identified seller" to send (or cause to be sent) a marketing text.

PUTTING IT INTO PRACTICE: This modification will likely have minimal impact on most companies who conduct marketing text campaigns. It serves as a reminder, however, to check your consent process, especially if you are working with a vendor for number acquisitions.

Ring, Ring, it's the FCC Calling – TracFone to Pay $16M to Settle FCC Investigation

Posted August 1, 2024

TracFone, the pre-paid phone company, recently settled with the FCC over allegations that the company failed to protect customer information during three different data incidents. According to the FCC, in each of the incidents, threat actors gained access to customer information, including names, addresses, and features to which customers had subscribed. The threat actors were able to gain access by exploiting vulnerabilities in the customer-facing application programming interfaces or APIs.

TracFone reported the initial breach to the FCC in January 2022. It then experienced two additional breaches, of which it notified the FCC in December 2022 and January 2023. (These notices occurred before the recent changes to the FCC's data breach notification rule.) In both incidents, threat actors again exploited API vulnerabilities, and used those vulnerabilities accessed users' order information.

The FCC alleged that the incidents occurred because TracFone did not have adequate security measures in place, in violation of FCC's rules for telecommunication carriers. As part of the settlement, TracFone has agreed to:

- Develop both a compliance plan and security program to ensure future compliance with FCC security requirements which shall be memorialized in a "Compliance Manual" available to both internal employees and third parties with whom the company contracts;
- Designate a compliance officer and train employees annually on safeguarding data in ways specific to their roles and responsibilities;
- Develop and adopt policies and procedures around access controls consistent with NIST and OWASP, and keep those policies and procedures current to any future NIST and OWASP measures;
- Adopt other security measures and processes, including for data transmitted online, around logging and monitoring, patch and security update management, and risk assessments;
- Have an assessment of its security program conducted every other year by external auditors (and internally review it each year);
- File with the FCC a compliance report six months and then 12 months after the effective date of the settlement, and ten annually thereafter for a period of three years.

PUTTING IT INTO PRACTICE: This settlement is a reminder that regulators may look closely after an incident at a company's security and compliance measures. The elements of this settlement, including access controls, risk assessments, and compliance monitoring suggest the types of procedures are expected.

A Wake-Up Call for Data Privacy in the Telecom Sector

Posted June 24, 2024

The FCC continues to take a more active role in privacy with its enforcement of the customer propriety network information ("CPNI") regulations. Recently, the FCC released Forfeiture Orders against the three largest mobile network operators for failing to safeguard CPNI. As we wrote about in our sister blog, violating FCC CPNI rules came with the cost of $57.3 million, $46.9 million, $12.2 million, and $80.1 million in fines to AT&T, Verizon, Sprint, and T-Mobile respectively.

CPNI is defined to include location information made available to the carrier by the carrier-customer relationship. Carriers are required to protect the confidentiality of CPNI and generally, may only share CPNI with customers' affirmative, express consent.

The FCC found the carriers ran afoul of this opt-in requirement by selling access to their customers' location information to companies known as location information aggregators. These location information aggregators then resold access to such information to third-party location-based service providers, or, in some cases, to intermediaries who went on to resell such information to location-based service providers.

PUTTING IT INTO PRACTICE: This case is a reminder for carriers to look at their agreements with entities to whom they give access to CPNI, and ensure that there are obligations to for the other party to comply with CPNI regulations.

AI-Generated Voice Calls: New Tech, Old Rules

Posted February 27, 2024

The FCC reminded companies this month that calls containing "artificial or prerecorded voices" are regulated by TCPA. And, that the FCC considers AI-generated voices to be just the kind of "artificial" that fall within the TCPA's regulations. This announcement was made in a declaratory ruling issued by the FCC at the start of the month.

As a refresher, under TCPA, *inter alia*, companies must (unless certain exceptions apply):

- Have prior express consent to make calls to residential and cell phones that include an artificial voice.
- Have prior express written consent to make marketing calls to residential and cell phones that include an artificial voice.
- Exceptions to these requirements include if the call is an emergency call, among other things.

PUTTING IT INTO PRACTICE: While it received a fair amount of publicity, this ruling should not come as a surprise. Voices created by artificial intelligence are as the term implies "artificial," and thus it makes sense that the FCC will include consider them as such under the TCPA.

CONSUMER PRIVACY

Click! FTC Updates Its Negative Option Rule

Posted November 19, 2024

The FTC updated its Negative Option Rule last month and gave it a new name to emphasize the expanded scope of programs to which it applies. It will now be the "Rule Concerning Recurring Subscriptions and Other Negative Option Programs." The updated rule, as the FTC outlines, will now be applicable to nearly all forms of negative option marketing.

While not necessarily a "privacy law," it is one that is normally on privacy practitioners' radar, as it impacts disclosures made at the time of collecting personal information. The modifications will have a rolling effective date, between December 15, 2024 (for provisions related to misrepresentations) and April 14, 2025 (for most remaining provisions). Some things for companies to keep in mind:

- **Scope of coverage expanded:** The FTC divides negative option programs into four categories: (1) prenotification plans; (2) continuity plans; (3) automatic renewals; and (4) free trial conversion offers. The new rule applies to all forms of negative options plans. Unlike the original rule, which applied more narrowly prenotification plans for the sale of goods.
- **Expanded transparency obligations**: Under the current rule, promotional information about the negative option feature must disclose the material terms of the plan. The new rules take this transparency requirement and applies it to the cancellation process as well. Additionally, the new rule prohibits businesses from misrepresenting any material facts about any goods or services with a negative option feature. Finally, under the new rule, marketing information cannot misrepresent any of the subscriptions features such as how to cancel or cost.
- **More notice about how the program works:** Under the current rule and as revised, companies are required to disclose the deal's material terms clearly and conspicuously to subscribers. Similar requirements exist at a state level. The new rule adds more specific requirements. Companies must now disclose any information about the subscription that may influence a customer's decision to sign up. For example, companies must disclose material terms of the deal before receiving customers' billing information. They will also need to notify them that they must act to stop charges and the deadline for doing so. (This mirrors requirements that exist for renewal disclosures at a state level.)

- **Changes to consent process:** Under the current rule, subscribers have to agree to the negative option plan before receiving an invoice and delivery of merchandise. As revised, companies will need to obtain customers' express proof of consent to the negative option feature before charging them. This mirrors similar requirements at a state level. They should keep proof of their consent for at least three years.
- **"Click-to-cancel" requirement:** Under the current rule, businesses must allow individuals to cancel negative option membership at any time. The new rule includes a "click-to-cancel" requirement. Namely, business must now provide to consumers a "fast and easy" method of cancellation. Depending on how someone signed up, the cancellation mechanism might be in person, by phone, or online. If a cancellation method is provided online, it must be easy to find. Cancellation should be as easy as signing up and carried out in the same medium.

PUTTING IT INTO PRACTICE: While the basic concept for negative option programs remains the same, the new rules do introduce some procedural changes. Companies who offer these programs should keep them in mind, including the "click to cancel" requirement for which the new rule has been named.

Malaysia In Process of Updating Its Privacy Law

Posted September 24, 2024

Malaysia is in the process of updating its Personal Data Protection Act to align more closely with laws in other jurisdictions. The law was originally passed in 2010 and then modified this year. As part of the modification process, the country's Personal Data Protection Department (PDPD) sought input at the end of the summer on different areas of the newly revised law. Included in the request for input was the breach notification process, DPOs, and data portability. The time frame for input ended at the beginning of this month, and we thus expect to see more direction on these points in the near future.

Changes to Breach Notice Process

The first area for which the PDPD sought input was on data breach notifications. The law as revised will impose a new notification obligation. In particular, there will be a mandatory obligation to notify the Personal Data Protection Commissioner in the event of a breach. The PDPD sought input on when that notice would need to be made and the time frame for the notice. In particular, it proposed that the commissioner notice happen only when the breach is of significant scale or will cause significant harm. And, that notice be made 72 hours after a company becomes aware of a breach. It also asked for input on the template form used to notify the commissioner and whether notice to individuals could go by email. And, what the timing should be for individual notice.

Changes to DPO Appointment

The second area that the PDPD sought input was on the new data protection officer obligations. While the law currently does not require a DPO, as amended, companies engaging in "large-scale" processing will need have a DPO. Among other things, the PDPD sought input on whether "large-scale" processing should be an express number or based on certain factors, and what qualifications the DPO should hold.

Changes to Data Portability Obligations

The third area that the department sought input was on data portability, a new right under the Malaysian privacy law. As amended, individuals will be able to ask companies to send their data to third parties. The PDPD wanted to know if those requests should be honored even if companies have technical challenges. It also wanted input on the types of information subject to these requests (like inferred data) and the time period of requested data.

PUTTING IT INTO PRACTICE: The changes to the privacy law in Malaysia are a reminder for global companies to have a process in place to (1) monitor for local law developments and (2) take an adaptable approach to privacy programs and privacy compliance. We expect to see ongoing updates to existing laws -like this one in Malaysia- at the same time that legislators around the world implement new laws.

Brazil's Data Protection Authority Issues Rules Clarifying Data Transfers

Posted September 20, 2024

Wondering what the requirements are for transferring personal information out of Brazil? Under the country's Data Protection Law, extra-territorial transfers of personal information are regulated in much the same way as in EU Member States. Parties can transfer personal information from Brazil to a third country only in limited circumstances. This includes, among other scenarios, if the entity receiving the information is located in a country that has been deemed adequate or if the parties put in place approved standard contractual clauses.

There have been questions for both of these, which were recently addressed through rulemaking by the Brazilian data protection authority:

- **Adequacy:** Currently, no country has been deemed adequate, although Brazil is working with the EU to establish that the EU's privacy laws meet the adequacy level. Similarly, the EU is working to recognize Brazil's law as adequate. Under the new rules, to make the process run more smoothly, the data protection authority (ANPD) has set out the criteria to assess if another region's privacy law should be found adequate.
- **Standard Contractual Clauses:** Until there are adequacy decisions, those wishing to export personal data out of Brazil will need to rely on other measures. Those other measures include standard contractual clauses or SCCs. These were also addressed in the new rulemaking. The rules include a set of approved SCCs. In addition, the rules contemplate using SCCs that differ from the approved set. Companies who wish to rely on SCCs will have until August 2025 to put sufficient ones in place.

In addition to adequacy decisions and SCCs, the rules address other questions and issues that have arisen relating to cross-border transfers. This includes providing -upon a data subject's request- a copy of the contract that was relied on for making the transfer of information.

PUTTING IT INTO PRACTICE: For those who wish to rely on SCCs for data transfers from Brazil, companies will have until August 2025 to put them in place. These might mirror SCCs being used for other jurisdictions, and we expect to see more clarification from the ANPD on this point. We also anticipate seeing more countries receiving "adequacy" decisions from Brazil in the near future.

NY AG Releases Website Privacy Guides for Businesses and Consumers

Posted August 22, 2024

New York Attorney General Letitia James recently released guidance for businesses and consumers about website tracking technologies. The consumer guide provided examples of common cookies, tracking technologies, and how consumers can manage both. The business guide lists steps the AG expects companies to take to avoid misleading or deceiving consumers in violation of New York's deceptive trade practices law.

The guides include concerns the AG's office had with websites' use of tracking tools. Included in these were mis-categorizing tracking tools in such a way that consumers' choices might not get honored. For example, labeling a cookie as essential -even if it is not. This resulted, the AG noted, in not letting a consumer opt out of it through a cookie preference tool. Another concern was offering tracking choices to all visitors, but then only honoring the choices from consumers in certain geographic locations (California or Connecticut for example). Also of concern to the AG was using tracking tools over which consumers could not exercise choices through common third-party management tools.

In each of the above scenarios, the AG alleged that these practices would be misleading or deceptive. The business guide suggests several strategies it expects companies to take:

- Designate someone with appropriate training to oversee tracking technologies
- Investigate data collection processes of new tech and tools carefully
- Configure tags and tools properly and test them to ensure they respect consumer choices
- Offer cookies and other tools to consumers in an accurate, clear manner to avoid misleading or confusing consumers.
- Avoid language that might lead consumers to accept a less privacy-protective option
- Pay attention to the design of the website and how choices are offered to avoid dark patterns, also a topic of concern for regulators
- Review tools, tags, cookies on a regular basis to understand how they operate and what data they collect.
- Theses guides are part of ongoing consumer protection efforts from the NY AG's office. In April 2023, the AG's Office released a data security guide to help businesses protect consumer information. This followed the release of a business guide for credential stuffing attacks. While there is no comprehensive state privacy law in New York, this guide indicates that the AG plans to enforce online cookie practices.

PUTTING IT INTO PRACTICE: The guide gives companies insight into what AG expects from companies who are engaging in online tracking. It also gives a perspective to companies as they review their cookie programs of what the NY AG might consider deceptive or misleading in this space.

#Hashtag Hashing: Still Not as Helpful as You Think!

Posted July 29, 2024

In a recent blog post, the FTC again cautioned entities that hashing data does not make that data anonymous. Hashing is a process that takes a particular input, such as a phone number or email address, and uses a mathematical formula to create a different output. However, hashing does not make the output "anonymized" from the FTC's perspective. This is because the hashing can be undone and reveal information that was initially obscured.

The Agency first highlighted its views on "hashing" in 2012. Since then, the FTC has brought enforcement actions against companies that have made statements about data use and collection practices that relate to hashing. For instance, if a company that sells hashed information states in their privacy policy that they do not share or sell personal information with third parties because they believe hashed information is no longer identifiable, that company could face allegations of unfair or deceptive trade practices under the FTC's Section 5 authority as the FTC takes the perspective that the hashed information is, in fact, still identifiable.

According to the FTC, although hashing may facially appear to conceal personal information, it still creates a unique identifier that corresponds to the initial input. This means that hashed information still has the ability to be tied to a particular individual. Sharing hashed information does not provide users with meaningful anonymity. Companies that utilize hashing believing it "anonymizes" or reduces the data's sensitivity may face scrutiny if they make certain claims to the contrary about their data sharing practices.

PUTTING IT INTO PRACTICE: The FTC's position on "hashing" is not new. That said, the renewed statements in this blog signals the Agency's likely upcoming focus on enforcing against businesses that use persistent unique identifiers in serving targeted advertising but nevertheless make statements that only "non-identifiable data" is shared. Companies that share hashed information or use other unique ID's should do their diligence to ensure public-facing statements are consistent with practices.

Mid-Year Recap: Think Beyond US State Laws!

Posted May 29, 2024

Much of the focus on US privacy has been US state laws, and the potential of a federal privacy law. This focus can lead one to forget, however, that US privacy and data security law follows a patchwork approach both at a state level and a federal level. "Comprehensive" privacy laws are thus only one piece of the puzzle. There are federal and state privacy and security laws that apply based on a company's (1) industry (financial services, health care, telecommunications, gaming, etc.), (2) activity (making calls, sending emails, collecting information at point of purchase, etc.), and (3) the type of individual from whom information is being collected (children, students, employees, etc.). There have been developments this year in each of these areas.

On the industry law, there has been activity focused on data brokers, those in the health space, and for those that sell motor vehicles. The FTC has focused on the activities of data brokers this year, beginning the year with a settlement with lead-generation company Response Tree. It also settled with X-Mode Social over the company's collection and use of sensitive information. There have also been ongoing regulation and scrutiny of companies in the health space, including HHS's new AI transparency rule. Finally, in this area is a new law in Utah, with a Motor Vehicle Data Protection Act applicable to data systems used by car dealers to house consumer information.

On the activity side, there has been less news, although in this area the "activity" of protecting information (or failing to do so) has continued to receive regulatory focus. This includes the SEC's new cybersecurity reporting obligations for public companies, as well as minor modifications to Utah's data breach notification law.

Finally, there have been new laws directed to particular individuals. In particular, laws intended to protect children. These include social media laws in Florida and Utah, effective January 1, 2025 and October 1, 2024 respectively. These are similar to attempts to regulate social media's collection of information from children in Arkansas, California, Ohio and Texas, but the drafters hope sufficiently different to survive challenges currently being faced by those laws. The FTC is also exploring updates to its decades' old Children's Online Privacy Protection Act.

PUTTING IT INTO PRACTICE: As we approach the mid-point of the year, now is a good time to look back at privacy developments over the past six months. There have been many developments in the privacy patchwork, and companies may want to take the time now to ensure that their privacy programs have incorporated and addressed those laws' obligations.

DATA BREACH

New Data Breach Notification Obligations for PA – and a New Reporting Portal

Posted September 17, 2024

Pennsylvania AG Michelle Henry announced yesterday the launch of an online portal for businesses to report data breaches to the AG's office. The portal launch comes before Pennsylvania's new breach amendments take effect on September 26, 2024. One of the amendments will require businesses to report to the AG Office any breach that impacts more than 500 Pennsylvania residents. Businesses can provide notice to the AG using the new online portal. The law also includes specific reporting content; this content is built into the online portal. The AG's website provides step-by-step instructions for submission.

As a reminder, from September 26, if a breach involves social security numbers, bank account numbers, or drivers' license/state ID numbers, then businesses will need to provide 12 months credit monitoring under the law as revised. Businesses will also have to provide impacted individuals with access to a free credit report, if they could not otherwise get free access. And similar to other states, the threshold for notify credit reporting agencies will be if the breach impacts 500 or more Pennsylvania residents.

PUTTING IT INTO PRACTICE: There are a growing number of states authorities that have web portals for submitting notices of breaches. For those who keep a running list, this new portal will get added to it. Given the frequency of updates in this area, companies who do keep this information in an appendix to their incident response plan will want to have a process in place to confirm that the list is current at the time of the incident.

Indiana Amends Breach Notification Law Along with New Adult Website Verification Requirement

Posted July 23, 2024

Indiana recently amended its breach notification law to include as personal information age verification information collected by adult websites. At the same time, the state passed a new law for adult websites. The law required that these sites use a "reasonable" method to verify users' ages. The law also creates a private right of action for parents of minors who access the sites. The law has been blocked, however, by a lawsuit arguing it violates First Amendment.

PUTTING IT INTO PRACTICE: This amendment, although not challenged along with the age verification law, will have limited impact. Not only does it apply only to adult websites, but it applies to information that they are not currently collecting. It does show, however, that states continue to tweak their data breach notification laws.

Keystone State Tweaks its Data Breach Notification Law Again

Posted July 22, 2024

In what may become an annual tradition, Pennsylvania has amended its breach notification law. The new provisions will take effect on September 26, 2024. As a reminder, Pennsylvania changed its law last year to expand the definition of "personal information" and to create exemptions for HIPAA-regulated entities.

The changes this year are more extensive, bringing the law into closer alignment with other state data breach notification laws. There are several changes to note:

- **Thresholds:** If a breach impacts more than 500 Pennsylvania residents, the Attorney General must be notified. Companies must send such notice concurrently with individual notices. If the breach impacts 500 individuals, then notice must be made to credit reporting agencies (the previous threshold was 1,000).
- **AG Notice Contents:** Beginning in September, Pennsylvania will join many other states in requiring companies to include specific content in the notice to the AG. This includes the organization's name and location, as well as the date of the breach and a summary of the incident. The notice must also include an estimate of the total number of impacted individuals, and number of impacted Pennsylvania residents.
- **Credit Monitoring**: If the breach involves social security numbers, bank account numbers, or drivers' license/state ID numbers, then companies will need to provide 12 months credit monitoring. Additionally, companies will need in these circumstances to give impacted individuals access to a free credit report, if they could not otherwise get free access.
- **Personal Information**: As a reminder, the 2023 amendments added "medical information" to the definition of personal information, that, if breached, would trigger a duty to notify. That definition is now narrowed to be only medical information held by a state agency or its contractor.

PUTTING IT INTO PRACTICE: Pennsylvania amended law serves as reminder to review incident response plans. To the extent they list with specificity timing or content requirements, ensure that they address these new developments.

Impact of Tennessee's Cybersecurity Class Action Safe Harbor

Posted June 25, 2024

Tennessee has joined a handful of other states to provide certain safe harbors in the cybersecurity realm. Unlike others, the law sites beside -but does not modify- the states' data breach notification law. Also unlike others, the safe harbor is very narrowly tailored, and is not triggered by having a data security program.

Under the new law, companies are not liable in class action suits that arise from a "cybersecurity event." The term is defined similarly to that used by the SEC when describing public entities 8K filing obligations. Namely, an event that arises from unauthorized access or misuse of either an "information system" or "non-public" information stored on that system.

Non-public information is defined to include elements like social security numbers, drivers' license numbers, and financial account numbers, mirroring the state's breach notice law. It also includes, though, "biometric records," an element not found in the breach notice law.

There is an exception to this safe harbor. It does not apply if the event was caused by a company's "willful and wanton misconduct or gross negligence." Terms that are not defined under the act.

PUTTING IT INTO PRACTICE: Given the carve out to this shield, and its limited jurisdiction (in Tennessee and not across the US), it is not clear if it will afford broad protections to companies. However, it may be the start of a trend that we might find in other states over the coming months.

Utah Breach Notice Law Amended, Effective May 1

Posted April 22, 2024

Utah, among other privacy laws it has enacted or modified recently, has also modified its breach notification law. This follows last year's changes to the law, which among other things codified the state's Cyber Center.

This year's modifications are primarily administrative. The law will now include a definition of "data breach" specifically for purposes of reporting to the Cyber Center (which definition mirrors the breach definition already in the law). Additionally, the law now affirmatively states that the notification submitted to the Cyber Center as well as information submitted to the Center or the Attorney General will be confidential. (If submitted to the Utah Cyber Center following existing Utah's process for making confidentiality claims).

The law has also been amended to list the specific information which must be provided to the Cyber Center. The list is similar to the information which other agencies who receive notices require, including the date the breach occurred and the date of discovery. Also required is the number of people impacted, including those impacted in Utah and the type of information impacted. Also required is the submission of a short description of the incident.

PUTTING IT INTO PRACTICE: Updating its breach notice law seems to be an annual occurrence for Utah. These changes are not significantly different from obligations under other states' laws. Come May 1, companies will want to keep track of these procedures for incidents that trigger Utah reporting requirements.

Operator? I'd like to Report a Data Breach—The FCC's Updated Data Breach Rule

Posted January 11, 2024

After waiting 16 years for a call, the FCC is finally back on the line. Last month the FCC updated their 16-year-old data breach notification rule. The updated rule makes drastic changes to the previous FCC notification requirements. However, many will already be familiar with the new requirements as they merge those found in state data breach notification laws in to the FCC context. Regulators may have felt wired to make these change in light of the new SEC rules, about which we have also previously written, that went into effect last month. Regardless of their motives, the FCC determined that the line had been ringing to for too long and it was time to pick up where they had left off 16 years ago.

As with the previous rule, the update applies to providers of telecommunications, interconnected Voice over IP, and telecommunications relay services. Updates to the rule include:

- The elimination of the mandatory waiting period prior to notification.
- Breaches must be reported to the commission and law enforcement within 7 days.
- Breaches that impact less than 500 individuals and where there is no reasonable likelihood of harm to individuals may be reported annually.
- Impacted individuals must be notified without unreasonable delay after notification to the commission and law enforcement, but no later than 30 days after the determination of a breach.
- Individual notification is not required if there is no reasonable likelihood of harm or if the data was encrypted and the encryption key was not impacted.
- Expanded definition of triggering information to include all personally identifiable information, including social security numbers and financial information.
- Expanded definition of breach to include inadvertent access, use, or disclosure, but the definition includes a good faith exception similar to those found in various state data breach notification laws.

PUTTING IT INTO PRACTICE: Providers must not let this call go to voicemail. It is time stay dialed in, review the updated regulations carefully, and update policies and procedures to ensure compliance. This is one call you don't want to miss.

DATA BROKER

New Program Under Biden Executive Order to Prevent Access to American's Sensitive Personal Data by Foreign Actors

Posted April 24, 2024

The Biden Administration recently issued an Executive Order aimed at protecting American's sensitive information and certain US Government data from threats posed by foreign actors. Of note is the Order's focus on data brokers that may share data in bulk with foreign entities and/or individuals.

Following issuance of the Executive Order, the Department of Justice (DOJ) issued a notice outlining its future program under the Order, which identifies data-brokerage transactions involving bulk US sensitive personal data or certain government data as one of two types of "prohibited transactions." (The other is transactions that provide certain foreign actors with bulk human genomic or human biospecimens.) DOJ will release proposed rules for the program that will be open for public comment.

For restricted transactions – identified so far as vendor agreements, employment agreements, and investment agreements involving bulk data or government-related data – US entities will need to implement specific security requirements. These will be determined as part of DOJ's program.

The new materials identify six categories of bulk US sensitive personal data that may trigger the new restrictions: (1) covered personal identifiers (the notice provides a list of identifiers such as SSN, financial account numbers, etc.); (2) personal financial data; (3) personal health data; (4) precise geolocation data; (5) biometric identifiers; and (6) human genomic data. DOJ is also considering a risk-based approach to defining *bulk* data, with different thresholds for different types of data. For example, human genomic data of more than 1,000 U.S. persons poses a high risk while personal financial data for the same amount of people would pose a low risk. "Government-related data" covered under the program (regardless of volume or "bulk") includes geolocation data associated with military and sensitive facilities (to be included in a forthcoming Government-Related Location Data List) and certain sensitive personal data associated with current and former federal officials and contractors.

Importantly, DOJ says the program is not meant to broadly prohibit commercial transactions and it does not impose requirements to keep data within the US (although this may be required by other laws and regulations). The focus is on national security and imposing limits on certain transactions of particular concern.

PUTTING IT INTO PRACTICE: The practical implementation of the Executive Order is largely still unknown as critical definitions and parameters still need to go through rulemaking. However, companies should determine what personal data they collect on the American public and U.S. Government employees or contractors, and when and how they transfer that data to other parties. This will be especially relevant to anyone in the government contracting, healthcare, technology, financial, or life sciences spaces where the type of data handled by entities in those industries is a focus of this Executive Order.

FTC Continues Focus on Data Brokers and Sensitive Information

Posted January 9, 2024

The FTC is beginning 2024 with a bang. Just a few short days after announcing a settlement with lead-generation company Response Tree, the FTC has announced another decision. In this latest announcement, the FTC has described this as its first settlement with data broker over the sale of sensitive information. According to the FTC, X-Mode Social, and its successor company Outlogic, LLC, tracked and sold to third parties precise location information, which information could identify if people visited "sensitive" locations like medical or reproductive clinics or domestic abuse shelters. This allegation is similar to that the agency made last year against Kochava, in a case that is still pending.

According to the FTC, X-Mode licensed location data in two ways. First, the company would tie raw location data to a device's unique identifier (the Mobile Advertiser ID or MAID). That raw data could, according to the FTC, be matched to where a person physically visited. This included sensitive locations. X-Mode also licensed audience segments based on location, which location might show interest (examples the FTC gave in its complaint included "Size Inclusive Clothing Stores."). Information was gathered from consumers both through X-Mode's own apps (Drunk Mode and Walk Against Humanity) as well as through third party apps. According to the FTC, X-Mode incentivized those apps to include its tracking tools by "promising passive revenue."

Although Android phone users can elect to opt out of personalized ads, the FTC alleged that X-Mode nevertheless gathered information even if consumers had exercised this opt-out. The FTC also alleged that X-Mode was deceptive in how it described its use of information. In particular, that it did not fully disclose the company's activities. Although, for example, it said that it shared information with brands or online ad networks, it did not disclose that it sold information to the government for national security purposes. Also of concern to the FTC were allegedly deceptive disclosures about information practices made to the third parties who might include the company's tracking tools in their apps. This was particular important, the FTC noted, since most of the location information gathered by X-Mode was from these third parties.

In settling with the FTC, under the proposed order the company must, among other things, destroy previously collected information and implement fairly detailed processes and procedures for ensuring that sensitive location information is not sold. The company will also need to give people a "simple and easy-to-find way" of opting out of collection and use of location information. Similar to requirements under state privacy laws, the proposed order also requires that consumers be given information about how to get a list of the third parties with whom their information has been shared.

PUTTING IT INTO PRACTICE: This settlement announcement is yet another reminder that the FTC will be looking closely at information sharing and sale activities, especially when the information is sensitive in nature. With this in mind, for those companies purchasing information from third parties, it will be helpful to add privacy compliance to the diligence process.

DATA SECURITY

New York AG Settles EnforcemENT Action with ENT

Posted November 15, 2024

The New York Attorney General's Office recently settled with Albany ENT & Allergy Services over claims that the healthcare provider failed to protect over 200,000 consumers' private health information. The claims stem from two ransomware attacks in 2023. The AG argued that the company had violated New York's data security law, resulting in the incident. As part of the settlement, Albany ENT agreed to pay $2.75 million in civil penalties and to implement additional security measures.

Among other things, the company has agreed to the following:

- Maintain a comprehensive Information Security Program that includes sufficient measures to protect personal information.
- Appoint personnel responsible for monitoring the information security program.
- Get annual third-party assessments of its security practices and the effectiveness of the program.
- Implement additional security measures, including multifactor authentication on devices that remotely access data and installing critical security updates in a timely manner.
- Implement oversights for data security vendors.
- Have a written Incident Response plan with internal procedures if there is a reasonable suspicion of a breach.

PUTTING IT INTO PRACTICE: As we've seen before, conducting business without essential safeguards to PI is the easiest way to find your company in trouble with regulators. This settlement should remind businesses to proactively assess their comprehensive information security program and practices for compliance.

Amendments to NYDFS' Cybersecurity Regulations Take Effect November 1

Posted October 28, 2024

The New York Department of Financial Services has modified its cybersecurity requirements for regulated entities. These requirements are in addition to those included in the regulations as last updated in November of last year. The new requirements go into effect November 1, 2024. They modify several parts of the rule, including:

- **CISOs reporting requirements:** Under the current regulations, CISO must report on cybersecurity to the company's leadership. The revised regulations now require the report to include information about remediation plans. Separate from the annual report, the CISO will also need to report any material cybersecurity issues (like a breach) to senior officers.
- **New responsibilities for the senior governing body:** As revised, the regulations emphasize that the regulated entities' senior governing body is responsible for overseeing cybersecurity risk management. This includes understanding cybersecurity-related concepts. Senior leadership's obligations also include reviewing management reports about cybersecurity matters. And confirming that the company has devoted enough resources to implement an effective cybersecurity program.
- **Encrypt all nonpublic information:** The new amendments removed an exception for encrypting data that is in transit. Now, companies need to encrypt all nonpublic information being moved to external systems.
- **Update the incident response plan:** As amended, the regulations call for different content in regulated entities' incident response plan. This includes processes for responding to a cybersecurity event and how to recover from systems backups. IRPs will also need to have provisions for conducting root cause analyses of incidents.
- **Business continuity and disaster recovery plan:** As amended, the regulations clarify the requirements for disaster recovery plans. Among other things, the plans need to be in writing and identify all things necessary to continue operations during a cyber-related event. Provisions also need to be in place to train employees who implement both IRPs and the recovery plans.
- **New categories for exempted companies:** As revised, businesses with fewer than twenty employees or less than $7,500,000 in annual revenue over the past three years are afforded certain exemptions. This increases the previous 10 employee and $5,000,000 exemption levels. Businesses with less than $15,000,000 (instead of $10,000,000) in year-end total assets are exempt as well.

PUTTING IT INTO PRACTICE: Modifying its cybersecurity regulations may become a November tradition for NYDFS. Companies covered by the regulation should keep in mind these new obligations, especially on reporting and internal plans, when reviewing their cybersecurity programs.

Countdown to Compliance: The Department of Defense Finalizes Its Cybersecurity Program Rule

Posted October 25, 2024

The Department of Defense published the final version of its Cybersecurity Maturity Model Certification (CMMC) rule last week. This rule establishes the parameters of the program and timeline for implementation. A separate rule to finalize associated contract requirements is expected early to mid-next year. For a deep-dive into noteworthy takeaways for the Final Rule, see our analysis here. Here are some highlights:

As many know, the goal of the CMMC program is to strengthen cybersecurity across the Defense Industrial Base by implementing a framework to ensure contractors and subcontractors adequately protect sensitive unclassified information under Department of Defense contracts. The framework requires contractors to implement cybersecurity standards at various levels (Levels 1-3) depending on the sensitivity of the information they hold, and to undergo related assessments and provide affirmations regarding compliance.

Once contract requirements are finalized, implementation of the CMMC program will be spread out over four phases spanning three years. With very limited exceptions, all companies contracting with the Department of Defense and their service providers will be impacted by this program.

PUTTING IT INTO PRACTICE: To be in the best position to be prepared, impacted companies should focus now on CMMC compliance – if they have not already. They can do this by scoping and completing the required assessments, which can take time. Once CMMC requirements are applied to a solicitation, companies will be ineligible to receive contracts if they do not have the required CMMC compliance in place.

Camera Company Will Pay $2.95 Million to Settle Security Claims

Posted September 11, 2024

Verkada, a manufacturer and retailer of security cameras, has settled FTC accusations of lax security measures. The company sells its products to businesses, including schools and medical facilities. It markets its products as "plug and play:" the cameras connect to the cloud and allow customers' remote access into both live and archived video footage. Among other features, the cameras have a "people analytics" tool that lets users "search images through facial recognition or face-matching technology." A review of the settlement raises many reminders for companies about (1) security claims in privacy policies and marketing, (2) remediation concerns following a breach, (3) adherence to the Privacy Shield, and (4) a reminder about related (and often overlooked) laws like CAN-SPAM.

The Company's Marketing Practices and Security Claims

As part of its marketing, the company made a variety of security claims and had engaged in other marketing activities with which the FTC had concerns:

- It was both "HIPAA certified" and compliant with the EU US Privacy Shield;
- In its privacy policy it said "we take customer privacy seriously" and that it uses "industry-standard methods to keep [customer] information safe and secure;"
- In other materials it claimed that the product is "secure out of the box" and that the company "pull[s] out all the stops to ensure that your data is protected as it is transmitted over the network;"
- Employees and investors posted positive reviews without disclosing their affiliation with the company; and
- The company engaged in an aggressive email campaign marketing its products.

The Data Incidents and Remediation Recommendations

The FTC's investigation of the company followed two data breaches. The first was in December 2020. At the time, a threat actor was able to install malware in Verkada's AWS environment. According to the complaint, the company did not discover this for three weeks because of insufficient alert capabilities. As part of the incident, the company hired a forensic firm that recommended certain remediation measures. It then also hired a cybersecurity firm to provide recommendations, which recommended several remediation steps. These included improvements in monitoring and logging. According to the FTC, these recommendations were not implemented. In March 2021, another threat actor was able to infiltrate the system. This time, by accessing an administrative level account. In this second attack, hackers accessed live cameras and stole sensitive personal information of 115,000 customers. Through the live cameras, hackers watched hospital patients sleeping, children playing inside of a room, and prisoners in their cells.

The Settlement

The FTC argued that the company had engaged in multiple legal violations, including insufficient security measures as required by HIPAA and deceptive privacy claims in violation of Section 5 of the FTC Act. Deceptiveness violations included:

- Claiming that it was complying with the Privacy Shield program: although the program is no longer viewed as adequate by the EU, the FTC found the company needed to adhere to its requirements if it was making public statements that it was doing so; and
- Making misleading claims like the online reviews, and privacy policy and website statements about security.

Finally, the FTC also found the company had violated CAN-SPAM by, among other things, not including an opt-out mechanism or valid physical address. As part of the stipulated order, Verkada will not only pay an almost $3 million civil penalty. It has also agreed to, among other things, update its access controls and implement multi-factor authentication. It has also agreed perform an annual test of its systems and only engage with vendors who can adequately protect personal information. Verkada has also agree to submit certifications of security compliance to the Commission annually for twenty years.

PUTTING IT INTO PRACTICE: This case included many reminders for companies about FTC privacy and security risks and potential "hooks" that can be used in the event of a breach. Among these are promises made in privacy policies and marketing materials about security measures. Also of concern can be remediation recommendations that are not implemented, including following a data incident.

SEC Continues its Cybersecurity Focus, Settles with Company over Lax Security Measures

Posted August 28, 2024

The SEC recently issued an order and settlement against a company from a pair of cyberattacks in which millions of dollars of client funds were stolen. While the company was able to recover a portion of the funds and ultimately reimbursed clients for the money lost, the SEC still fined the company $850,000 for failure to provide the necessary safeguards to protect its clients' funds.

In both attacks, cyber criminals were able to transfer of large sums of money to external bank accounts. The first incident stemmed from a threat actor hijacking an existing email chain and pretending to be a client. The attacker then requested the issuance and liquidation of new shares to an external account. In the second incident, an attacker used stolen Social Security Numbers from an unknown source to create fake accounts and link to legitimate accounts even though other personal information attached to the accounts didn't match. In both instances, the attacker transferred funds out to external accounts.

The order highlights what the SEC expects when it comes to employee training and security protocols. Although the company had sent employees alerts about fraud and guidance on the importance of call-backs to verify requests and to pay attention to requesters' email addresses, the SEC found this to be insufficient. The SEC said that the company should've taken additional steps such as confirming that the warning email was read by employees, that training was provided, and to otherwise confirm that call-backs were in-fact being performed.

PUTTING IT INTO PRACTICE: This case servers as a reminder of the types of monitoring and measuring criteria regulators may expect when it comes to demonstrating that employees have been adequately trained. Copies of training materials or warning newsletters may no longer be enough. Regulators are more and more interested in how a company evaluates whether its cyber training is effective and how they are monitoring employee compliance.

Biotech Company Settles with Three State AGs Over Security Practices

Posted August 27, 2024

A biotech company recently settled with three AGs over allegations that it had failed to protect consumer information. According to the AGs of Connecticut, New York and New Jersey, this led to a 2023 data incident. The company, Enzo Biochem, agreed to pay a $4.5 million civil penalty and take several steps to modify its information security program. According to the three states, Enzo engaged a third party to conduct a risk assessment and analysis in 2021. The focus of the assessment was the company's compliance with the HIPAA Security Rule. The vendor identified several issues to remediate. They included encrypting PHI at rest on Enzo servers and desktops and implementing automated systems to detect network anomalies. They also recommended documenting policies and procedures and creating a formalized approach to potential risks. According to the AGs, these changes were not made.

In 2023 threat actors gained access to Enzo's systems. The threat actors accessed and exfiltrated 2.4 million patients' information. The information included social security numbers and medical treatment and diagnosis information. According to the AGs, the threat actors were able to move laterally throughout Enzo's systems using the login credentials of two administrator accounts. Those credentials were shared among five employees. In addition, one of those credentials had not been changed for ten years. The AGs alleged that the company had specific security failures that resulted in the breach.

As part of the settlement, Enzo agreed to document internal and external risks to personal information and to implement reasonable safeguards for information it holds. It also agreed to test its program annually and to use vendors who can adequately safeguard personal information. It has also agreed to harden its access controls, implement multi-factor authentication, and password management processes. Enzo also agreed to submit to a third party data security assessment, the results of which it agreed to provide to the NY AG. The company also agreed to implement a variety of policies and procedures, including an incident response plan. It will also retain and make documents required under the settlement available to the AGs for at least six years.

PUTTING IT INTO PRACTICE: The terms of this settlement, and the issues identified by the AGs in their assurance of discontinuance, highlight regulator expectations in the security space. These include identifying and documenting potential risks and having a process to address and remediate identified risks.

NIST Expands Cybersecurity Framework with Release of Version 2.0

Posted March 18, 2024

In its first major overhaul since 2014, the National Institute of Standards and Technology (NIST) updated its Cybersecurity Framework (CSF) on February 26, 2024. The updated 27-page CSF version 2.0 builds on version 1.1 and provides guidance to industry, government agencies, and other organizations on how to manage cybersecurity risks. While voluntary, the CSF has been a popular compliance resource within the private sector, both domestically and internationally, and has increasingly appeared in state and federal regulations as well as federal grants and grant incentive programs. The revised guidance, therefore, potentially has significant implications for organizations managing cybersecurity risks.

Version 2.0 is the result of a multiyear process reflecting discussion with and input from the public on how the CSF can better advise companies on how to identify, prevent, and recover from cyberattacks. Key developments in CSF 2.0 include:

- **Expanded audience.** While the prior CSF was primarily aimed at cybersecurity professionals working in organizations providing or supporting critical infrastructure like hospitals or power plants, CSF 2.0 is designed for all audiences regardless of sector, organization type, or cybersecurity sophistication. As such, 2.0 comes with a number of implementation examples and quick-start guides to better assist a diverse set of users in implementing NIST's cybersecurity recommendations.

- **Emphasis on governance.** CSF 2.0 increases emphasis on governance with a new "Govern" core function, augmenting the existing Identify, Protect, Detect, Respond, and Recover functions. Govern encompasses how organizations make and carry out informed decisions regarding cybersecurity as a component within an organization's broader enterprise risk management strategy.
- **New tools.** A suite of tools accompanies the updated framework intended to assist companies in implementing and customizing the CSF. For example, a new reference tool allows users to browse, search, and export data and details from the CSF's core guidance. A new searchable catalog contains informative references that show how an organization's current actions map onto the CSF, including the ability to cross-reference the CSF's guidance onto other cybersecurity documents.

PUTTING IT INTO PRACTICE: NIST intends to continue to update and enhance its resource to make the CSF as useful as possible to the broadest set of users. This will occur, in significant part, through community feedback and NIST hopes users will share their experiences and successes with NIST as they customize the CSF to fit their organizations.

Defense Department Outlines Its Future Cybersecurity Program

Posted January 25, 2024

The Department of Defense published a much-anticipated Proposed Rule at the end of last year for its Cybersecurity Maturity Model Certification program. The proposed rule is our first comprehensive look at the latest iteration of the CMMC program (referred to as CMMC 2.0), which will become effective once final changes are made to DoD regulations for contractors. The program attempts to streamline the various DoD cybersecurity requirements and provide greater flexibility in the certification process.

As many are aware, the CMMC program is the DoD's method to ensure that defense contractors and their service providers implement required cybersecurity measures. Under the program, companies will need to achieve a level of certification (either through self-assessment or third-party assessment) based on the sensitivity of the information related to the DoD program before they can receive contract awards.

CMMC 2.0 introduced a tiered model (with three levels). Under the proposed rule, there would also be a four-phase, 2.5 year approach for implementation of the program starting with the basic requirements and progressing to the most rigorous requirements. Once the program starts to take effect, companies will need to meet the requirements associated with the current phase and CMMC level associated with their contracts.

There is a 60-day comment period for the Proposed Rule, with comments due February 26, 2024. Comments can be submitted here. We expect there will be a significant number of comments submitted in response to the Proposed Rule. In conjunction with this proposed rule, DoD is also updating the DoD regulations for contractors through separate rulemaking, which is the trigger for the CMMC program taking effect. This creates uncertainty as to when program implementation will officially begin, but we anticipate the first phase of implementation could begin as early as late 2024, but more likely in 2025. For a more complete briefing please visit our recent blog post here.

PUTTING IT INTO PRACTICE: Given that the requirements for each CMMC Level are unlikely to change, defense contractors and companies that serve the defense industry should begin executing on their plans for how to implement the CMMC 2.0 obligations. Even outside the defense industry, the CMMC standards are worth reviewing. They may be a guidepost for best practices and inform data security requirements for companies in critical infrastructure and other sectors.

How Legitimate Is Your Business Interest? The EDPB Has Some Thoughts

Posted November 7, 2024

The European Data Protection Board issued draft guidelines last month that outline when processing can be considered done for "legitimate interest." The public has until November 20 to provide comments to the draft.

As most know, under GDPR, legitimate interest is one of the six legal bases for processing personal information. There has been some confusion about what might constitute a legitimate interest, though. And for the EDPB, fear that this has become a default selection companies select without sufficient thought or deliberation. Thus, these draft guidelines. In them, the EDPB provides a three-step approach to assess if a processing activity can be considered done for the company's legitimate interest.

1. **Establish that the use is legitimate**. The EDPB recognized that there is no definition of this term in GDPR. Noting that there can be no "exhaustive list," it gave three criteria for determining legitimacy: (a) the interest does not violate the law, (b) it is "clearly and precisely articulated," and (c) it is real and not speculative. Additionally, any legitimate interest must be related to the business; sharing information with law enforcement, for example, might not be a legitimate interest related to the business. That said, the legitimate interest could relate to the business or a third-party. In such cases, the legitimate interest must relate to the business and not to strictly community interests. Finally, the draft guidelines offer examples of processing for legitimate use. These examples include using information for marketing or ensuring that a website continues to function properly. Other "legitimate use" examples included product improvement or assessing someone's creditworthiness.
2. **Determine if the processing is "necessary" for the legitimate interest**. The draft guidelines reiterate that any processing in pursuit of legitimate interest must be strictly necessary to pursue that interest. It is not enough that the processing be "useful" to a business' legitimate interest – the processing must be "necessary." This means that a business must carefully consider the necessity of certain processing. If there are reasonable, less intrusive means of processing available, then the business cannot consider it necessary.
3. **Balance business interests against the interest of individuals.** Even if the first two criteria are met, a business' legitimate interest does not automatically override the interests of individuals. Before concluding that the basis can be one of legitimate interest, businesses must balance their interests against the interests of individuals. To make the assessment, businesses should consider the impact of the processing on individuals. Businesses should also consider the reasonable expectations of individuals. The goal is not to avoid any impact, but instead *disproportionate* impact. If this factor falls in favor of the individual business can pursue means to mitigate any processing impacts. Otherwise, the company cannot process the data based on Article 6 of the GDPR.

The draft guidelines also explain how businesses should conduct this assessment in specific contexts. These include direct marketing. Also included are fraud prevention and information security.

PUTTING IT INTO PRACTICE: These guidelines offer a roadmap for companies to assess if they can rely on 'legitimate interest" as their legal basis under GDPR. Included in the assessment is looking whether there were alternatives to the processing and that there is a real, and not speculative, need.

EU Cybersecurity Regulation Adopted, Impacts Connected Products

Posted October 22, 2024

The EU Regulation on horizontal cybersecurity requirements for products with digital elements, the so-called Cyber Resilience Act, has been officially adopted on 10 October 2024 and will be published in the EU's official journal in the coming weeks. This law will impose important obligations on manufacturers of connected products and those placing them onto the EU market. Implementation will begin in 2026 for certain portions of the law, and continue until 2027/2028 for some provisions. There are several elements for a company to keep in mind, which we have outlined below.

- **Why?:** The goal of the EU Cyber Resilience Act is to enhance the cybersecurity of products with digital elements ("PDE") by harmonising cybersecurity measures to be implemented throughout the supply chain and the products' lifecycle to reduce the increased risk of cyber threats affecting consumers, business and the public sector given the increased reliance on PDEs.
- **What?:**The Act introduces and harmonises EU-wide cybersecurity requirements for the design, development, production and making available on the market of PDEs. It applies to all products that are connected, directly or indirectly, to another device or to a network (e.g. home cameras, fridges, TVs, toys), with some exceptions, such as products for which EU cybersecurity requirements already exist (medical devices, aviation, cars) or military products. The Act only applies to economic operators in relation to PDEs supplied for the distribution or use in the EU market in the course of commercial activity. Software, including cloud as part of a product is covered by the Act but where software is provided as a service it is not covered by the Act but may be by the NIS 2 Directive. The Act does apply to radio equipment in scope of the Radio Equipment Directive 2014/53/EU.
- **Who?:** The Act creates obligations for manufacturers and, to a lesser extent, for authorised representatives, importers and distributors of PDE sold on the EU market.
- **When?:**The new regulation will enter into force 20 days after its publication in the EU's Official Journal and will apply 36 months after its entry into force, with some provisions to apply at an earlier stage. In particular, reporting obligations will apply 21 months after the entry into force of the Regulation.

Obligations

Manufacturers who wish to sell PDEs in the EU are subject to numerous obligations. They shall notably ensure that their products have been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Annex I of the Regulation. They shall also assess the cybersecurity risks of their PDEs, exercise due diligence when integrating components sourced from third parties into their PDE, and ensure that vulnerabilities of the PDE are handled effectively and in accordance with the vulnerability handling requirements for a support period of least 5 years after sale. The cybersecurity risk assessment shall be documented and updated during the support period, and will be part of the technical documentation the manufacturers have to draw up before placing the PDE on the market. They also have other transparency and reporting obligations, and shall, for example, notify the CSIRT (Computer Security Incident Response Team) designated as coordinator and ENISA (the European Union Agency for Cybersecurity) of any actively exploited vulnerability contained in the products that they become aware of.

Manufacturers will only be allowed to draw up the EU declaration of conformity and affix the mandatory CE marking on their PDE once they have demonstrated the compliance of their PDEs with the essential cybersecurity requirements by one of the conformity assessment procedures foreseen in the Regulation. Manufacturers shall keep the technical documentation and the EU declaration of conformity at the disposal of the market surveillance authorities for at lease 10 years after the placement of the PDE on the market.

Importers and distributors will also have to abide by the Regulation and place/make available on the market only products that comply with the essential cybersecurity requirements. Their obligations are less stringent but they may also be considered manufacturers in some cases, e.g. if they carry out a substantial modification of a product with digital element already placed on the market.

Risk-Based Approach

The EU Cyber Resilience Act categorises PDEs by risk. PDEs without critical cybersecurity risks are in the 'default' category and can be self-assessed by their manufacturer. Two categories of 'important' PDEs – Class I (e.g. identity management systems, standalone and embedded browsers, password managers, or smart home general purpose virtual assistants) and Class II (e.g. firewalls, intrusion detection, prevention systems, or tamper-resistant microprocessors)– are subject to more onerous requirements and can require third-party conformity assessments. In addition, critical products (i.e. hardware devices with security boxes, smart meter gateways within smart metering systems and other devices for advanced security purposes, and smartcards or similar devices) will be required to obtain a European cybersecurity certificate at assurance level at least "substantial" under a European cybersecurity certification scheme.

Essential Cybersecurity Requirements – Annex I of the Regulation

Essential cybersecurity requirements are numerous, and of two types; the requirements relating to the properties of products with digital elements and the vulnerability handling requirements. The latter concerns only manufacturers. The first type includes, based on a cybersecurity risk assessment undertaken by the manufacturer, the availability of the products on the market without known exploitable vulnerabilities, with a secure by default configuration (unless agreed with the business user for a tailor-made product), security updates to address vulnerabilities, protection from unauthorised access by appropriate control mechanisms, confidentiality, integrity and minimisation of processed data, limitation of attack surfaces, provision of security related information, etc.

The second type of requirements covers the identification and documentation of vulnerabilities and components contained in the targeted products, the treatment and remediation of vulnerabilities without delay, the effective and regular testing and review of the products' security, the implementation of a policy on coordinated vulnerability disclosure, etc.

Non-Compliant Products – Penalties

Failure to comply with the Regulation's obligations may result in administrative fines imposed by the competent national market surveillance authorities of up to between EUR 5 and 15 million or, if the offender is an undertaking, up to between 1% and 2,5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher, depending on the type of obligation. Withdrawal of the PDE from the EU market and a prohibition to sell can also be imposed by the national market surveillance authorities.

PUTTING IT INTO PRACTICE: Manufacturers are well advised to start conducting security risk assessments (with the different categories of products in mind, i.e. "regular", "important" and "critical" PDEs) of their connected products and identify any vulnerabilities. They should address these and start drafting the necessary technical documentation. At the same time manufacturers should start integrating the principles of safety by design into their product development process, taking into account the essential cybersecurity requirements set out in the Regulation, and put in place policies such as the mandatory one on coordinated vulnerability disclosure. In practice, reporting obligations will take effect in the course of 2026, and the other obligations incumbent on manufacturers will follow at the end of 2027/beginning of 2028.

ICO Has Concerns Over Facial Recognition Use

Posted March 25, 2024

Earlier this month the UK privacy office put a stop to several related entities' use of facial recognition technologies and fingerprint monitors for their employees. The UK Information Commissioner's Office found that the companies were using the tools to monitor attendance. However, the ICO felt that the companies could have used "less intrusive technologies" -like fobs or ID cards- to accomplish the same goals. In reaching its conclusion the ICO noted that employees were allegedly not given a meaningful choice, given the "imbalance of power" between the employer and the employee. And as such employees were made to feel, the ICO believed, that clocking in and out with facial recognition/fingerprint scanning was "a requirement in order to get paid."

This decision against Serco Leisure, Serco Jersey and its related entities shows a trend with data protection authorities in the employment monitoring space. The UK ICO, like many of its European counterparts, has issued a guidance on use of biometric recognition, which was released on the same day as the decision. In its guidance, the ICO outlines when and how companies can collect biometric information in compliance with UK privacy laws (and when they should not).

PUTTING IT INTO PRACTICE: We anticipate that there will be more decisions of this nature coming from other data protection authorities, if not the UK as well. Companies who are engaging in these practices will want to review guidance like that issued by the ICO to ensure that it is collecting and using biometric information appropriately.

EDPB Provides Guidance on Determining Primary Supervisory Authority

Posted February 27, 2024

This month the EDPB shed light on the question of lead supervisory authorities. The issue arose in response to a question late last month from the French supervisory authority. Some background. As most international organizations are aware, GDPR provides for a "lead" supervisory authority where companies have their "main establishment" in that location. In the event, for example, if an investigation into a company's violation of a particular provision of GDPR, the lead supervisory authority would be the sole authority to pursue the problem. This question can also come up when companies are trying to determine what authority to notify of a data breach. Without a lead supervisory authority, all supervisory authorities where there are data subjects would be able to participate.

The "lead supervisory authority" benefit has been referred to as the "one-stop-shop mechanism." As might be imagined, both companies and supervisory authorities have a strong interest in understanding how to establish if a company has a "lead" supervisory authority. This month the EDPB issued an opinion intended to guide supervisory authorities in how to decide if a multinational qualifies for a lead supervisory authority. Two key criteria must be met:

1. The operations in the EU country in question must be where the company makes decisions about the "purpose and means of processing" personal information.
2. That EU operation must have the power to implement those decisions.

The EDPB stated in its opinion that if decisions and power to implement the decisions are "exercised *outside of the [European] Union"* (emphasis added) then there can be no EU lead supervisory authority (opinion, executive summary). The burden of proof, the EDPB noted, is on the company, which must cooperate with the supervisory authority that is attempting to determine if it should be viewed as the "lead." While the existence of a regional headquarters in the country in question may suggest that the country is the lead, it is not dispositive evidence. The supervisory authority will still, the EDPB clarified, still need to look at the full evidence.

PUTTING IT INTO PRACTICE: This opinion, although reiterating what is already in GDPR itself (Art 4(16)(a)), demonstrates the EDPB's focus on supporting cooperation and streamlining between EU member state privacy authorities. Multinational companies, especially those with operations outside of the EU, should keep in mind the decision making and implementation criteria outlined in the EDPB's opinion.

UK ICO Uses AI In Cookie Banner Review

Posted February 7, 2024

The UK Information Commissioner's Office recently reported that it is continuing its review of website cookie banners. It had expressed concern late last year that these banners were not giving "fair choices" because they did not make it as easy for users to reject all advertising cookies as it was for users to accept all. The ICO reached out to 53 companies and has now indicated that it will be reaching out to more companies: 100 at a time. To conduct its review, it will run a hackathon this year to develop an AI tool to comb the web for "noncompliant" banners.

What does the ICO consider a noncompliant banner? In an August 2023 joint white paper with the Competition and Markets Authority, the entities cautioned companies against what it called "harmful nudges." These included cookie banners that encouraged users to accept cookies that were not strictly necessary. The example it gave was a banner with only the choices "cookie settings" and "accept."

PUTTING IT INTO PRACTICE: This announcement is a reminder for companies that operate in the UK and use tracking tools to assist with targeted advertising to review their cookie banners. The white paper contains many examples of what the ICO will view as a non-compliant banner.

CJEU Decision Will Have Impace on Potential Fine Setting Under GDPR

Posted January 17, 2024

The Court of Justice of the European Union (CJEU) clarified in two judgments in the last month of 2023 (Deutsche Wohnen, ECLI:EU:C:2023:950 [DW] and Nacionalinis visuomenės sveikatos centras, ECLI:EU:C:2023:949 [NVSC]) the conditions under which data protection authorities across the EU may impose fines on companies for violations of the GDPR. Specifically, when those violations were committed either by unidentifiable employees at a company (DW) or by third parties (NVSC).

The NVSC case arose in Lithuania, and concerned the development of a Covid-tracking app by a third-party vendor on behalf of the Lithuanian public health services. The dispute in DW related to the company's storage of information allegedly in violation of the GDPR. At issue in both cases were the extent to which the companies could be held responsible if infringements of GDPR had occurred, but a third party (NVSC) or unidentifiable employees (DW) engaged in the allegedly violating acts. Both cases involved interpretation of national law in light of the GDPR, and were thus referred by national courts to the CJEU.

By way of background for the DW matter, German law thus far, a corporation could only be fined if the bad acts of which it has been accused could be traced to wrongdoing of an identifiable individual. In contrast this is not a prerequisite, under the GDPR. The CJEU ruled that national law (in this case German law) cannot impose a stricter liability threshold than GDPR.

Additionally, the CJEU ruled that under the GDPR, there must be intention or negligence to be established on the part of the controller, in addition to a finding of infringement, for fines to be levied although a natural person does not need to be identified specifically.

With respect to the NVCS matter, the CJEU clarified the liability of controllers for actions of processors. In principle, controllers are liable for infringements of processors acting on their behalf. This does not, however, apply if the processor departs from the agreement in place with the controller.

In both cases, the CJEU noted that while Member States can design the administrative procedure leading to the imposition of a fine, the substantive conditions establishing liability are solely governed by GDPR. In reaching its decisions, the CJEU indicated that the maximum liability for assessing an administrative fine should be based on 4% of the total worldwide group turnover of the undertaking concerned. The concept of an undertaking is well known to European competition lawyers. An undertaking is the 'economic unit' encompassing all entities which form together a unitary organization of personal, tangible and intangible elements is well established.

The CJEU's findings confirm the view expressed by the European Data Protection Board in its Guidelines 04/2022 on the calculation of administrative fines under the GDPR. There, the Board supported the transposability of the competition law concept of undertaking, and the above-mentioned principles of employee conduct attributability already. It is noteworthy, though, that in the cases discussed in this article the CJEU stressed that the concept of undertaking is only relevant for determining the amount of the administrative fine. This begs the question if and to what extent the principle of parental liability, well-established for private enforcement of EU competition law, also applies to private actions for damages under the GDPR.

PUTTING IT INTO PRACTICE: The European rulings send a mixed message to data controllers and processors. The rejection of strict liability (irrespective of wrongdoing on the part of the controller) will come as a relief. While the clarification that fines might be as high as 4% of the global turnover of a corporate group is not surprising, even where the infringement was committed by a local subsidiary, this serves as a reminder that GDPR breaches can result in serious (financial) consequences and the European regulators have steadily increased the fines imposed since the coming into force of the GDPR.

HEALTHCARE PRIVACY

FTC Finalizes Breach Notification Rule Amendments Directed at Digital Health

Posted May 29, 2024

The FTC recently announced that it had finalized the changes to the Health Breach Notification Rule (HBNR). This is roughly one year later from when the proposed changes were first released and three years later from the Agency's initial "position statement" on the rule sparking controversy. The final changes clarify the scope of the rule to health apps and expands what must be told to consumers when notifying them of a breach. The updated rule goes into effect June 25, 2024.

Though enacted in 2009, the HBNR had not been enforced (or really even discussed) until 2021. The Rule as originally drafted was intended to apply narrowly to 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. With the Agency's increasing interest in health information not covered by HIPAA, HBNR resurfaced into discussions in 2021. In recent enforcement actions, the FTC has controversially asserted that HBNR could apply to health related browsing and usage data shared with advertising vendors without consent.

The finalized updated Rule incorporates changes to key definitions including "PHR identifiable health information"; "breach of security"; and "PHR related entity." Notably (though consistent with the proposed changes), a "breach" is more broadly defined to include not just data security breaches, but also intentional, but unauthorized disclosures and unauthorized *uses*. Commentary in the Final rule says that where data has been obtained for one legitimate purpose, but later used for a secondary purpose that was not originally authorized by the individual, that may be a "breach." While the FTC has long-held that secondary use of data may be "deceptive," (under FTC Section 5) classifying such activity as also a potential "breach" is new. The amended rule also adopts changes to the method and content for notice to consumers.

The unprecedented and expansive view taken by the FTC in this amendment was not issued unanimously. The Commissioners voted 3-2 to finalize the changes. In a dissenting statement, Holyoak and Ferguson that the HBNR final rule adopted by the FTC "exceeds the Commission's statutory authority, puts companies at risk of perpetual non-compliance, and opens the Commission to legal challenge that could undermine its institutional integrity."

PUTTING IT INTO PRACTICE: Companies not covered by HIPAA but that are collecting or providing mechanisms to track health related information should evaluate to what extent this law may apply. Data uses and data sharing activities (even with vendors) should be closely analyzed to confirm that there is evidence of authorization for such disclosures and uses in place. This is in addition to considering how the emerging state health privacy law landscape may apply.

Out in the Open: HHS's New AI Transparency Rules

Posted March 21, 2024

The Department of Health & Human Services through the Office of the National Coordinator for Health Information Technology recently updated the process for certification of health information technology. Some of the modifications are intended to address use of artificial intelligence in health IT systems. ONC's certification is required for certain programs, such as where the health IT will be used for Medicare and Medicaid Incentive programs. It is optional for others. Those who are already certified will need to update their certifications. Those seeking new certifications will be subject to the new process.

The certification process requires developers of health IT to demonstrate that their products satisfy certain criteria. The demonstration can be completed through documentation or through inspection which must be approved by the Office of the National Coordinator for Health Information Technology. The updated certification process applies to health IT systems that use predictive modeling to assist with decision making (often referred to as "DSIs"). In particular, those that use training data for that modeling. Of particular interest, companies that want to have their systems certified will need to demonstrate conformance to the appropriate criteria while also demonstrating that they:

- Have taken steps to ensure that users understand how the DSI works. As part of this, give users access to underlying information about the DSI's design and development.
- Conducted risk practice assessments on the health IT and publish a summary of these practices publicly.

If your health IT is already certified, you will need to update your product and certification to ensure they satisfy the new criteria. If you do not complete the necessary updates, you may forfeit certification. Looking ahead, developers of health IT incorporating predictive DSIs must comply with the updated criteria by the end of 2024. That said, the rule spaces out many of the other new requirements over a period of years.

PUTTING IT INTO PRACTICE: Developers that wish to secure certification should review these requirements to assess whether their products satisfy the new criteria or need to be adjusted. Developers that wish to maintain certification should review these requirements and start updating their certifications to avoid forfeiture.

The Landscape of GIPA in Illinois

Posted March 18, 2024

Class action litigation has exploded in cases involving violations of Illinois' Biometric Information Privacy Act ("BIPA"). Less known and litigated is Illinois's Genetic Information Privacy Act ("GIPA") – enacted in 1998. But recent trends may portend an increase in GIPA filings on the horizon.

The Illinois legislature enacted GIPA to enhance privacy protections prohibiting the unauthorized disclosure and use of Illinois residents' genetic information. Specifically, GIPA prohibits disclosure of the identity of any person subjected to a genetic test (or the genetic results) without the individual's written consent. GIPA also bars employers from soliciting, requesting, requiring or purchasing genetic testing or genetic information of a person or a family member of the person as a condition of employment. Persons "aggrieved" by a GIPA violation can sue to recover liquidated damages of $2,500 for each violation.

Illinois courts have increasingly looked to BIPA decisions as a guide for interpreting GIPA. This is not surprising considering their similarities. Both statutes protect individuals' privacy rights and entitle plaintiffs to liquidated damages so long as they are "aggrieved." GIPA requires entities to obtain a person's express written consent prior to requesting, disclosing, using or storing their genetic information. GIPA also incentivizes class actions. And indeed, Illinois courts have started to grant motions for class certification in GIPA cases. *See Melvin v. Sequencing, LLC*, 344 F.R.D. 231 (N.D. Ill. Aug. 3, 2023). These developments represent troublesome trends for GIPA defendants and mirror the Illinois courts' treatment of BIPA cases.

In short, GIPA and BIPA are statutory cousins. They present similar challenges to any entity that collects, uses, stores, solicits, or discloses individuals' sensitive personal information. To the extent a company obtains or otherwise handles an individual's genetic information or genetic testing results, GIPA compliance is imperative.

PUTTING IT INTO PRACTICE: GIPA's definitions of "genetic information," "genetic services" and "genetic test" have the same meaning ascribed to them under HIPAA, as specified in 45 C.F.R. 160.103. Also, defendants sued under GIPA should investigate whether the plaintiff's claim is subject to dismissal on a motion to compel arbitration.

PRIVACY MANAGEMENT

FTC Social Media Staff Report Suggests Enforcement Direction and Expectations

Posted October 21, 2024

The FTC's staff report summarizes how it views the operations of social media and video streaming companies. Of particular interest is the insight it gives into potential enforcement focus in the coming months, and into 2025. Of particular concern for the FTC in the report, issued last month, were the following:

1. The high volume of information collected from users, including in ways they may not expect;
2. Companies relying on advertising revenue that was based on use of that information;
3. Use of AI over which the FTC felt users did not have control; and
4. A gap in protection of teens (who are not subject to COPPA).

As part of its report, the FTC recommended changes in how social media companies collect and use personal information. Those recommendations stretched over five pages of the report and fell into four categories. Namely:

1. Minimizing what information is collected to that which is needed to provide the company's services. This recommendation also folded in concepts of data deletion and limits on information sharing.
2. Putting guardrails around targeted digital advertising. Especially, the FTC indicated, if the targeting is based on use of sensitive personal information.
3. Providing users with information about how automated decisions are being made. This would include not just transparency, the FTC indicated, but also having "more stringent testing and monitoring standards."
3. Using COPPA as a baseline in interactions with not only children under 13, but also as a model for interacting with teens.

The FTC also signaled in the report its support of federal privacy legislation that would (a) limit "surveillance" of users and (b) give consumers the type of rights that we are seeing passed at a state level.

PUTTING IT INTO PRACTICE: While this report was directed at social media companies, the FTC recommendations can be helpful for all entities. They signal the types of safeguards and restrictions that the agency is beginning to expect when companies are using large amounts of personal data, especially that of children and/or within automated decision-making tools like AI.

What Does an Adaptable Privacy Program Look Like?

Posted June 13, 2024

Privacy professionals know "adaptable" programs are important. But what does that really mean? What does it look like? And how do we create one? We know that with the never-ending list of new laws and modifications to existing laws, being adaptable is key. To say nothing of regulatory enforcement and class action exposure. The following are ideas to help create -or modify- your program to be adaptable in face of the constantly changing privacy patchwork.

1. Align With Corporate Mission

There is nothing worse than spending time, energy and funds on a privacy program, only to find leadership unwilling to fund or adopt it. Before beginning your work, think about your organization's underlying mission. How can the privacy program support that mission? If your program aligns with the needs of the organization, you are more likely to get leadership buy in, and sufficient personnel, technology, financial and other support to make the program a reality. Many tools exist for aligning your program with your corporation's mission, including Balanced Scorecard work from Robert Kaplan and David Norton.

2. Appropriately Identify and Categorize Risks

"Be prepared" has become a buzzword for regulators and legislators. There is a growing expectation from both legislators and regulators that the corporate world will identify and prepare for risks. However not all risks are alike. Some risks, as Robert Kaplan and Anette Mikes tell us, are unknowable and unexpected. These could be novel cyberattacks, or new laws that regulate activities in ways not previously seen. Policies alone may not prepare a company for these risks. Instead, think about how train teams to work together in new circumstances. Tabletops that focus on teamwork, rather than preparation for a particular fact pattern, can be helpful.

3. Don't Over-Engineer: Make it Strategic

Obviously, a privacy program will need to address the laws and legal risks. It will also need to take into account the growing and complex matrix of third parties with whom organizations work. However a strategic program does not necessarily have to take a scorched-earth approach. In fact, many have found this makes implementation impossible. Instead, an adaptable program addresses the organization's business needs and risks. It takes into account the changing nature of privacy and data security laws and risks and builds in mechanisms to review and revise. For example, frameworks against which new programs or processes can be audited. Or, personnel within different business units that serve as "champions" of privacy: both bubbling up concerns to central privacy teams and spreading knowledge about obligations to their business team constituents.

4. Customize to Your Organization

An adaptable privacy program is one that has been adapted to the company. While informed by external requirements and risks, it is also informed by internal activities. Privacy policies, for example, describe the *company's* activities. Data protection protocols protect the company against risks *it* faces. Additionally, the program includes a process for ensuring compliance with those processes and procedures. It is an implementable plan that avoids being overly aspirational. It is easily understandable by the business and thus one to which employees can adhere. A place to start might be a standard SWOT analysis, identifying gaps between the current program and the company's mission, as well as gaps in addressing risks facing the company. Those opportunities can then inform a list of remediations – including personnel and technology support.

5. Use Change Management: Celebrate Small Wins

Finally, an adaptable program takes into account not just written policies and procedures, but the personnel who will be implementing and following those documents. To the extent that the documents place new expectations or restrictions on individuals, these changes may be resisted. Privacy professionals would thus be well served to borrow pages from change management, thinking about the traditional "freeze, change, refreeze" triad from Karl Lewin. Or,

from John Kotter, create urgency, a coalition, a vision, an implementation army, remove barriers and importantly: celebrate small wins. This last can keep motivation going, especially when getting to the end, instituted change, is hard. Or, when as with privacy, once reaching the end, one needs to restart as the privacy patchwork has shifted!

PUTTING IT INTO PRACTICE: As the privacy patchwork continues to develop and shift, the need for adaptable programs becomes all the more critical. These five suggestions are based on both legal and regulatory risks. They are also informed by the teachings of change management, something privacy professionals might overlook when building their privacy program toolbox.

The Privacy Patchwork: Beyond US State "Comprehensive" Laws

Posted June 3, 2024

We've cautioned before about the danger of thinking only about US state "comprehensive" laws when looking to legal privacy and data security obligations in the United States. We've also mentioned that the US has a patchwork of privacy laws. That patchwork is found to a certain extent outside of the US as well. What laws exist in the patchwork that relate to a company's activities?

There are laws that apply when companies host websites, including the most well-known, the California Privacy Protection Act (CalOPPA). It has been in effect since July 2004, thus predating COPPA by 14 years. Then there are laws the apply if a company is collecting and using biometric identifiers, like Illinois' Biometric Information Privacy Act.

Companies are subject to specific laws both in the US and elsewhere when engaging in digital communications. These laws include the US federal laws TCPA and TCFAPA, as well as CAN-SPAM. Digital communication laws exist in countries as wide ranging as Australia, Canada, Morocco, and many others. Then we have laws that apply when collecting information during a credit card transaction, like the Song Beverly Credit Card Act (California).

PUTTING IT INTO PRACTICE: When assessing your company's obligations under privacy and data security laws, keep activity specific privacy laws in mind. Depending on what you are doing, and in what jurisdictions, you may have more obligations to address than simply those found in comprehensive privacy laws.

Sheppard Mullin Creates Privacy Law Resource Center

Posted March 19, 2024

Sheppard Mullin is pleased to announce the creation of its new Privacy Law Resource Center to help companies navigate the increasing complexity of privacy and data security laws. We know that companies are struggling to keep track of and address the myriad global obligations that may affect them. These tools are aimed to help.

The requirements facing companies go well beyond general privacy laws like those being passed by US states, or which exist around the globe (GDPR, for example). There are privacy and security laws at an entity level (health care, financial services), activity level (texting, online behavioral advertising), and those that protect types of individuals (children, employees). We hope that the resources in the new center help organize these vast and complex requirements.

The center features a variety of tools, including checklists addressing topics from data breaches to data protection agreements. It also houses an interactive US state comprehensive privacy law tracking tool. The tool organizes obligations under these laws, from their scope and exemptions to rights and choices.

PUTTING IT INTO PRACTICE: These resources are not intended to serve as legal advice, but instead as planning and preparation materials to help companies as they navigate through the ever-changing landscape of privacy and data security laws.

DPA 101: Do You Know Where Your Data Is?

Posted February 28, 2024

As more and more states enact laws that mirror aspects of GDPR, and as companies begin to get used to the EU's new standard contractual clauses, now may be a good opportunity for a refresh on data sharing agreements. As most in the privacy space are well aware, the laws in many states -and countries- call for certain oversight in these situations. And many require specific content to be included in contracts. What might you want to include in your contract roadmap?

First, assess what law(s) are in scope. This depends not only on where the parties are located and doing business, but also where those individuals whose information is being processed are located as well. The EU requires specific clauses to protect its member states' citizens under GDPR. California, Colorado, Connecticut, Utah, and Virginia have similar provisions (with other states coming into effect).

Second, understand the parties' relationship. Will they be deciding jointly how to use the information ("joint controllers")? Will both be making independent decisions ("controller-to-controller")? Will one party be telling the other what to do ("controller-processor")?

Joint controllers, controller-processor, or independent controllers to use EU terms. But before selecting terms, make sure you understand who is doing what with the information. Next, make sure to include the right provisions. We have laid out below a summary of considerations for three circumstances: (1) joint controllers; (2) independent controllers; and (3) controller-to-processor. Included below are both things contemplated under the various laws, as well as practical considerations to cover when contracting in these situations.

Joint Controllers and Independent Controllers:

- Think through and outline in the contract what each parties' role will be in processing information. Who is responsible for what? How will rights requests be processed?
- For contracts that involve transfer of data from the EU to non-EU locations, ensure that there are the appropriate mechanisms in place for that transfer. That might include additional provisions around security in the agreement.
- Address length of processing, obligations relating to use of information, and provisions for data security and confidentiality.
- Think through mechanisms for notice and other steps to take in the event of a data breach.
- The parties can be or will be providing services to the other party such that it might trigger other obligations (for example being a "service provider" "processor" or "third party"). As applicable, have the correct provisions from the next section been included and have the parties' roles and obligations otherwise been thought through.

Controller-Processor:

- Include clear instructions for what is processed and how. Include the purpose of processing and the type of information being processed. Also indicate how long information will be processed and the parties' specific obligations with respect to use of the information. Include in those obligations around data security and confidentiality.
- For contracts that involve transfer of data from the EU to non-EU locations (or outside of the UK or Switzerland), ensure that there are the appropriate mechanisms in place for that transfer. That might include additional provisions around security in the agreement.
- Make sure that the processor helps the controller comply with legal obligations. This includes assistance in responding to rights requests.
- Think through mechanisms for notice and other steps to take in the event of a data breach.

- Have the processor provide proof of compliance on reasonable request. Also address audits (whether conducted by the controller or an independent third party).
- Ensure that any subcontractors follow the requirements set out in the contract with the processor. Consider whether you want to approve each subcontractor in writing or allow for general authorization of subcontractors through the contract.
- When the contract ends, have the processor return or destroy information.

PUTTING IT INTO PRACTICE: When putting together a data processing agreement with a third party, think not just about the legal obligations under GDPR and the growing list of state laws- but also the practical. What content can be included to best protect the parties? Now is a perfect time for a DPA refresh.

Privacy Day 2024: A Look Back at Developments from 2023

Posted January 26, 2024

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. Our privacy team tracked these developments and more during 2023, and we have put together this complete resource that includes our summaries of all of the privacy law developments from 2023.

Following this year's privacy day (falling on Sunday), many will be reminding their organizations about the importance of privacy and cybersecurity in 2024 and beyond. We hope that this resource is a useful tool to help in your privacy and cybersecurity efforts. And for a look back, here are links to past year-in-review summaries: 2022, 2021, 2020, 2019 and 2018.

PUTTING IT INTO PRACTICE: Privacy day is an opportunity to look ahead to 2024 and prepare for upcoming potential issues and risks in the privacy and cybersecurity space. From increased data breaches, artificial intelligence, a focus on data brokers and information sale, health and children's privacy, and dark pattern enforcement, the coming year will likely be a busy one.

Current Status of US State Privacy Law Deluge: It's 2024, Do You Know Where Your Privacy Program's At?

Posted January 9, 2024

As we begin the new year, many are wondering whether the growing list of US state privacy laws apply to them, and if so, what steps they should take to address them. For companies that gather information from consumers, especially those that offer loyalty programs, collect sensitive information, or have cybersecurity risks, these laws may be top of mind. Even for others, these may be laws that are of concern. As you prepare your new year's resolutions -or how you will execute on them- having a centralized list of what the laws require might be helpful. So, a quick recap:

- **States With Laws**: There are five state laws in effect: California, Virginia, Colorado, Connecticut and Utah. Four more go into effect this year: Florida, Oregon, and Texas (July 1) and Montana (October 1). The remainder go into effect either in 2025 (Delaware and Iowa (January 1) and Tennessee (July 1). Finally, Indiana is set to go into effect January 1, 2026.
- **Applicability**: Just because you operate in these jurisdictions or collect information from those states' residents doesn't mean that the laws necessarily apply to your organization. For many, there are either a number of individuals and/or revenue threshold that apply. On a related front, companies will want to keep in mind the various exceptions that might apply. For example, in some states health care or financial services entities might be exempt from the state laws. And in most, the laws' obligations are limited to the treatment of consumer information (as opposed to employee information).

- **Notice:** If the laws do apply, then companies will need to keep in mind the laws' notice obligations. Most stringent in this regard may be California and Colorado, however don't overlook the obligations that exist in other states.
- **Rights and Choices:** Companies subject to these laws will need to provide consumers with "rights" (access, deletion, correction). The type of rights and process for providing them varies slightly on a state-by-state basis. On a related front, these laws require giving consumers choices beyond those that exist under other privacy laws (CAN-SPAM's opt-out obligation for emails, for example). This includes choices around information targeted advertising, information sale, sensitive information, and profiling. The laws also place specific obligations on companies that operate certain types of loyalty programs (that might be viewed as financial incentives).
- **Record Keeping:** The laws contain some record keeping requirements that companies will want to keep in mind. These include records of rights requests and in some circumstances, data protection assessment records. This latter for companies engaged in specific activities like selling data.
- **Vendor Contracts:** Those that engage third parties to collect personal information on their behalf, or share personal information with third parties, will need to keep in mind the states' contract requirements. States that have these obligations include not just California, but others like Connecticut, Utah and Virginia.

PUTTING IT INTO PRACTICE: As we begin the new year and set our year's resolutions, now may be a good time to add projects around state privacy law compliance. After you have determined whether or not your company is engaging in activity that brings these laws into scope, you will want to think about how you will comply with their requirements. From notice and choice to working with third parties, there are many practical items to keep in mind for your privacy programs in 2024.

US PRIVACY

FTC Keeps Sights on Data Brokers that Sell Sensitive Location Sites

Posted December 20, 2024

The Federal Trade Commission recently settled complaints against two data brokers over their handling of consumers' sensitive location information. The agency alleged that such practices constitute unfair practices. Under the settlement, both Gravy Analytics and Mobilewalla, agreed to stop using and selling sensitive consumer location data.

The FTC alleged that Gravy Analytics and its subsidiary Venntel unlawfully tracked and sold precise (and thus sensitive) location information about millions of consumers. The information, according to the FTC, could be used to track individuals to places of worship, medical facilities, and political rallies. Similar to the FTC's complaint against Kochava last year, the FTC argued that this constituted an unfair business practice and posed harm to consumers. In its complaint against Mobilewalla, the FTC argued that the data broker -which engaged in down-stream information collection as part of its digital advertising bidding exchange platforms- created audience segments based on visits to health clinics and places of worship. It did not, though, according to the FTC obtain consent directly from consumers, nor did it ensure that consumers were informed when their personal data was obtained. Among other things, the FTC pointed to the company's "failure" to review privacy notices of the third parties who provided it with consumer information (the information used to create the audience segments).

Both companies have agreed to stop selling sensitive location information and will remove sensitive locations from their data sets. Both have also agreed to create supplier assessment programs. These programs will verify whether consumers provided consent to the collection and use of their location data. They will also be developing methods to allow consumers to withdraw consent and delete their data. These mirror similar provisions from the FTC's settlement with X-Mode Social earlier this year.

PUTTING IT INTO PRACTICE: These FTC settlements are a reminder of several areas of focus for the FTC and many regulators. First, the concern with passive information collection generally. Second, a focus on collection and use of precise location data that can be used to identify someone's visits to "sensitive" venues like health clinics and places of worship. Third, expectations to understand business partners' information collection when using information they provide. Given that data brokers continue to be in regulator's sights, we anticipate that 2025 will continue to be a year focused on indirect data collection and data sharing.

Coming to a State Near You: 5 State Privacy Laws Take Effect in January 2025

Posted December 18, 2024

Are you ready for the next set of US state privacy laws going into effect? Delaware, Iowa, Nebraska, and New Hampshire are effective January 1, and New Jersey's law go into effect two weeks later (January 15).

These states will join California, Colorado, Connecticut, Florida, Montana, Oregon, Texas, Utah and Virginia as states with "comprehensive privacy laws." What should businesses do as the ball drops in 2024? An initial stop is our interactive tool that tracks the laws' obligations. Highlights are also listed below:

- **Review consumer notices**. For the most part, businesses' notice obligations mirror the obligations in other states. Each state requires businesses to provide notice to individuals about their information collection, use, and disclosure practices. There are some slight differences in content like, New Jersey's law requires businesses to include the date the notice was last updated.
- **Ensure that there are processes in place for consumer choices and rights**. Under the upcoming laws, consumers have a variety of familiar rights. These include the right of access, correction, deletion, and portability. Each state also prescribes a timeline for responding (all states require a response in 45 days, while New Jersey and Iowa allow 60 and 90 days, respectively). Additionally, the new state laws allow consumers to opt-out of certain digital advertising, something to keep in mind if your organization has been taking a jurisdiction-specific approach.
- **Update vendor contracts**. At this point, most businesses are familiar with contractual requirements for vendors. The new state laws don't add into the mix any unfamiliar provisions.

PUTTING IT INTO PRACTICE: When we return from the upcoming holidays, keep in mind that there will now be 14 US states with "comprehensive" laws in effect. Three more (Minnesota, Tennessee and Maryland) are already set to take effect in 2025, and three (Indiana, Kentucky, and Rhode Island) in 2026. We expect this number to grow, with more states passing similar laws next year.

California's Privacy Regulator Had a Busy November, Data Broker Edition: What Does It Mean for Businesses?

Posted December 13, 2024

In the fifth in our series of California developments, we turn to data broker obligations. There are two of note. First, the California privacy agency is moving forward Delete Act regulations it proposed earlier this year. (Its board voted to move regulations addressing data broker requirements to the Office of Administrative Law for review and approval last month.) Second, it announced an investigative sweep of compliance with the Act.

Delete Act Regulations

Under the Delete Act, a data broker is a business that "knowingly collects and sells" personal information about consumers with whom they do not have a direct relationship. The law, as many are aware, requires annual registration with the state (similar to laws in Texas, Oregon, and Vermont). There are exceptions, including for those who are governed by GLBA or an entity whose processing of information falls under HIPAA.

The Delete Act regulations, if approved, will become effective January 1, 2025. The rules set the annual data broker registration fee at $400. The rules also clarify that the obligation to register falls on any business that meets the data broker definition, "regardless of its status as a parent company or subsidiary of another business." As outlined in the rules, data brokers will not be removed from the registry but can provide updated contact information.

Agency Sweep

In advance of the next annual data broker registration deadline (January 31, 2025), the CPPA announced it will take "appropriate actions" against those who do not register. Appropriate actions could include a penalty of $200 per day plus administrative costs. In its announcement, the CPPA also reminded data brokers that they must do the following:

- Report if their collection of data includes personal information of children under 16, precise geolocation data, or reproductive healthcare data. Reproductive healthcare data defined in the proposed rules as including information searching for, buying or otherwise "interacting" with goods like contraception or fertility vitamins.
- Provide a link on the company's website that informs consumers of their rights under the California Consumer Privacy Act.
- Disclose the number of data deletion request they receive and the average response time.

What's Next?

California is planning to launch a Data Broker Requests and Opt-Out Platform ("DROP"). It will let consumers direct all data brokers to delete their personal information in a single request. Data brokers must then also delete the requestor's personal information every 45 days. DROP is supposed to be available in 2026. Beginning in 2028, the CPPA will require covered businesses to undergo an independent audit every three years to verify compliance.

PUTTING IT INTO PRACTICE: The draft rules provide a baseline for what to expect from the CPPA in these areas. The board expressed their intention to make significant changes to the draft rules during the formal rulemaking process. Companies should keep an eye out for these changes and submit any relevant comments to the CPPA for consideration.

California's Privacy Regulator Had a Busy November, Cybersecurity Audits and Insurance Edition: What Does It Mean for Businesses?

Posted December 12, 2024

In the fourth in our series of new CCPA regulations from California, we look at both cybersecurity audit obligations as well as the impact of the CCPA on the insurance industry.

Cybersecurity Audits

The proposed rules address the cybersecurity audit obligations anticipated under CCPA (1798.185(15)). The new proposed rules incorporate much of what was contemplated in the August 2023 version, but do also make some changes. These are detailed below:

- **Applicability**: Adopted from the August version of the proposed rules, if adopted, companies will be required to conduct a cybersecurity audit and submit it to the CPPA if they are engaging in processing personal information in such a way that there is "significant risk" to someone's privacy or security.
- **Timing**: The first audit would need to be done within 24 months of the effective date of the proposed regulations. It must be then done annually thereafter. These obligations have not changed from the prior proposal.
- **Process:** Adopted from the prior version of the proposed rules, the audit would need to be done by independent auditors. They can be either external or internal professionals who are qualified and use "generally accepted" audit

standards. Audit results must be presented to the board or management. They, in turn, must certify the audit findings and that they did not attempt to influence its conclusions.

- **Contents:** As was required by the previous version of the rules, the audit would need to evaluate the effectiveness of the program and identify any gaps and remediation steps taken. It would also need to specifically name the auditors and their qualifications (and they must certify the audit). The audit must evaluate a myriad of items that make up the company's cybersecurity program. This includes authentication, encryption, virus controls, hardware and software security, access controls, and more. It will also need to document the company's written cybersecurity program and its appropriateness to the size and complexity of the business's data processing activities. If the company has had a reportable breach, the audit would also need to -among other things- include a copy of the notice made to impacted individuals and regulatory authorities. The audit must also evaluate how a company prepares for and handles data security incidents. The updated version of the rule adds unauthorized access and unauthorized activity resulting in the loss of personal information to the definition of a "security incident." The updated rules also remove the requirement to include the number of hours each auditor worked on the audit.

Applicability to Insurance Industry

The proposed rules also clarify when CCPA applies to those in the insurance industry. Namely, if CCPA provides greater consumer protections than the Insurance Code and the information is not otherwise subject to the Insurance Code. For example, when information is collected *not* in connection with an insurance transaction. The agency gives examples, including when the insurance company uses website visitor information to serve targeted ads across multiple company sites. In that instance, the company must honor GPC signals and opt-out requests.

PUTTING IT INTO PRACTICE: The level of detail that will need to be included in a cybersecurity audit -if the rules are implemented as currently drafted- is lengthy and complex. While the requirements may mirror industry standards like NIST or ISO, they may be more than some companies currently have in place. Now may be a good time to revisit current measures against the rules to identify potential gaps.

California's Privacy Regulator Had a Busy November, Risk Assessment Edition: What Does It Mean for Businesses?

Posted December 11, 2024

In the third in our series of new CCPA regulations from California, we look at obligations for conducting risk assessments under CCPA. CCPA had called on the California agency to promulgate rules to address such assessments, and when they would be needed.

This new proposal retains much of what was proposed in 2023, but does make some modifications:

- **Scope**: As previously proposed, a company would need to conduct a risk assessment if they are doing something that could "present a significant risk" to individuals. This has not changed, although some of the examples and situations outlined in the rule have been modified. As currently proposed, this would include (1) selling or sharing personal information, (2) processing sensitive personal information, or (3) using automated decisionmaking technologies in a way that would result in a significant decision (as discussed in our earlier post in this series). The updated version also simplifies requirements for conducting risk assessments for automated decisionmaking technology.
- **Timing and Retention**: As proposed, the risk assessment will need to be conducted before beginning the process. I.e., engaging in the activity outlined above. This obligation has not changed from the prior proposal. However, there is now a timing obligation for current activities. Namely, that companies would need to conduct risk assessments within two years of the rules going into effect. Also new is that the assessment would need to be reviewed -and if needed, updated- every three years. Retained from the prior version is an obligation to update the assessment immediately if there has been a material change to the processing activity. As proposed, the assessment must be kept for five years (this has also not changed from the prior proposal).

- **Submissions**: Risk assessments will need to be submitted to the California agency under the proposed rule. Under the new proposed rules, the first must be done within two years of the effective date of the rules and then annually thereafter. Unchanged from the prior version is that as part of the submission companies will need to include a "certificate of conduct." They can then include an "abridged" or full copy of the assessment. (The possibility of providing the full risk assessment is new, the prior proposal contemplated having business submit only an abridged version.)
- **Process**: As was included in the previous version of the rules, the proposed rules require those whose job duties relate to the activities being assessed to participate in the risk assessment. These might include external employees as well as internal ones. The purpose of the assessment is to analyze whether the risks to individuals outweighs the benefits to them. In recognition that the assessment process outlined in the rule is very similar to that contained under other laws, the proposal permits using an assessment that was conducted for compliance with another law, if it "meets all of the requirements" of the regulations.
- **Contents**: In line with both the previous version of the rules, the proposed rules call for the risk assessment to identify -with specificity- the purpose for processing information and the categories of information to be processed. It would also need to outline the steps the company has taken to "maintain the quality" of the information being processed by automated decisionmaking technology or artificial intelligence tools. Other contents include how long the company will keep the information and the approximate number of people whose information will be processed. It must also include the benefits to the business, negative impacts on individuals, and safeguard measures. Under the new proposed rules, companies would also need to include a description of how disclosures will be made to individuals.

PUTTING IT INTO PRACTICE: These proposed rules contain a retroactive component and would apply to activity currently in place. Thus, as we await a final version of the rules regarding risk assessments, companies who are engaging in activities that might fall within scope may wish to begin the assessment process.

California's Privacy Regulator Had a Busy November, Automated Decisionmaking Edition: What Does It Mean for Businesses?

Posted December 10, 2024

In the second in our series of new CCPA regulations from California, we look at proposed rules for use of automated decisionmaking technology. As a reminder, CCPA discusses these technologies in relation to profiling, namely "any form of automated processing of personal information" to analyze or predict people's work performance, health, and personal preferences, among other things.

The law had called on the California privacy agency (CPPA) to promulgate rules to give consumers the ability to opt out of the use of these technologies and get access to information about how the tools are used when making decisions about them. The first set of proposed rules were met with some concern, some of which has been addressed in this newest version. Highlights of the changes are below:

- **Narrowing the definition of "automated decisionmaking technology:"** The law does not define this term, and in 2023 the agency had proposed that it be broadly any system that "in whole or in part" facilitates human decisionmaking. The term has now been narrowed to that which either *replaces* humans or *substantially facilitates* their decisionmaking. Meaning, that it is a "key factor" in the human's decision. The rule gives an example: using a tool's score as primary factor in making a significant decision about someone.
- **Automatic decisionmaking and risk assessments**: As part of the new rules for risk assessments, the agency has included specific provisions on profiling. First, companies would need to conduct risk assessments themselves. Second, the proposed rule imposes obligations on entities that make automated decisionmaking or AI technologies available to others if it trains on personal information. In those cases, the company would need to give the other entities the information they need to conduct their own risk assessments. That information would need to be given in "plain language."

- **Automated decisionmaking that results in a "significant decision**:" If there will be a "significant decision" made, the rules contemplate a "pre-use" notice. This was also contemplated in the 2023 version of the rules. However, in the 2023 version, the obligation arose if there was a "legal or similarly significant" impact (the language of CCPA). Under the proposed rules, the agency discusses "significant decisions" impacting an individual. It gives examples, including education and employment opportunities. Also included are extensive profiling and training automated decisionmaking technology that might, among other things, identify someone or make a significant decision about them.
- **Changes to company privacy policies**: The rule as revised would require companies to add into the privacy policy (in the rights section) that an individual can opt out of having their information used by automated decisionmaking that results in a "significant decision." The policy also needs to explain how someone can access automated decisionmaking.

PUTTING IT INTO PRACTICE: The California privacy agency has addressed some of the concerns raised in the initial automated decisionmaking rules. However, the obligations continue to be expansive, and may impact many organizations' uses of AI tools, especially in the HR space. That said, the obligations outlined in the rule should look familiar to those who already fall under NYC's AI law.

California's Privacy Regulator Had a Busy November: What Does It Mean for Businesses?

Posted December 9, 2024

The California Privacy Protection Agency released proposed CCPA rules for a variety of topics in November, as well as announcing an investigative sweep for compliance with the Delete Act. Topics include the following, which we cover in this week's California-focused blog posts:

- *Automated decisionmaking*: the draft revises what was previously proposed in November 2023.
- *Risk assessments*: the draft revises what was previously proposed in August 2023.
- *Cybersecurity audits*: the draft revises what was previously proposed in August 2023.
- *Insurance industry*: clarifies applicability of CCPA to the insurance industry.
- *Data broker obligations*: both adopting rules as well as an announced enforcement sweep.

Companies have until January 14, 2025 to comment on the proposed rules (for the first four topics above). The agency will then begin the formal rulemaking process, during which it can make significant changes to these drafts.

PUTTING IT INTO PRACTICE: Companies who engage in activities that could be viewed as "automatic decisionmaking" under CCPA will want to review these new proposals. Similar review should be made of the risk assessment, audit and data broker obligations. We will look at each in turn in further posts this week.

California Joins Colorado in the Brain Wave Action

Posted October 1, 2024

California's governor has signed an amendment to CCPA, the state's well-known privacy law. While California was the first to pass a "comprehensive" privacy law, it is the second -with this new amendment- to include "neural data" to the definition of sensitive personal information. It follows Colorado, which added this information to its law earlier this year. Unlike Colorado, the modification will not go into effect until January 1, 2025. (Colorado's amendment, on the other hand, became effective at the beginning of August.)

While the language of the two state's definition of what constitutes neural data similar, they are not identical. California defines neural data as information that is "generated by measuring the activity of a consumer's central or peripheral nervous system, and *that is not inferred from nonneural information*." Colorado, on the other hand, defines it as "information . . . generated by the measurement of the activity of an individual's central or peripheral nervous system and *that can be processed by or with the assistance of a device*." (Emphasis added on both.)

PUTTING IT INTO PRACTICE: As a reminder, for companies that process sensitive data in California, obligations include giving people choices about how that information is processed, providing notice around the collection and use of that information, and limiting use of that information to the purposes for which it was collected.

October 1st Reminder – Big Sky Privacy Law Goes into Effect

Posted September 23, 2024

2024 seems like it is flying by. For those keeping track of US state "comprehensive" privacy laws you know that October 1 – a week away – brings the effective date of the Montana privacy law. The "big sky" state will join Texas, Oregon and Florida as the fourth effective privacy law of 2024. This brings to total to nine state privacy laws in effect (with California, Colorado, Connecticut, Utah, and Virginia). Check out our tracker for the status of the remaining -signed- state laws, along with a comparison between their key provisions.

A few things to keep in mind for next week. Fortunately, Montana's law mostly mirrors the obligations in other states. This includes respecting opt-out signals and providing individuals with rights (like access and deletion). And like others, there is no private right of action. Montana is also a state with a 60-day cure period (the ability to cure does sunset, though, on April 1, 2026). Montana's applicability threshold is lower that other state laws in effect (except for Texas). Businesses that control of process the personal data of 50,000 Montana residents will be in scope.

PUTTING IT INTO PRACTICE: The next set of state laws to go into effect will be in January 2025: Delaware, Iowa, New Jersey, Nebraska, and New Hampshire. As of now, there will be three additional US states with similar laws that go into effect in 2025, and three slated for January 2026. For those who have not already developed an adaptable privacy program, next week's Montana law effective date is a reminder to consider that for the list for 2025.

New Hampshire AG Announces New Data Privacy Unit

Posted August 28, 2024

The privacy space continues to evolve with the announcement of the new Data Privacy Unit within New Hampshire's Consumer Protection and Antitrust Bureau. This new unit will enforce New Hampshire's Data Privacy Act, which takes effect January 1, 2025. Enforcement includes seeking civil penalties against businesses that fail to comply with consumer rights requests. The AG's office is currently accepting applications for the new unit.

Of interest to businesses, the Data Privacy Unit will issue a series of FAQs before the law's January 1, 2025, effective date. The FAQs are meant to assist consumers and businesses in understanding their rights and responsibilities under

the privacy law. While this is not formal rulemaking like we've seen in California or Colorado, this type of guidance may offer another example of how enforcement entities will interpret their state laws. It may also offer guidance for businesses to consider for their privacy programs.

PUTTING IT INTO PRACTICE: Other states may follow New Hampshire and create agencies or units within their AG office to assist in the enforcement of their privacy laws. Each may choose their way to provide businesses with the tools they need to align with new privacy laws. As always, businesses should remain vigilant and flexible as the changing landscape of state privacy laws.

Colorado's Privacy Law Gets in on the Brain Wave Action

Posted August 6, 2024

The amendment to the Colorado Privacy Act, expanding the scope of sensitive data, goes into effect today (August 6). The law will now include as sensitive information biological data that is used for identification purposes. Biological data is data generated by the technological processing of, inter alia, an individual's physiological and biochemical properties, or a consumer's body or bodily functions.

On a more unusual front, the law now also includes as sensitive information "neural" data. This is information generated by devices that measure brain activity. Or, as worded by the statute, "information . . . generated by the measurement of the activity of an individual's central or peripheral nervous system and that can be processed by or with the assistance of a device."

As a reminder, when processing sensitive information under Colorado's law, companies must adhere to the following requirements:

- State which categories of sensitive information they collect in their privacy policy
- Get consent before collecting and processing that information
- Respect deletion requests
- Conduct data protection impact assessments which assessments adhere to rules implemented under the Act

PUTTING IT INTO PRACTICE: This amendment is the first US privacy law to contemplate "neural" information. We may see similar amendments in other laws, as legislators contemplate new and novel information collection measures.

Rhode Island, the Ocean State, Sails the Privacy Waves

Posted July 8, 2024

Rhode Island's new privacy law has now passed into law, adding to the constantly evolving US privacy law patchwork. Rhode Island becomes the 20th state to enact a "comprehensive" privacy law (this one passing by default, without governor signature). It will go into effect on January 1, 2026, the same day as Indiana and Kentucky. For a recap of all of the US state privacy laws, including their obligations and effective dates, visit our interactive tool.

Rhode Island's law does not have the same deviations from the standards that we saw with those recently enacted Maryland and Minnesota. The key provisions will thus look familiar:

- **Applicability**. The law will apply to businesses that either (1) process personal data of at least 35,000 Rhode Island consumers or (2) control or process personal data of at least 10,000 consumers and derive more than twenty percent of gross revenue from the sale of personal data. The notice obligation, however, applies regardless of organize size or volume of data processed. Like all states except California, the law defines "consumer" to exclude those in an employment or commercial context. The law contains familiar exemptions for entities and information subject to GLBA and HIPAA.

- **Collection and Notice Obligations**. Rhode Island's notice obligations are narrower than most other states. It has specific provisions for website operators who sell information. This includes what information is collected, to whom it is sold, and if the company engages in behavioral advertising. Sale, like in California and several other states, includes the exchange of information for monetary or other consideration. Rhode Island does not include a data minimization requirement.
- **Sensitive information**. Businesses that process the sensitive information of Rhode Island residents will need to first get consent, mirroring all other states except California, Iowa and Utah. The list of information deemed "sensitive" is familiar and aligns with other state laws. It includes, for example, consumers' religion, sexual orientation, and health diagnoses.
- **Consumer rights.** Rhode Island consumers are provided the same rights (access, correction, deletion) found in other state laws. Timing for processing rights will be 45 days. Authorized agents can submit requests on a consumer's behalf. Businesses will not need to comply with universal online opt-out mechanisms joining roughly half the states with comprehensive privacy laws.
- **Opt-out mechanism.** Businesses that engage in targeted advertising, the sale of personal data, or profiling will need to give Rhode Island residents notice and the ability to opt out of those activities. This is in addition to the notice required for selling information discussed above.
- **Data Protection Impact Assessments**. Like all states except Iowa and Utah, businesses must conduct data protection impact assessments if processing data presents a heightened risk to consumers. This includes processing consumer data for targeted advertising, risky profiling, selling consumer data, or processing sensitive information.
- Like other states, consumers will not have a private right of action. The Rhode Island Attorney General's office will be responsible for enforcement. Unlike other state privacy laws, Rhode Island's law does not contain a cure period, meaning businesses may not have an opportunity to remediate before enforcement actions. The law contains no rulemaking provisions.

PUTTING IT INTO PRACTICE: As the privacy tidal waves brings more laws, companies may feel overwhelmed by the constant flux. Companies will be well served to take an adaptive approach to developing their privacy programs. This can be particularly helpful since, as we have written before, the US privacy patchwork includes more than just state "comprehensive" laws.

It's (Almost) July 1!: Did You Remember Oregon and Texas (and Florida)'s New Privacy Laws?

Posted June 25, 2024

As we enter into the heart of the summer there is no time to relax in privacy-land with the next batch of "comprehensive" privacy laws coming into effect on July 1. Namely, those in Texas and Oregon (and Florida if you count it as "comprehensive"). These states will join those already in effect in California, Colorado, Connecticut, Utah, and Virginia. (For a recap of effective dates and requirements, visit our tracker.)

For the most part, the Texas and Oregon laws mirror the obligations in other states. They do not provide for a private right of action, and both have a 30 day cure period (although Oregon's sunsets on January 1, 2026). There are, though, a few things to keep in mind for under these new laws:

- Where other states establish numeric or monetary thresholds, Texas' data privacy law applies to any business in Texas (except for those classified as "Small Businesses" under the Small Business Administration).
- Texas will join California in requiring specific disclosures if processing sensitive information. Namely, companies that sell sensitive data will need to post the following specific statement. "NOTICE: We may sell your sensitive personal data." The notice needs to appear in the "same manner and location" as where the company posts its privacy policy. (Sale includes the exchange for monetary *or* other consideration, but not to vendors, affiliates, or if it is needed to provide a product or service to the consumer.) A similar requirement exists if selling biometric data.

- While providing mostly the same rights as other states, Oregon has slightly different wording for its access rights. Namely, the right is to give consumers, upon request, a list of *specific* third parties, but this specificity is "at the controller's option."

Finally, as a reminder, the law in Florida is quite narrow, and applicable only to a handful of companies, as we discussed when the law was first passed.

PUTTING IT INTO PRACTICE: As more states enact privacy laws, companies may want to revisit their privacy programs. Now is a good time to see if they are sufficiently adaptable and expandable in the face of the changing legal patchwork.

Vermont Governor Vetoes Comprehensive Privacy Bill

Posted June 17, 2024

Governor Phil Scott has vetoed the state's proposed comprehensive privacy law. In rejecting the bill, he stated he was worried it created an "unnecessary and avoidable level of risk." He had concerns in three areas.

First, unlike other states, the Vermont bill would have given individuals a private right of action. He stated that this was unnecessarily "hostile" to businesses. Second, the bill contained a "kids code" provision. It mirrored other state kids' privacy laws ("age appropriate design" type laws). However, as he pointed out, these have been challenged in courts. As such, he stated that the appropriate timing for a children-focused law is after the case against the California law has concluded. Finally, he stated that the law will place "big and expensive new burdens" on companies and be a "disadvantage for the small and mid-sized businesses" that his state's residents rely on.

In returning the bill, Governor Scott recommended that it be revised to be aligned with the language of Connecticut's law. An approach, he noted, that New Hampshire had taken.

PUTTING IT INTO PRACTICE: This is the first time that a governor has pushed back on one of the US state comprehensive privacy laws. It is likely that the law will be revised to be more in line with other states' privacy laws. (And, it may retain the July 1, 2025 effective date.)

The Land of 10,000 Lakes Adds New Consumer Privacy Law: Minnesota Joins Privacy Fray

Posted June 10, 2024

Minnesota's governor has now signed into law that state's comprehensive privacy law. For those keeping count – that is number 19 of state "comprehensive" privacy laws, with six in 2024 alone. The Minnesota law will go into effect on July 31, 2025, thirty days after Tennessee's.

Minnesota's law tracks closely to the same foundations found in other states, but does have small variations. For a recap of all of the US state privacy laws and their obligations you can visit our interactive tool. Key provisions include:

- **Applicability**. The law will apply to businesses that either (1) process personal data of at least 100,000 Minnesota consumers or (2) control or process personal data of at least 25,000 consumers and derive more than twenty-five percent of gross revenue from the sale of personal data. Minnesota's law mirrors all other states (except California) and defines "consumer" to exclude those in an employment or commercial context. The law also exempts certain information and certain entities, like banks and credit unions. Like Texas and Nebraska, small businesses are also exempt. Like Utah, Minnesota's law exempts tribes. Information collected under HIPAA and GLBA is also exempt from the law.
- **Collection and Notice Obligations**. While the obligations regarding privacy policy notices is mostly similar to other states, Minnesota will also require describing data retention in privacy policies.[1] Businesses will also need to notify consumers of material changes and give consumers a "reasonable" opportunity to withdraw consent.

Like Maryland, Minnesota's law has a non-discrimination provision. Companies cannot collect, use, or process information in a way that "unlawfully discriminates" against someone.

- **Sensitive information**. Businesses that process the sensitive information of Minnesota residents will need to first get consent. The list of information deemed "sensitive" is familiar and aligns with other state laws. It includes consumers' religion, sexual orientation, and health diagnoses. Though small businesses are generally exempt from the law, they cannot sell sensitive information without a consumer's consent. This echoes Texas and Nebraska.
- **Consumer rights.** Minnesota consumers will enjoy the same rights (access, correction, deletion) provided by other state laws. In addition, they can opt out of decisions based on profiling. Consumers can also review the information that the business used to make the decision, correct any inaccuracies, and ask for reevaluation. Timing for processing rights will be 45 days. Authorized agents can submit requests on a consumer's behalf in certain circumstances. Businesses will need to comply with universal online opt-out mechanisms. Records of all appeals and responses must be kept for 24 months and the Attorney General can request copies of these records.
- **Opt-outs mechanism.** Businesses that engage in targeted advertising, the sale of personal data, or profiling will need to give Minnesota residents notice and the ability to opt out of those activities.
- **Data Protection Impact Assessments**. Like all states except Iowa and Utah, businesses must conduct data protection impact assessments if processing data presents a heightened risk to consumers. This includes processing consumer data for targeted advertising, risky profiling, selling consumer data, or processing sensitive information.
- **Record Keeping**. Businesses must document and maintain a description of the policies and procedures they have adopted to comply with the Minnesota privacy law. This includes the name and contact information for the individual with responsibility for the policies as well as how compliant policies have been implemented.
- Like other states, consumers will not have a private right of action. The Minnesota Attorney General's office will be responsible for enforcement. The law contains a 30-day cure period which is set to expire on January 31, 2026. There are no provisions for additional rulemaking.

PUTTING IT INTO PRACTICE: As more privacy laws are passed and go into effect, companies will want to take stock of their privacy programs. Are they sufficiently adaptable to take into account these new obligations? And do they otherwise think beyond "comprehensive" privacy laws?

Maryland, the Old Line State, Creates New Lines with Consumer Privacy Law

Posted May 20, 2024

Maryland's new comprehensive data privacy law, the Maryland Online Data Privacy Act, was recently signed into law by Governor Moore. This brings the total number of state "comprehensive" privacy laws to 18, five of which have been passed in 2024. Maryland's law will take effect in 2025 along with several others. Maryland's effective date is October 1, 2025 (after Tennessee (July 1, 2025) and before Indiana and Kentucky (January 1, 2026)). For a full list of effective dates, as well as other details of these state privacy laws, visit our resource page.

While many provisions mirror that which we have seen in other states, there are some differences. Key provisions of the law include the following:

- **Applicability**. Maryland's law will apply to businesses that either (1) process personal data of at least 35,000 Maryland residents; or (2) control or process personal data of at least 10,000 consumers and derive more than twenty percent of their gross revenue from the sale of personal data. The law exempts certain non-profits. It also has entity-level HIPAA and GLBA exemptions. The law covers only consumers, not employees.
- **Collection and Notice Obligations.** The content requirements for privacy policies under the Maryland law echoes that in other jurisdictions. Additionally, the law will require that businesses describe categories of third parties with whom information is shared in sufficient detail that a consumer can understand the type of, business model of, or processing conducted by each third party. This is similar only to Oregon's privacy law. The Maryland law will also

require information collected to be aligned with what is needed to provide someone with a product or service. This differs from other states, with minimization provisions tied to specified purposes (i.e., what is disclosed to someone). Finally, unlike other states, Maryland's law has a non-discrimination provision: companies cannot collect, use, process information in a way that "unlawfully discriminates" against someone.

- **Sensitive Information**. Businesses that process the sensitive information of Maryland residents will need to first get consent. The list of information deemed "sensitive" is familiar and aligns with other state laws. The law also contains data minimization obligations for sensitive data, which differs from other states. Also different, businesses will not be able to sell sensitive information. There are no exceptions listed for this prohibition.
- **Health Data**. Maryland's law also contains provisions specific to consumer health data, unlike other state privacy laws. Employees and contractors will not be able to access this information unless they have signed a confidentiality agreement, or confidentiality is a condition of employment. Processors are not allowed access to consumer health data unless they, and the controller, both comply with Maryland's law.
- **Minors**. In addition to mirroring parental consent provisions of other states, Maryland also prohibits selling children's information. Under the law, companies will also not be able to engage in targeted advertising to children. Children are defined as those under 18. These obligations apply both with actual knowledge, as well as if the company "should have known" the person was a child.
- **Consumer Rights**. Maryland consumers will have rights (access, correction, deletion) that mirror those provided by other state laws. Like other states, businesses cannot discriminate against a consumer for exercising their rights. Timing will be 45 days. Consumers can also designate an authorized agent to submit the request on their behalf. Maryland departs from other states as far as universal opt-out mechanisms. Businesses can provide an online opt-out link mechanism *or* recognize a universal opt-out mechanism.
- **Impact Assessments**. Like all states except Iowa and Utah, businesses must conduct data protection impact assessments if processing data that presents a heightened risks to consumers. This includes processing consumer data for targeted advertising, risky profiling, selling consumer data, or processing sensitive information. Unlike other states, Maryland's this includes a data protection assessment "for each algorithm that is used." Unfortunately, the law is silent as to what is meant by "algorithm."

Consumers do not have a private right of action. The law contains a 60-day cure period which sunsets on April 1, 2027. The law does not provide for additional rulemaking.

PUTTING IT INTO PRACTICE: Over a third of US jurisdictions now have "comprehensive" privacy laws. We may reach half of states -if not more- by the end of this year. With this in mind, now is a good time for companies to revisit their privacy programs to ensure they are sufficiently flexible and adaptable.

The CCPA Signals Focus on Data Minimization and Consumer Requests

Posted April 25, 2024

Earlier this month, the California Privacy Protection Agency (CPPA) issued its first-ever enforcement advisory (No. 2024-01). The advisory addresses what it calls the "foundational principle" of data minimization, and more specifically, as applied to the processing of consumer requests.

The advisory was issued in response to the Enforcement Division's purported observation of certain business practices that require consumers to "provide excessive and unnecessary personal information" when processing consumer requests. It outlines a few less obvious circumstances where the concept of data minimization applies and provides examples and guidance on how to respond. The examples include handling of consumer requests to opt-out of the sale or sharing of data and the verification of a consumer's identity.

PUTTING INTO PRACTICE: Covered businesses should carefully evaluate their internal policies and procedures and assess the extent to which they could be viewed as collecting more information than "strictly necessary" to verify and process consumer requests.

May 1 Brings Another Privacy Law to the Beehive State: The Utah Motor Vehicle Data Protection Act

Posted April 29, 2024

May 1 is a busy privacy day in Utah, with not only updates to the breach notification and social media platforms and minors laws going into effect, but also a new AI law, and one in the vehicle space. This last, the Utah Motor Vehicle Data Protection Act, has a narrow scope. It impacts "dealer data systems," i.e., systems used by car dealerships to house consumer information.

Under the law, franchisors (car brands) can't force franchisees (car dealers) into giving the brand access to the dealer's data system. Further, brands can access the franchisee's data system only with the franchisee's prior express written consent. The law also includes provisions for contracts between the car dealer and service providers who process dealer data. It also imposes obligations on entities that provide dealer data systems. These include technical measures for transferring information and data protection obligations.

The law expressly states that it does not apply to "data outside of a dealer data system." This would include information generated by the car itself, or devices people connect to their cars. It also does not give car dealerships the right to use consumer information in a way that is different either from agreements with the individual, or the reasons why the person gave the dealership the information. Finally, the drafters of the law specifically call out that the franchisee does not, through this law, get ownership of either diagnostic data or the right to share such data.

PUTTING IT INTO PRACTICE: There are other states with dealer data systems laws, thus regulating this space is not new to Utah. While the scope of the law is narrow, applying only to dealer data systems, it is part of a clear privacy trend in the beehive state.

Nebraska Fourth State to Enact Privacy Law in 2024

Posted April 25, 2024

Nebraska's governor has now signed into law the state's "comprehensive" privacy law making it the fourth one this year, and the 17th overall. It will take effect on January 1, 2025 – the same day as Delaware, Iowa, and New Hampshire. (For a round-up of all of the recent state privacy laws visit our new online resource.)

The Nebraska law's provisions are similar to those found in other states. Like all states except California, "consumer" does not include those in an employment context. Key provisions include:

- **Applicability**. The law's applicability is broader than most others (except Texas). It will apply to all businesses that conduct business in Nebraska or produces products or services used by Nebraska residents process or sell persona data; and are not s a small business (as defined under the Small Business Act of January 1, 2024). There are, though exceptions. It does not apply to non-profits, higher education institutions, and entities and data covered by GLBA and HIPAA. The law also exempts data processed by natural gas and electric utilities.
- **Sensitive information**. Businesses that process the sensitive information of Nebraska must obtain consent first – even if they are small business that would otherwise be exempt. The list of information deemed "sensitive" aligns with other state laws and includes religion, precise geolocation, and health diagnoses.
- **Consumer rights.** Nebraska will provide consumers with rights similar to other state laws. This includes the right to access, correct, delete, and port personal information. Consumers must be provided with two or more methods with which to exercise their rights. Timing for processing rights request is 45 days. Nebraska's law is silent on whether consumers can designate an authorized agent to submit the request on their behalf with the exception of parents with minor children. Businesses are not required to comply with universal online opt-out mechanisms.
- **Opt-outs mechanism.** Businesses that engage in targeted advertising, the sale of personal data, or profiling will need to give notice Nebraska residents with notice and the ability to opt out of those activities.

- **Data Protection Impact Assessments**. Like all states except Iowa and Utah, businesses must conduct data protection impact assessments if processing data that presents a heightened risks to consumers. This includes processing consumer data for targeted advertising, risky profiling, selling consumer data, or processing sensitive information.

As in other states, consumers will not have a private right of action. Instead, actions will be brought by the Nebraska Attorney General. The law has a 30-day cure period that does not sunset. There are no provisions for additional rulemaking.

PUTTING IT INTO PRACTICE: The drumbeat of states passing very similar privacy laws does not seem to be slowing down, underscoring the need for a privacy program approach that is both adaptable and flexible.

Kentucky's New Consumer Privacy Law: Is the Privacy Grass Greener in the Bluegrass State?

Posted April 12, 2024

With the Kentucky governor recently signing into law that state's privacy law the US now has 16 states with "comprehensive" privacy laws. This newest one will go into effect on January 1, 2026 – the same day as Indiana. It closely resembles other state privacy laws, in particular, Virginia's privacy law. For a recap of all of the US state privacy laws and their obligations you can visit our interactive tool.
The new Kentucky law will mirror all other states (except California) and define "consumer" to exclude those in an employment context. Key provisions of the law include:

- **Applicability**. Kentucky's privacy law has familiar applicability thresholds. It will apply to businesses that either (1) process personal data of at least 100,000 Kentucky residents or (2) control or process personal data of at least 25,000 consumers and derive more than fifty percent of gross revenue from the sale of personal data. The law also contains several familiar exemptions. Non-profits, higher education institutions, and entities that comply with GLBA and HIPAA. The law also exempts data processed by a utility, an affiliate or a holding company organized specifically for providing goods or services. Only Colorado, Indiana, and Texas have carveouts for utilities.
- **Sensitive information**. Businesses that process the sensitive information of Kentucky residents will need to first get consent. The list of information deemed "sensitive" is familiar and aligns with other state laws. It includes consumers' religion, precise geolocation, and health diagnoses.
- **Consumer rights.** Kentucky consumers will enjoy the rights provided by other state laws. These include the right to access, correct, delete, and port personal information. Timing for processing rights will be 45 days. Kentucky's law is silent on whether consumers can designate an authorized agent to submit the request on their behalf with the exception of parents with minor children. Kentucky's law does not require businesses to comply with universal online opt-out mechanisms.
- **Opt-outs mechanism.** Businesses that engage in targeted advertising, the sale of personal data, or profiling will need to give Kentucky residents notice and the ability to opt out of those activities.
- **Data Protection Impact Assessments**. Like all states except Iowa and Utah, businesses must conduct data protection impact assessments if processing data presents a heightened risk to consumers. This includes processing consumer data for targeted advertising, risky profiling, selling consumer data, or processing sensitive information.

Like other states, consumers will not have a private right of action. Instead, the Kentucky Attorney General's office will be responsible for enforcement. The law contains a 30-day cure period which is not set to expire, unlike other states' privacy laws. There are also no provisions for additional rulemaking.

PUTTING IT INTO PRACTICE: With the enactment of a sixteenth privacy law, the similarities can obscure important differences. We anticipate more states will pass similar laws in the coming months, and companies will thus want a privacy program approach that is both adaptable and flexible.

New Hampshire, the Granite State, Joins Privacy Law Deluge: Sets Its Law in Stone

Posted March 27, 2024

New Hampshire's governor has signed into law the second state comprehensive privacy law of 2024. The law takes effect on January 1, 2025 – the same day as Iowa and Delaware (with New Jersey going into effect two weeks later). The law closely resembles other state privacy laws.

Like most other state privacy laws, New Hampshire does not define "consumer" to include those in an employment context. The New Hampshire Attorney General's office has enforcement powers and like other states, there is no private right of action. The law also does not include provisions for additional rulemaking, mirroring most of the states (with the notable exception of California, Colorado, and New Jersey).

Key provisions include:

- **Applicability**. Like Delaware and Montana, New Hampshire's privacy law has a lower applicability threshold, perhaps reflecting the state's lower overall population. The law will apply to businesses that either (1) process personal data of at least 35,000 New Hampshire residents or (2) control or process personal data of at least 10,000 consumers and derives more than twenty-five percent of their gross revenue from the sale of personal data. The law also contains several familiar exemptions. Non-profits, higher education institutions, and national securities associations are exempt. The law also contains exemptions for entities that comply with GLBA and HIPAA.
- **Sensitive information**. Businesses that process New Hampshire consumers' sensitive information must obtain consumer consent before processing. The list of information deemed "sensitive" is familiar by now and aligns with other state laws. This information includes consumers' religion, health information, and sexual orientation.
- **Consumer rights.** New Hampshire consumers will have a familiar slate of rights as those found in other states. This includes the right to access, correct, delete, and port personal information. Consumers may designate an authorized agent to act on the consumer's behalf. Timing for processing rights is 45 days – the same as other states except Iowa and New Jersey, which states provide 60 days and 90 days respectively. Like nine other states, businesses will need to comply with universal online opt-out mechanisms by July 1, 2025, six months after the law takes effect.
- **Opt-outs mechanism targeted advertising, sale, profiling.** New Hampshire residents must be given notice of, and the ability to opt out of, targeted advertising, the sale of their data, and profiling. If a business engages in these activities, they will need to conduct a data protection assessment.
- **Data Protection Impact Assessments**. Like all states except Iowa and Utah, businesses must conduct data protection impact assessments if processing data that presents a heightened risks to consumers. This includes processing consumer data for targeted advertising, risky profiling, selling consumer data, or processing sensitive information.

PUTTING IT INTO PRACTICE: If these provisions are sounding familiar, it is because they are in many ways. It appears that passage of these laws will continue apace in 2024. Businesses will want to keep this in mind as they develop their privacy programs. Keeping in mind the potential for new requirements as well as understanding the nuanced differences between these states will be useful for a scalable compliance program. Our new tracking tool can help.

California AG Turns on CCPA Investigation of Streaming Services

Posted February 2, 2024

To close out Data Privacy Week, California Attorney General Rob Bonta announced a new investigative sweep probing streaming apps' and devices' compliance with the California Consumer Privacy Act (CCPA).

The announcement highlights three key areas of focus for the AG in this investigation:

1. Consumers should be able to go into device settings on a SmartTV to find and enable the "Do Not Sell My Personal Information" setting.
2. Opt-out choices should be honored across devices if the consumer is logged into their account when they opt out.
3. A streaming service's privacy policy covering CCPA rights should be easy to find.

The investigative sweep covers both smart devices and more Internet-enabled traditional devices like phones and computers.

But companies offering streaming services through smart devices face unique challenges when it comes to CCPA compliance. Smart device interfaces do not always offer the same straightforward opportunities as traditional devices for enabling users to opt out, identifying users, and giving quick access to readable privacy policies. The AG has clarified that his office will make sure streaming services follow California privacy laws even when the interface makes it difficult.

PUTTING IT INTO PRACTICE: Companies operating streaming services should use this opportunity to revisit their opt-out practices across devices. This announcement is a reminder that California expects that navigating to the opt-out option and carrying it across devices be easy for users. Further, it expects that privacy policies be both findable and understandable.

The Garden State Cultivates a Consumer Privacy Law – The First for 2024

Posted January 29, 2024

New Jersey's governor has signed into law the first US state comprehensive privacy law of 2024. It will go into effect January 16, 2025. For those keeping score, that puts New Jersey after Florida, Oregon, Texas (all July 1, 2024), Montana (October 1, 2024), Delaware, and Iowa (both January 1, 2025). But, before Indiana (January 1, 2026). (Visit this post for a more detailed recap).

The requirements of the New Jersey law will feel quite familiar for those who familiar with the other US state privacy laws. Key provisions include:

- **Applicability**. Like all states except California, New Jersey's privacy law will apply to consumer information and not to employees. Further, the law will apply to businesses that either (1) process personal data of at least 100,000 New Jersey residents or (2) control or process personal data of at least 25,000 consumers and receives revenue or discounted goods or services for the sale of personal data. The law contains exemptions for entities that are subject to (and comply with) GLBA. There is no entity-level exception for HIPAA regulated entities, but there is an exemption for information regulated by HIPAA (similar to the California approach).
- **Sensitive information**. New Jersey falls into the group of states that will require consent before processing personal information. Like other state laws, sensitive information includes racial or ethnic origin, religious beliefs, mental or physical health information, sex life or sexual orientation, citizenship or immigration status, status as transgender or non-binary, personally identifying genetic or biometric data, children's personal data, or precise geolocation. Unlike most others, New Jersey also includes financial information in its definition of "sensitive information. Companies that process sensitive information will also have to conduct a data protection assessment.

- **Consumer rights.** New Jersey consumers will have a familiar slate of rights as found in other states. This includes the right to access, correct, delete, and port personal information. Consumers may designate an authorized agent to act on the consumer's behalf. Timing for processing rights is different from the typical 45 days – New Jersey businesses must respond within 60 days. Additionally, businesses will need to comply with universal online opt-out mechanisms by July 16, 2025, six months after the law takes effect.
- **Targeted advertising, sale and profiling.** New Jersey residents must be given notice of, and the ability to opt out of, targeted advertising (including a universal opt-out mechanism). They must also be given the ability to opt out of the sale of their data, and of certain "profiling." Additionally, if a business engages in these activities, they will need to conduct a data protection assessment.
- **Enforcement**. The New Jersey law does not contain a private right of action. The NJ Division of Consumer Affairs has discretion to allow companies it believes have violated the law an opportunity to cure. This cure provision will expire after 18 months.

What's next? Like California and Colorado, the law provides for rulemaking by the Director of the Division of Consumer Affairs. Areas for rulemaking include specifications for universal opt-out mechanisms.

PUTTING IT INTO PRACTICE: These state privacy laws contain provisions that while familiar, have subtle nuances. Flexibility and adaptation will be key as businesses tailor their privacy programs in light of what we anticipate to be a growing number of US privacy laws at a state level.

Bookmark This!: Colorado Launches Universal Opt Out Mechanism List

Posted January 8, 2024

In anticipation of July 1, 2024, requirements to allow consumers the ability to use "universal opt out mechanisms" in certain circumstances, Colorado has posted its "universal opt out shortlist." The list is indeed short. Only one mechanism, the already-known global privacy control (GPC) is on it. The Colorado Attorney General has indicated that the list can be updated. And it may be in the coming months.

As most are no doubt already aware, the Colorado privacy law requires, among other things, that covered companies let website users opt out of having their personal information sold or used for targeted advertising. To exercise these rights, companies need to -beginning July 1 of this year- allow consumers to make their choices using a listed mechanism (also referred to as a UOOM). The regulations to the law, finalized last year, require that the Colorado AG maintain a public list of UOOMs, which list it must update "periodically."

PUTTING IT INTO PRACTICE: Companies operating in the US now have four comprehensive state privacy laws to keep on their radar for 2024. 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.

As you move forward in planning and implementing your privacy efforts this year, we hope that this compilation serves as a useful tool.

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual."

—Earl Warren

2024 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

Carolyn Metnick
Partner
cmetnick@sheppardmullin.com
312.499.6315

Oliver Heinisch
Partner
oheinisch@sheppardmullin.com
44.203.178.7833

David Poell
Partner
dpoell@sheppardmullin.com
312.499.6349

Julie Kadish
Partner
jkadish@sheppardmullin.com
312.499.6334

Drew Svor
Partner
dsvor@sheppardmullin.com
202.747.2305

Elfin Noce
Special Counsel
enoce@sheppardmullin.com
202.747.2196

Joseph Antel
Associate
jantel@sheppardmullin.com
202.747.2654

Tracy Chau
Associate
trchau@sheppardmullin.com
312.499.6341

Samantha Davis
Associate
skdavis@sheppardmullin.com
212.896.0670

Snehal Desai
Associate
sdesai@sheppardmullin.com
415.774.2960

Charles Glover
Associate
cglover@sheppardmullin.com
212.896.0679

Robert Hough II
Associate
rhough@sheppardmullin.com
469.391.7408

Ethan Lamb
Associate
elamb@sheppardmullin.com
202.747.1870

Jordan Mallory
Associate
jmallory@sheppardmullin.com
202.747.1866

Kathryn Smith
Associate
kasmith@sheppardmullin.com
312.499.6355

Alyssa Sones
Associate
asones@sheppardmullin.com
424.288.5305

Michael Sutton
Associate
msutton@sheppardmullin.com
469.391.7455

Nikole Snyder
Associate
nsnyder@sheppardmullin.com
202.747.3218

Brittany Walter
Associate
bwalter@sheppardmullin.com
858.876.3525

Sam Cournoyer
Law Clerk
scournoyer@sheppardmullin.com
212.896.0608

Sharilyn Clark
Cybersecurity & Privacy Fellow
shclark@sheppardmullin.com
312.499.6380

Sidney Howe
Cybersecurity Fellow
showe@sheppardmullin.com
202.747.1886

James O'Reilly
Cybersecurity & Privacy Fellow
joreilly@sheppardmullin.com
312.499.6356

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