June 2023

Skadden

Privacy & Cybersecurity Update

Florida and Montana Enact Privacy Laws

Florida has officially adopted a comprehensive digital privacy law targeted specifically at regulating large technology companies and the use of voice and facial recognition technology. In addition, after unanimously passing through the Montana State Legislature, Gov. Greg Gianforte signed the Montana Consumer Data Privacy Act (MTCDPA) into law on May 19, 2023, which is largely modeled on the state of Connecticut's privacy law.

Florida

On June 6, 2023, Florida Gov. Ron DeSantis signed Senate Bill 262, which is also known as the "Florida Digital Bill of Rights." While the law is modeled off of aspects of privacy laws enacted in Washington, Utah and Texas, the scope of businesses the law would apply to is more targeted toward large technology companies than the laws in those states. Florida's law will take effect on July 1, 2024.

Which Businesses Are Covered?

The Florida Digital Bill of Rights follows other states' privacy laws in adopting a controller-processor framework, but uniquely limits application of the law to a more narrow subset of controllers. Controllers are defined under the law to include only those businesses that make over $1 billion in global annual revenue and satisfy one of the following criteria:

- make at least 50% of its global gross revenue from online advertising;
- operate a consumer-facing smart speaker and voice command service with an integrated virtual assistant that is connected to a cloud computing service that uses hands-free verbal activation; or
- operate an app store or digital distribution platform that offers at least 250,000 apps for download.

The law applies to all "processors," or individuals that process personal data on behalf of a controller, regardless of their size.

Nonprofits, government organizations, higher education institutions, financial institutions and entities covered under the Health Insurance Portability and Accountability Act (HIPAA) are exempt from the law. These carve-outs are consistent with other states' privacy laws.

Which Consumers Are Covered?

The Digital Bill of Rights covers Florida consumers acting in an individual or household context, but not those acting in a commercial or employment context. Thus, personal information collected from employees or in a business-to-business context is not covered.

What Information Is Protected?

Under the Digital Bill of Rights, protected personal information includes either a username or email address in combination with a password or security question that would permit access to an online account, or an individual's first name or first initial and last name in combination with any or more of the following data:

- Social Security number;
- driver license or identification card number, passport number, military identification number or other similar numbers issued on a government identification document;
- financial account number or credit/debit card number in combination with any required security passwords needed to access the financial account;
- information regarding an individual's medical history, treatment or diagnosis by a health care professional, or mental/physical condition;
- an individual's biometric data, defined as data that is generated by "automatic measurements of an individual's biological characteristics," including fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or traits that can be used to identify a specific individual. Physical or digital photos, video or audio recordings (or data generated from such recordings) do not constitute biometric data; and
- any information regarding an individual's geolocation.

The law also protects sensitive data, defined as any personal data that reveals the consumer's race, ethnicity, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship/immigration status, genetic or biometric data, and geolocation data.

Any data that falls under the Gramm-Leach-Bliley Act (GLBA), HIPAA, or the Family Educational Rights and Privacy Act (FERPA) also is exempt from the law.

Consumer Rights

Under the Digital Bill of Rights, Florida consumers have the right to:

- Confirm the controller's possession of their personal data.
- Access their data.
- Correct their data.
- Request that their data be deleted.
- Obtain a copy of their data.
- Get a portable copy of their data that they previously provided.
- Revoke their consent for certain uses of their data.
- Appeal if their request to the controller is denied.
- Know that their personal data will not be used against them when purchasing a home, obtaining health insurance or being hired.

Consumers also have the right to opt out of targeted advertising, data sales, profiling and the collection of their sensitive and biometric data. The law also gives consumers the express right to opt out of the collection of personal data done by the controllers' voice and facial recognition technology.

If a consumer makes a request to a controller regarding their data, the controller needs to respond to the request within 45 days, with a 15-day extension to be granted if reasonably necessary. If the controller cannot take action on the request, it must inform the consumer and provide a justification, while also providing instructions to the consumer on how to appeal the controller's decision and providing a conspicuously available process for appeal.

Obligations Imposed on Businesses

The Digital Bill of Rights imposes certain obligations on both controllers and processors regarding the collection and use of consumers' personal data, and includes several unique provisions not included in other state privacy laws concerning surveillance, online search engines and online platforms accessible by children.

Generally, controllers must limit personal data collection to only what is adequate, relevant and reasonably necessary for the purposes of the data processing that was disclosed to the consumer, and cannot use the data for a purpose that is out of this scope unless the consumer gives consent.

Controllers must provide accessible and clear privacy notices that are updated at least once a year. The privacy notices must denote the types of personal data being processed and, if any sensitive data is included they must include the purpose of processing the data, how consumers may exercise their rights including for appealing a controller's decision, the types of personal data the controller shares with third parties and the types of third parties receiving the shared data.

If a controller sells biometric personal data, it also must provide the following additional privacy notice to consumers: "NOTICE: We may sell your biometric personal data." The notice should be published in the same location and manner as the privacy notice concerning personal data.

Surveillance Restrictions

The Digital Bill of Rights restricts controllers and processors from collecting data on a voice-activated device if the device is not being actively used by a consumer, unless expressly authorized by the consumer. This includes any audio or video recording devices or device features, as well as any electronic, visual, thermal or olfactory feature that collects data for the purpose of surveillance. The law does not provide a definition of "surveillance," which is an area of ambiguity that companies employing these technologies will need to navigate when asking consumers for consent or authorization.

Search Engine Disclosures

Companies employing online search engines must provide easily accessible descriptions of how they determine search result rankings, including regarding political partisanship or ideology.

Duty Regarding Websites and Online Services Accessible to Children

The Digital Bill of Rights features protections for minors and children accessing online platforms. The law imposes restrictions on controllers regarding the processing and use of a child's personal information; profiling of a child, collecting, selling or sharing a child's geolocation data; and the use of personal information to estimate a child's age.

Duty Regarding Sensitive Data

Under the law, businesses cannot sell sensitive data without prior consent from the consumer and cannot process children's sensitive data without authorization of a parent or guardian, which is consistent with the Children's Online Privacy Protection Act.

Duty to Non-Discriminate

If a consumer chooses to exercise their rights, controllers cannot discriminate against a consumer by denying goods or services, charging different prices or providing a different quality of goods or services.

Data Protection Assessments

Similar to privacy laws in California, Colorado, Connecticut, Montana and Virginia, Florida's Digital Bill of Rights requires controllers to conduct data protection assessments. These assessments also must include a comparison weighing the direct or indirect benefits of the data processing to the controller, consumer and general public against the risks to the consumer.

Data Processors

Under the Digital Bill of Rights, a processor's obligations include assisting the controller with compliance with the law, whether through addressing consumer requests, processing data or supporting the controller in data protection measures. Processors also are obligated to delete or return consumers' personal data to the controller when requested, make all applicable data available to the controller if needed to comply with the law and allow for reasonable assessments by the controller.

Contracts between controllers and processors must establish instructions for data processing and detail the nature and purpose of processing the data, the type of data being processed, parties' obligations regarding the data, the duration of the processing and require that the processor be subject to a duty of confidentiality.

Enforcement

The Office of the Florida Attorney General has the sole authority to enforce the Digital Bill of Rights. Consumers do not have a private cause of action under the law. Organizations can be subject to a civil penalty of up to $50,000 for each violation of the law, and this penalty can be tripled if the violation involves a child consumer, if there is a failure to delete or correct information after receiving a consumer's request or if an organization continues to sell or share consumer data after a consumer opts out.

Key Takeaways

The Florida Digital Bill of Rights differs from other states' privacy laws due to the narrower subset of businesses to which it applies, as well as the law's unique requirements in areas such as surveillance measures and search engine usage. Companies that fall within coverage of the new law must be mindful of these distinct obligations.

Montana

Largely modeled after the Connecticut Data Privacy Act (CTDPA), the MTCDPA will be one of the most consumer-friendly state privacy laws when it goes into effect on October 1, 2024, given its low applicability threshold, broad consumer rights and additional protections for children's privacy. Although each requirement and obligation that the MTCDPA imposes on impacted businesses can be found in at least one of the other eight enacted state-level comprehensive consumer data privacy laws, the addition of the MTCDPA further complicates the compliance efforts of businesses that collect or process personal data in the United States.

Scope of the MTCDPA

The MTCDPA applies to organizations that conduct business in Montana, or produce products or services targeted to residents of the state, and either:

- control or process personal data of at least 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- control or process the personal data of at least 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.

In contrast to certain more business-friendly comprehensive state privacy laws, such as Utah's Consumer Privacy Act (UTCPA), organizations do not have to surpass a certain annual "revenue" threshold in order to be subject to the MTCDPA. This lower applicability threshold can, at least in part, be attributed to Montana's sparse population and low annual gross domestic product.

Personal Data, Consumers and Exemptions

Under the NTCDPA, the term "personal data" is defined as any information that is linked or reasonably linkable to an identified or identifiable individual. However, consistent with most of the other enacted state privacy laws, the MTCDPA does not apply to the following entity categories: governmental entities of the state of Montana; nonprofit organizations; higher education institutions; national securities associations registered under the 1934 Securities Exchange Act; financial institutions (and their affiliates) subject to the GLBA; and covered entities or business associates subject to HIPAA.

In addition to the foregoing, certain types of data are also exempt from the MTCDPA's scope including, *inter alia*, deidentified data or publicly available information; personal data collected, processed, sold or disclosed in compliance with the GLBA, Driver's Privacy Protection Act, Farm Credit Act or Airline Deregulation Act; personal data regulated by the FERPA; protected health information under HIPAA; and certain other classes of data and information regarding patients, health records and scientific research.

The MTCDPA only applies to natural persons who are Montana residents acting in a personal context and expressly excludes individuals acting in a commercial or employment context or as an employee, owner, director, officer or contractor of an organization whose communications or transactions with the controller (as defined below) occur solely within the context of that individual's role with the organization.

Finally, as further explained below, the MTCDPA also includes certain safeguards to prevent consumers from compelling controllers to reveal trade secrets, which is regarded under Montana state law as information or computer software that derives actual or potential independent economic value from not being generally known to, and not being readily ascertainable by, others and where reasonable efforts also are used to maintain its secrecy.

Obligations of Controllers

Under the MTCDPA, a controller — defined as an individual or legal entity that, acting alone or jointly with others, determines the purpose and means of processing personal data — has the following ongoing affirmative obligations:

- **Data Minimization.** Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.
- **Data Security Practices.** Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue.
- **Data Processing.** Only process personal data to the extent that the processing is reasonably necessary, proportionate, adequate, relevant and limited to what is necessary in relation to the specific purpose.
- **Consent Revocation.** Provide a mechanism for consumers to revoke their consent that is at least as easy as the mechanism used by the consumer to provide their consent, and also cease processing such consumer's personal data within 45 days of receiving notice of such revocation.
- **Privacy Notice.** Provide consumers with a reasonably accessible, clear and meaningful privacy notice outlining (i) the categories of personal data being processed, (ii) the purpose for the processing, (iii) the categories of personal data shared with third parties, (iv) the categories of such third parties to whom personal data is shared (v) a mechanism to contact the controller such as an active email address and (vi) how consumers may exercise their consumer rights, including how to appeal a controller's decision regarding their request.
- **Deidentified Data.** If in possession of deidentified data — *i.e.*, data that cannot be used to reasonably infer information about, or otherwise be linked to, an identified or identifiable individual or a device linked to the individual — (i) take reasonable measures to ensure that such data cannot be associated with a natural person, (ii) publicly commit to maintaining and using such data without attempting to reidentify the data and (iii) contractually obligate any recipients of such data to comply with the MTCDPA.
- **Data Protection Assessments.** Conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer, such as (i) processing personal data for targeted advertising

purposes, (ii) the sale of personal data, (iii) processing personal data for profiling purposes, where such profiling presents a reasonably foreseeable risk of substantial injury to consumers and (iv) processing sensitive data. Even though the MTCDPA goes into effect on October 1, 2024, the law's data protection assessment requirements must apply to processing activities created or generated after January 1, 2025, and are not retroactive. The MTCDPA also provides that if a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, such assessment will satisfy the MTCDPA if it is "reasonably similar in scope and effect" to the data protection assessment that would otherwise be conducted pursuant to the MTCDPA. Lastly, while such assessments are confidential, upon request they must be provided to the Montana attorney general.

As used in the MTCDPA, the phrase "sale of personal data," excludes certain data transfers, including the (i) disclosure or transfer of personal data to an affiliate of the controller, (ii) disclosure of personal data that the consumer both intentionally made available to the public via a channel of mass media and did not restrict to a specific audience and (iii) disclosure or transfer of personal data to a third party as an asset that is part of a transaction in which the third party assumes control of all or part of the controller's assets (*e.g.*, a merger, acquisition or bankruptcy).

As defined in the MTCDPA, "sensitive data" is personal data that includes (i) data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status, (ii) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person, (iii) personal data collected from a known child under 13 years of age or (iv) precise geolocation data derived from technology that directly identifies an individual's specific location with precision and accuracy within a 1,750-foot radius.

In addition to the aforementioned affirmative obligations, the MTCDPA prohibits controllers from engaging in the following actions:

- **Proportionality.** Without the relevant consumer's consent, controllers cannot process personal data for purposes that are not reasonably necessary to, or compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer.
- **Processing Sensitive Data.** Without the relevant consumer's consent, or in accordance with the Children's Online Privacy Protection Act (COPPA) in the case of a known child under 13 years of age, controllers cannot process sensitive data concerning such consumer.
- **Anti-Discrimination.** Controllers cannot discriminate against consumers for exercising their consumer rights under the MTCDPA or process personal data in violation of Montana state law or federal law that prohibits unlawful discrimination against consumers.
- **Known Children.** Process personal data for targeted advertising purposes or the sale of personal data without the consumer's consent when a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age.

Obligations of Processors

Under the MTCDPA, a processor — defined as a natural person or legal entity that processes personal data on behalf of a controller — also has certain ongoing obligations. A processor must adhere to the controller's instructions and assist the controller in meeting its obligations under the MTCDPA, including by (i) considering the nature of processing and the information available to the processor by (a) appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests and (b) assisting the controller in meeting its obligations in relation to the security of processing the personal data and in relation to a security breach notification; and (ii) providing information necessary to enable the controller to conduct and document data protection assessments.

The controller and processor must have a contract that governs the processor's data processing procedures with respect to processing performed on behalf of the controller. In addition to setting forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and both parties' rights and obligations, such contract must require the processor to:

- ensure that all persons processing personal data are subject to a duty of confidentiality with respect to such data;
- at the controller's discretion and to the extent permissible by applicable law, delete or return to the controller all personal data as requested at the end of the provision of services;
- demonstrate compliance with the MTCDPA upon the controller's reasonable request;
- through a written contract, subject any engaged subcontractors to the same obligations as the processor with respect to personal data; and
- allow and cooperate with all reasonable data assessments by or on behalf of the controller or otherwise provide the controller with its own data assessment report.

Consumer Rights

The MTCDPA expressly provides that controllers must comply with certain requests from authenticated consumers. If a controller is unable to authenticate a consumer's request through commercially reasonable efforts, the controller is not obligated to comply with the request. In such situation, a controller must notify the consumer that it is unable to authenticate the request until the consumer provides the information reasonably necessary for the controller to authenticate the consumer as well as the consumer's request to exercise their rights.

The MTCDPA affords authenticated consumers the right to require certain elements from the controller, including:

- **Confirmation and Access.** Confirm whether a controller is processing their personal data and provides access to such personal data, unless such confirmation or access would require the controller to reveal a trade secret.
- **Correct Inaccuracies.** Correct inaccuracies in their personal data, taking into account the nature of, and purpose for, processing such personal data.
- **Data Deletion.** Delete personal data about such consumer.
- **Portability.** Obtain a copy — where processing is carried out by automated means, provided that the controller is not required to reveal any trade secret — of their personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows such consumer to transmit the data to another controller without hindrance.

The foregoing consumer rights do not apply to "pseudonymous data," defined as personal data that cannot be attributed to a specific natural person without the use of additional information, so long as the additional information is kept separately and is subject to appropriate technical and organizational measures that ensure the personal data is not attributed to an identified or identifiable natural person.

Controllers must respond to an authenticated consumer's request within 45 days after receiving such request, with a right to extend for an additional 45 days when reasonably necessary considering the complexity and number of requests, so long as the controller timely and properly notifies the requesting consumer. Consumers may file an appeal if a controller declines to act regarding the consumer's request. The controller must notify the requesting consumer and provide instructions as to how to appeal such a decision. Although the MTCDPA does not set forth a timeline by when a consumer must file an appeal, it expressly states that controllers have 60 days to respond to a submitted appeal. If a consumer's appeal is denied, the controller must provide the consumer with a mechanism to contact the Montana attorney general's office to submit a complaint.

Opt-Out Right for Consumers

The MTCDPA adopted broad consumer opt-out rights and requires that consumers have the right to opt out of a controller's processing of personal information for purposes of targeted advertising, the sale of the consumer's personal data and profiling through solely automated decisions that produce legal or similarly significant effects concerning such consumer. Consumers may designate an authorized agent to act on their behalf to opt out of the processing of their personal data.

If a controller denies an opt-out request because it believes the request is fraudulent, the controller must notify whomever made the request that it believes the request is fraudulent and that it may not comply with the request.

If a controller sells personal data to third parties or processes personal data for targeted advertising, the MTCDPA mandates that such controller must clearly and conspicuously disclose the processing, as well as methods by which a consumer may exercise the right to opt out of the processing. In particular, such opt-out methods must include "a clear and conspicuous link" provided on the controller's website to enable consumers or their agents to opt out of targeted advertising or the sale of the consumer's personal data. Furthermore, from January 1, 2025, onward, controllers must permit consumers to opt out of the sale of their personal information or targeted advertising through an opt-out "preference signal." Such opt-out preference signals may not unfairly disadvantage another controller or make use of a default setting, and instead must: (i) require the consumer to make an affirmative, freely given and unambiguous choice to opt out, (ii) be consumer-friendly and easy for the average consumer to use, (iii) be consistent with any federal or state law or regulation and (iv) allow the controller to "accurately determine" whether the consumer is a Montana resident and whether the consumer has made a legitimate request to opt out.

Where a consumer's opt-out decision made through an opt-out preference signal conflicts with the existing controller-specific privacy setting or the consumer's voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller must still comply with the consumer's opt-out, but may notify the consumer of the conflict and provide the choice to confirm controller-specific privacy settings or participation in such a program.

No Private Right of Action

The MTCDPA does not provide for a private right of action. Rather, MTCDPA violations are only enforceable by the Montana attorney general.

Until April 1, 2026, prior to initiating any action for a violation of the MTCDPA, the Montana attorney general must issue a notice of the alleged violation to the controller and provide the controller with 60 days to cure such a violation. If the controller cures the violation within that period, and provides an express written statement to the Montana attorney general confirming the cure and that no such further violation will occur, no action may be initiated against the controller. No right to cure exists after April 1, 2026.

The MTCDPA does not specify the types of remedies available to, or provide limits on the monetary penalties that may be sought by, the Montana attorney general.

Key Takeaways

Businesses that have established privacy policies and practices in compliance with other consumer-friendly state privacy laws should be well-positioned to comply with the MTCDPA when it goes into effect on October 1, 2024. While the MTCDPA is not significantly distinguishable in substance from comprehensive privacy laws enacted in other states, businesses that will be subject to the MTCDPA should devote resources to ensure that their operations will satisfy and fulfill the law's requirements, particularly given that the 60-day cure period will sunset only 18 months after the MTCDPA goes into effect. Businesses also should be mindful of the uncertainty regarding the civil penalties that may be levied and lack of clarity on other remedies provided by the Montana attorney general for correcting MTCDPA violations.

Return to Table of Contents

Connecticut Privacy Act Goes Into Effect With New Amendment

The Connecticut Data Privacy Act[1] went into effect on July 1, 2023, along with a recently adopted separate amendment that provides protections for residents' health-related data and online safety for minors.

New Amendment to the CTDPA

On June 26, 2023, Connecticut Gov. Ned Lamont signed into law Senate Bill 3 (SB 3), which amended certain portions of the CTDPA. The primary amendments feature substantive data privacy requirements concerning a consumer's health-related data and more robust protections for minors when using the internet.[2] The consumer health provisions go into effect on July 1, 2023, while most of SB 3's provisions aimed at protecting minors will not become effective until October 1, 2024. The provisions that address a minor's ability to unpublish or delete their social media accounts will become effective on July 1, 2024.

Which Businesses Are Covered?

Compared to the CTDPA, SB 3's consumer health-related provisions are broader in scope regarding persons that conduct business in the state and persons that produce products or services that are targeted to residents of the state.

The provisions concerning online safety for minors also are broad in scope, applying to social media platforms that are utilized by consumers within the state and controllers that offer any online service, product or feature to minors.

Which Consumers Are Covered?

Any individual who is a resident of Connecticut is covered under the law. Connecticut consumers acting in a commercial or employment context are not considered protected consumers, meaning individuals acting as employees and information collected in a business-to-business context are not covered.

Which Information Is Protected?

SB 3 creates a robust framework for protecting consumers health-related data by adding health-related definitions and establishing controls and restrictions concerning the collection, access and sale of a health-related data. SB 3 adds related definitions to the CTDPA, including "consumer health data" (*i.e.*, any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data) and "consumer health data controller" (*i.e.*, any controller that, alone or jointly with others, determines the purpose and means of processing consumer health data). Additionally, the definition of "sensitive data" is amended to include "consumer health data."

SB 3 also expands protections for minors online by adding definitions such as "minor" (*i.e.*, any consumer who is younger than 18 years of age) and "heightened risk of harm to minors" (*i.e.*, the processing of minors' personal data in a manner that presents any reasonably foreseeable risk of (i) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (ii) any financial, physical or reputational injury to minors, or (iii) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person.)

[1] See our May 2022 *Privacy & Cybersecurity Update* for more information about the CTDPA.

[2] The text of SB 3 can be accessed here.

Consumer Health-Related Data

SB 3 includes a number or prohibitions with respect to consumer health data:

- **Confidentiality.** Companies may not provide any employee or contractor with access to consumer health data unless the employee or contractor is subject to a duty of confidentiality.
- **Providing Processors Data.** Companies may not provide any processor with access to consumer health data unless such person or processor complies with specific requirements.
- **Geofence.** Companies may not use a "geofence" — meaning any technology that uses a form of location detection to establish a virtual boundary — for various purposes near any mental health facility or reproductive or sexual health facility.
- **Selling Data.** Companies may not sell, or offer to sell, consumer health data without first obtaining the consumer's consent.

Online Safety for Minors

SB 3 applies specific criteria for social media platforms concerning deleting and unpublishing a minor's social media account. Specifically, they must:

- **Unpublish.** Unpublish a minor's social media platform account not later than 15 business days after a request is received from a minor or, if the minor is younger than 16, from their parent or legal guardian.
- **Deletion.** Delete a minor's social media platform account and cease processing their personal data except where otherwise permitted or required by applicable law not later than 45 business days after a request from a minor or, if the minor is younger than 16, from their parent or legal guardian. This deadline can be extended by an additional 45 business days if reasonably necessary, provided the social media platform informs the minor or, if the minor is younger than 16, their parent or legal guardian within the initial 45 business day response period of such extension and the reason for such extension.
- **Mechanism.** Establish and describe (in a privacy notice) one or more secure and reliable means for submitting a request to unpublish or delete a social media platform account.

SB 3 establishes a standard of care, limits on certain features and an obligation to conduct data protection assessments on controllers that offer any online service, product or feature to minors. Specifically, they must:

- **Risk of Harm.** Use reasonable care to avoid any heightened risk of harm to minors caused by such online service, product or feature.
- **Consent Mechanism.** Not provide a consent mechanism that is designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decision-making or choice.
- **Direct Messaging.** Not offer any direct messaging apparatus without providing readily accessible and easy-to-use safeguards to limit the ability of adults to send unsolicited communications to minors with whom they are not connected, unless it is a service where the predominant or exclusive function is: (i) email; or (ii) direct messaging consisting of text, photos or videos that are sent between devices by electronic means, where messages are (a) shared between the sender and the recipient, (b) only visible to the sender and the recipient, and (c) not posted publicly.
- **Data Protection Assessment.** Conduct a data protection assessment. An assessment conducted to comply with another applicable law or regulation that is reasonably similar in scope and effect can satisfy this requirement.

SB 3 also places restrictions on a controller's ability to control minors' online experiences and their ability to collect minors' data. Specifically, subject to obtaining consent or complying with the parental consent requirements in COPPA, they must:

- **Targeting, Selling, Profiling.** Not process any minor's personal data for the purposes of targeted advertising, any sale of personal data or particular categories of profiling.
- **Limits on Necessity and Duration.** Not process any minor's personal data that is not reasonably necessary or longer than reasonably necessary to provide such online service, product or feature.
- **Unstated or Unrelated Purpose.** Not process any minor's personal data for an unstated and unrelated processing purpose.
- **System Design To Increase Use.** Not utilize any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature.
- **Geolocation.** Not collect a minor's precise geolocation data unless reasonably necessary to provide such online service, product or feature, but only for the time necessary to provide such online service, product or feature, and must indicate to the minor that such controller is collecting such precise geolocation data.

Additional Provisions

SB 3 also imposes requirements on online dating platform operators that offer services to users located in Connecticut and establishes a Connecticut Internet Crimes Against Children Task Force.

- **Online Dating.** Each online dating operator that offers services to Connecticut users shall maintain an online safety center which will provide (i) an explanation of the online dating operator's reporting mechanism for harmful or unwanted behavior, (ii) safety

advice for use when communicating online and meeting in person, (iii) a link to an internet website or a telephone number where a Connecticut user may access resources concerning domestic violence and sexual harassment and (iv) educational information concerning romance-related scams. A policy for the online dating platform's handling of harassment reports by or between users must also be adopted.

- **Task Force.** The Connecticut Internet Crimes Against Children Task Force is established within the Division of Scientific Services.

Cure Period

Between October 1, 2024, and December 31, 2025, the attorney general will grant a 30-day cure period for entities that have violated SB 3, provided that the attorney general has determined that the violation is capable of being cured. Starting on January 1, 2026, the state attorney general has the discretion to decide whether to grant a cure period. In determining whether to grant a cure period, the attorney general may consider (i) the amount of such violations that the applicable controller or processor is alleged to have committed, (ii) the size and complexity of such controller or processor (iii) the nature and extent of such controller or processor's processing activities, (iv) whether there is a substantial likelihood that such alleged violation has caused or will cause public injury, (v) the safety of persons or person, (vi) whether such alleged violation was likely caused by a human or technical error and (vii) the sensitivity of the data, as informed by a multi-factor framework.

Key Takeaways

As concerns regarding data privacy become more pervasive, SB 3 provides robust protections for consumer health-related data and online safety for minors. In particular, the amendment's protection of health data reflects a growing state-level trend of seeking to protect health data beyond what might be protected under HIPAA.

Return to Table of Contents

Colorado Comprehensive Privacy Law Goes Into Effect

On July 1, 2023, Colorado's consumer privacy law, the Colorado Privacy Act (CPA), went into effect, following the issuance of a number of related regulations by the Colorado attorney general in March 2023 (the CPA rules). Below is a summary of some of the key provisions of the CPA, which was first enacted in June 2021.[3]

Coverage

The CPA applies to both "controllers" and "processors" that conduct business in Colorado, as well as those that conduct business outside of the state but produce commercial products or services intentionally targeted to Colorado residents if they either:

- control or process the personal data of at least 100,000 Colorado residents per calendar year; or
- derive revenue from the sale of personal data and control or process the personal data of at least 25,000 Colorado residents.

The CPA is unique among state-level consumer privacy laws to date in that it also applies to nonprofit organizations.

Key Terms

A "controller" is defined as any "person that, alone or jointly with others, determines the purposes and means of processing personal data," while a "processor" is defined as any "person that processes personal data on behalf of a controller." Additionally, a "consumer" is defined broadly as "an individual who is a Colorado resident acting only in an individual or household context," while "personal data" is defined as "information that is linked or reasonably linkable to an identified or identifiable individual," with exclusions for publicly available information and pseudonymous data.

Consumer Rights

The CPA establishes a series of personal consumer data privacy rights:

- **Right to Opt-Out:** The right to "opt out of the processing of personal data concerning the consumer for purposes of: (a) targeted advertising; (b) the sale of personal data for monetary or other valuable consideration; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer." A sale excludes personal data transfers as part of a merger, acquisition, bankruptcy or other transaction in which a third party assumes control of the controller's previous assets.
- **Right of Access:** The right to "confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data."
- **Right to Correction:** The right to "correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data."
- **Right to Deletion:** The right to "delete personal data concerning the consumer."

[3] See our June 2021 *Privacy & Cybersecurity Update* article "Colorado Expected To Become Third State To Adopt Comprehensive Privacy Law."

- **Right to Data Portability:** The right to "obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance."

Consumers may exercise these rights under the statute by submitting verifiable requests to controllers. These controllers would then have 45 days to respond to the requests, with the response window allowed to be extended so long as the controller provides the consumer with timely notice within that initial period.

Consent

Controllers may provide consumers with the option to consent to the processing of their personal data so long as they also provide "a clear and conspicuous notice" that outlines what categories of data will be processed, for what purposes they will be processed and by what means the consumer can subsequently elect to withdraw consent.

Obligations of Covered Businesses

The CPA imposes numerous obligations on businesses covered under the statute. These include a duty of transparency to provide consumers with a privacy notice when personal data is being collected or processed. The statute also authorizes a duty of purpose specification, duty of data minimization, duty to avoid secondary use, duty of care, duty to avoid unlawful discrimination and a duty regarding sensitive data.

The statute compels controllers to conduct a data protection assessment for each of its processing activities involving personal data that present a heightened risk of harm to consumers. These activities include, but are not limited to, processing sensitive data, selling personal data and processing personal data for targeted advertising or certain profiling. The Colorado attorney general and district attorneys are solely authorized to review these data protection assessments.

Cure Period and Civil Penalty Framework

The CPA requires the Colorado attorney general and district attorneys to provide notice to controllers of any alleged violations by the controllers prior to bringing enforcement actions. Such controllers would then have 60 days to cure the alleged violations. The cure period will only remain in existence until January 1, 2025. The Colorado attorney general (or a district attorney) can seek up to $20,000 in civil penalties for each potential violation and up to $500,000 for any related series of violations.

Key Provisions of the CPA Rules

Strict Consent Requirements

The CPA rules specify that controllers must obtain affirmative consent from consumers prior to processing their personal data. The CPA rules identify five distinct elements that constitute consent. Accordingly, consent must: (1) be obtained through the consumer's clear, affirmative action, (2) be freely given by the consumer, (3) be specific, (4) be informed and (5) reflect the consumer's unambiguous agreement.[4] Thus, a standard-form acceptance of general terms would not constitute consent under the CPA rules.

The CPA rules specify that affirmative consent by consumers is required prior to the processing of children's sensitive or personal data, selling a consumer's personal data, processing personal data for advertising, profiling, and processing personal data for unnecessary or incompatible purposes.

Profiling

The CPA rules allow for a consumer to opt out of profiling under particular circumstances, such as profiling that is based on either "Solely Automated Processing" or "Human Reviewed Automated Processing."[5] If a controller denies the opt-out request, the consumer must be informed of, among other things, what went into the decision-making process to deny as well as the extent of human involvement in the decision-making process.

Universal Opt-Out Provisioning

The Colorado General Assembly specifically tasked the Colorado attorney general with developing technical specifications for at least one universal mechanism that consumers can use to opt out of the sale or use of their data for targeted advertising.[6] The attorney general will release an approved list of "Universal Opt-Out Mechanisms" by January 1, 2024. Beginning on July 1, 2024, consumers will be able to opt out through one of the mechanisms, which will apply to all controllers subject to the CPA.

Loyalty Program Disclosures

The CPA rules require that businesses offering consumers loyalty programs make disclosures[7] of: (1) the categories of personal data or sensitive data collected through loyalty programs that will be sold or processed for targeted advertising, (2) categories

[4] CPA Rule 7.03(A).
[5] CPA Rule 9.04(B).
[6] CPA Rule 5.01.
[7] CPA Rule 6.05

of third parties that will receive the consumer's personal data and sensitive data, (3) a list of any bona fide loyalty program partners and (4) the bona fide loyalty program benefits provided by each bona fide loyalty program partner. Businesses will need to review their respective loyalty programs to ensure that they are providing the necessary disclosures.

Elaboration of Data Protection Assessments

The CPA rules provide specific details for how controllers should construct their data protection assessments. Accordingly, they set forth the scope[8] of what types of data the assessments should cover, providing extensive detail[9] as to what information should be included. At a minimum, a data protection assessment must include a summary of the processing activity, the categories of personal data being processed, the core purposes of the processing activity, a description of how the benefits of the processing outweigh the risks and numerous other requirements. Upon request by the Colorado attorney general, controllers are required to provide their data protection assessments within 30 days of said request.

Key Takeaways

As stated previously, Colorado's law adds to the patchwork of state-level privacy laws that companies must adhere to. Those that are covered by the CPA should be mindful of the requirements set forth in the CPA and in the accompanying CPA rules.

Return to Table of Contents

Verizon Releases Annual Data Breach Investigations Report

The 2023 Verizon Data Breach Investigations Report examines 5,199 confirmed breaches and highlights the continuance of ransomware as the most common form of system intrusion, the growth of pretexting in social engineering incidents, lessons learned from the Log4j vulnerability exploitation, the increase in breaches involving cryptocurrency and the importance of protecting portable assets such as work phones and computers.

For the last 15 years, Verizon has issued a Data Breach Investigations Report containing a summary and analysis of cybersecurity breaches from the previous year. Each report identifies current trends in attack types, details the risks that breaches can present for companies and suggests ways for organizations to strengthen their systems and protect themselves against future breaches. The 2023 report provides some valuable insights into the current state of cybersecurity and notes the following:

Remote Work Risks

The report identified a large number of incidents involving the loss and theft of physical assets in 2022 that were likely due to the increase of remote work. The report recommends that organizations protect against the risk of theft by reminding employees to be mindful of their devices while working remotely, programming portable devices so that they can be wiped in the case of theft or loss, and training employees about the importance of securing paper assets, which are unshielded and cannot be wiped clean if lost or stolen.

Pretexting

The report noted that social engineering incidents have increased generally, and while phishing is still prevalent, most of the incidents in 2022 (about 60%) involved pretexting. Pretexting is the practice of an attacker tricking a person into believing that an urgent request is coming from someone they know who has an immediate financial need, but it is actually the attacker impersonating this familiar person. This style of social engineering requires more skill than a deceptive phishing email because it involves investigating the individual person under attack. The report highlights that quick detection continues to be essential in minimizing the effects of social engineering attacks such as pretexting, and employees should be trained to recognize these types of attacks so that incidents can be promptly reported and, ideally, avoided. The report explicitly recommends making social engineering detection training more collaborative and less compulsory to promote active reporting and strengthen organizations' ability to defend against these attacks.

Cryptocurrency-Involved Breaches

According to the report, there has been a 400% increase in cryptocurrency-involved breaches since last year. In one method of attack, phishing in chat rooms and other similar programs has resulted in assets being diverted from the cryptocurrency holder's wallet. The report recommends that wallet information should be treated as securely as bank account information, and that organizations' employees should be trained about the dangers of phishing and pretexting incidents in chat rooms such as Slack and Discord.

Ransomware

The report indicates that ransomware is still the most common form of a system intrusion attack, accounting for more than 80% of incidents overall. The costs to recover an organization's systems after a ransomware attack also are increasing as hackers are becoming more automated and efficient. The report recommends

[8] CPA Rule 8.02.

[9] CPA Rule 8.04.

that organizations have well-tested, recent backups to restore their systems in case of an attack — however, this defensive measure still does not protect against hackers threatening to release information they have obtained from these systems. As a preventative measure, organizations should focus on maximizing their fundamental security strength and diligently training employees to prevent the installation of dangerous malware.

Log4j

The exploitation of the Log4j vulnerability allowed hackers to find gaps in many organizations' security systems and gain entry, with incidents that impacted numerous programs and applications across a variety of companies. In response, the report suggests that organizations should maintain an updated software bill of materials to easily see every element of their software, which would allow for quick notations of vulnerabilities in organizations' systems and allow for fixes to prevent against a similar attack in the future.

Stolen Credentials

According to the report, the most common way (about 45% of incidents) that attackers gained access to an organization's system was by using stolen employee credentials. The report recommends that companies should use multifactor identification to limit a potential attacker's ability to use any stolen credentials that they may gain access to. Also, in some instances that occurred last year, social engineering was used to force employees to assist an attacker in bypassing organizations' multifactor identification system, meaning enhanced phishing and pretexting training should further strengthen organizations' defense against hackers using stolen credentials.

Internal Attacks

Attacks originating from inside organizations grew in 2022 in connection with fraudulent transfers of funds to attackers' bank accounts. To limit this, the report recommends that companies implement controls to detect if an employee is inappropriately accessing certain company assets.

State-Sponsored Attacks

Although there was concern that state-sponsored attacks would increase due to growing global conflicts, the report revealed that in 2022 there were actually more internal misuse errors than state-sponsored attacks.

Key Takeaways

As attackers modify the methods they employ to infiltrate an organization's systems, the report outlines how employee trainings focused on securing portable assets and identifying social engineering attacks could help prevent many breaches from happening. Additionally, an organizations that maintain records of their software's elements and detect employees who are inappropriately accessing company assets can help to fortify against both internal and external attacks.

Return to Table of Contents

Eleventh Circuit Addresses Negligence Claims in Employer Data Breach Cases

In a recent decision, the U.S. Court of Appeals for the Eleventh Circuit reversed the dismissal of negligence claims of the plaintiffs in a data breach case, outlining a new legal standard for such cases under Georgia law. The court explained that there may be a duty to protect employees' personally identifiable information (PII) when it is foreseeable, given the size and sophistication of a company and how it could be the target of a cyberattack. The decision effectively reduced the burden on plaintiffs to provide specific facts about foreseeability in the pleading stage. A subsequent decision in the Eleventh Circuit also highlighted the importance of the new legal standard for ransomware attacks on employers.

The Duty of Care and Employee PII

On June 5, 2023, in *Ramirez v. The Paradies Shops, LLC*,[10] the Eleventh Circuit reversed the dismissal of a negligence claim involving a ransomware attack targeting sensitive employee PII in a class action against Paradies, a retail and concessionaire services company. The lead plaintiff in the case was a former employee who provided his employer with sensitive PII as a condition of his employment. In October 2020, the company was the victim of a ransomware attack that gained access to employee PII, including the names and Social Security numbers of more than 76,000 current or former employees. After being notified of the cyberattack, the plaintiff filed claims for breach of implied contract and negligence in a putative class action on behalf of himself and those who had their data accessed as part of the breach.

The company moved to dismiss the negligence claim, arguing that it did not owe its employees a duty to safeguard data under Georgia law. The U.S. District Court for the Northern District of Georgia agreed and dismissed the claim, stating that the plaintiff did not adequately allege that Paradies could have foreseen the harm. The district court reasoned that the allegations in the complaint were not foreseeable because the company did not have "actual knowledge of public announcements about data breaches nor any particular reason to be aware of them."

[10] *Ramirez v. The Paradies Shops, LLC*, No. 22-12853 (11th Cir. June 5, 2023).

Eleventh Circuit Reverses Dismissal

On appeal, the Eleventh Circuit disagreed and reversed the dismissal of the negligence claim, stating that the "district court asked for too much specificity at the pleading stage" with respect to foreseeability of the ransomware attack. Although there was no clear state-level legal guidance regarding the duty of employers to safeguard PII, the Eleventh Circuit examined the case using common-law tort principles. The court reasoned that an employer "owes a duty of care to those with whom it has a special relationship" and "leaving [a] substantial database unsecured created a 'potentially dangerous situation' whereby cybercriminals could improperly access and exploit" PII. The court explained that when examining the sufficiency of foreseeability of a cyberattack, it would be an impossible burden for plaintiffs to meet to plead "every aspect of a company's security history and procedures" that might make a data breach foreseeable. The court therefore held that the plaintiff had sufficiently pled facts for the negligence claim to survive a motion to dismiss, given the existence of a special relationship and a foreseeable risk of harm.

The Impact of *Ramirez*

In a separate class action lawsuit, *Sean Sheffler, et al v. Americold Realty Trust*,[11] plaintiff Sean Sheffler, on behalf of himself and other former employees, brought a suit against Americold Realty Trust, a warehousing company headquartered in Atlanta, Georgia, asserting negligence and breach of contract claims stemming from a ransomware attack targeting the company. The plaintiffs had worked for Americold for 10 years prior to the attack and had been required to provide sensitive PII as a condition of employment. Americold learned of a possible ransomware attack on its network on November 16, 2020, and, after conducting an investigation, learned that the plaintiffs' PII, including the plaintiffs' names, Social Security numbers and dates of birth, was exposed to the third-party attackers. Americold notified its employees of the cyberattack in March 2021, approximately four months after the incident took place.

Americold filed a motion to dismiss arguing that the plaintiffs lacked standing to bring the claim, stating (i) there was no common law negligence duty to safeguard the PII in any relevant state, (ii) the plaintiffs had not suffered any cognizable injury and (iii) there was no meeting of the minds necessary to establish an implied contract. The U.S. District Court for the Northern District of Georgia agreed with Americold and dismissed the case, stating that the plaintiffs' negligence claim failed because the harm was not foreseeable — the complaint did not provide any factual allegations to plausibly support a conclusion that the company had "reason to be on guard for this type of ransomware attack." Following the court's decision to dismiss the case, the plaintiffs requested leave to amend their complaint to address the foreseeability issue, arguing that the company had reason to know that it could be the target of a data breach and failed to take steps to secure their network. Ultimately, the district court denied the plaintiffs' post-judgment motion for leave to amend, stating that the plaintiffs' had failed to argue the court's dismissal contained manifest errors of law or fact, or that they had newly discovered evidence.

Eleventh Circuit Grants Leave to Amend

On June 9, 2023, shortly after *Ramirez* was decided, a panel of judges for the Eleventh Circuit reversed the district court's denial of the plaintiffs' motion for leave to amend. The plaintiffs argued that a motion for relief after dismissal should be construed liberally and, absent a substantial reason to deny leave to amend, it should be granted freely. The court agreed with the plaintiffs, explaining that "the plaintiffs would have been hard-pressed to predict that they might need to amend their complaint to add more specific foreseeability allegations." Moreover, the court stated that the recent opinion in *Ramirez* had "undermined" the district court's dismissal of the negligence claim. The court also noted that the plaintiffs' should have the opportunity to address the new legal standard for data breach negligence claims. While not addressing the merits of the claim, the panel remanded the case so that the plaintiffs could proceed on their amended complaint.

Key Takeaways

The Eleventh Circuit decision in *Ramirez* created a new legal standard under Georgia law in data breach negligence cases that lowers the burden on employees to plead specific facts showing that a cyberattack on their employer was foreseeable. A company may not be shielded from liability when, given its size and sophistication, it would be foreseeable that it could be the target of a cyberattack. The importance of the new legal standard was highlighted in *Sheffler*, where the court allowed a class action to go forward to address the foreseeability of a ransomware attack on the company. Going forward, plaintiffs may take advantage of this lower pleading standard and courts may be more flexible in data breach negligence cases when ruling on a motion to dismiss.

Return to Table of Contents

[11] No. 22-11789 (11th Cir. June 9, 2023).

Credit Rating Agency AM Best Reports on US Cyber Insurance Market Trends

On June 13, 2023, insurance credit rating agency AM Best published a cyber insurance report based on U.S. data reported to the National Association of Insurance Commissioners. The report helps to provide an overall update on the cyber insurance market.

Market Growth and Pricing

AM Best reported strong cyber insurance market growth in 2022, with premiums increasing by nearly 50% year over year to $7.2 billion — more than triple what it was three years ago. This growth, which AM Best attributed to the prevalence of remote working and online shopping, along with the growing threats of hacking, "outpaced the rest of commercial premium by a wide margin." With the cyber universe continuing to expand and develop, the demand for cyber coverage will only continue to grow, AM Best posited in the report.

According to the report, cyber pricing continues to rise, with a 8.4% increase in the first quarter of 2023. However, considering all economic factors, such as inflation, pricing is effectively flat. The 2021 and 2022 price increases — an effort by insurers to combat losses following the wave of ransomware attacks during the early stages of the COVID-19 pandemic — brought much needed capacity to the cyber insurance market, predominantly in surplus lines. Surplus lines insurance is issued by non-admitted (as opposed to admitted) insurers that are not licensed by the department(s) of insurance of the state(s) in which they operate. AM Best reported that premiums written by surplus lines insurers increased by over 500% in 2021 and 2022, and that surplus lines writers now account for a majority of cyber premiums. However, admitted insurers still write 70% of premiums on package policies (policies providing cyber coverage in addition to one or more distinct coverages), as opposed to stand-alone policies (policies providing cyber coverage only).

In addition to price increases, cyber underwriters have used several other methods to rein in losses and return to profitability, including lowering limits, increasing policyholder retention and improving risk selection.

Stand-alone cyber policies (as opposed to package policies) have become the preferred policy among larger policyholders. In 2022, stand-alone policies accounted for over 70% of cyber premiums. Package policies account for a significantly lower average premium than most stand-alone policies, with package policies accounting for only 35% of total premiums but almost 90% of cyber insurance policies. The report notes that this shift toward stand-alone policies could help minimize disputes and litigation costs given that standalone policies contain affirmative coverage grants and exclusions, which may lead to less ambiguity about what the policy covers.

Market Dynamics

According to AM Best, the top 20 insurers wrote approximately 78% of the entire cyber market in 2022. The top four insurers, based on premium, (unchanged from 2021) are Chubb, Fairfax, XL and Tokio Marine, but, by policy count, Hartford wrote the most policies by a wide margin (also unchanged from 2021). AM Best expects to see the field of cyber insurers continue to grow as the demand for cyber coverage continues to increase.

According to the report, the difficult marketplace in 2021 and 2022 made captive insurance an attractive cyber management option for corporations, providing flexibility to navigate underwriting cycles and maintain access to coverage the corporation requires.

Emerging Issues

While 2022 saw a decline in ransomware claims, first-party claims (such as data and security breach notification and remediation costs) nevertheless accounted for close to 75% of the nearly 27,000 claims reported during the year. AM Best attributed this to an increase in business email compromise claims. The report notes that the number of third-party claims (such as lawsuits alleging privacy and security violations) is still significant, but such claims have lengthier development.

According to the report, systemic risk remains an ongoing concern, citing cyber catastrophes, such as NotPetya, that can have worldwide implications, and attacks on cloud service providers, which can cause outages for multiple businesses. Another emerging issue is war risk insurance coverage. According to the report, the scope of this coverage varies by insurer, with some sticking with traditional war exclusions and others covering certain war exposures. AM Best predicts that policyholders and insurers alike will be expected to carefully scrutinize war-related policy language and notes that the identity of the attacker (an individual or state actor), as well as the attacker's intentions (to perpetrate war or for profit), may determine the final payout under the policy. Ultimately, however, coverage may be dependent at least in part on an insurer's risk appetite and, to a certain extent, the coverage that reinsurers are willing to provide. AM Best further stated that the increased use of artificial intelligence and "deepfakes" in phishing scams presents additional threats to security systems, which will require insurers to be more vigilant about underwriting and pricing cyber insurance.

Key Takeaways

As the report underscores, the cyber insurance market is constantly evolving, and 2022 saw significant growth and change — from the rapid surge in demand and increase in written premiums to pricing hikes, a shift to stand-alone policies, and emerging risks, such as war, artificial intelligence and "deepfakes" — posing new challenges. It remains to be seen what the state of the market will be next year, but AM Best predicts that the demand for cyber coverage will only continue to grow.

Return to Table of Contents

Business Liability Insurer Must Defend BIPA Litigation, Seventh Circuit Finds

On June 15, 2023, the U.S. Court of Appeals for the Seventh Circuit issued an opinion holding that Citizens Insurance Company of America (Citizens) must defend its insured, IT services firm Wynndalco Enterprises, LLC (Wynndalco), in two underlying putative class actions alleging violations of Illinois' Biometric Information Privacy Act (BIPA), pursuant to the terms of its business liability insurance policy.[12]

The Underlying BIPA Class Actions

The coverage dispute stems from two underlying putative class actions, each filed by Illinois residents on behalf of themselves and other state residents whose facial images have been collected and scanned into a database created by Clearview AI, Inc. (Clearview), an artificial intelligence firm specializing in facial recognition software. Clearview allegedly created a database of over 3 billion facial scans, amassed by "scraping" photographs from the internet, as well as a facial recognition app, which enables end-users to identify persons by comparing their facial scans to those included in Clearview's database. The Chicago Police Department, through its purchasing agent, allegedly gained access to Clearview's database and app by means of a contract with Wynndalco.

Both lawsuits allege that Wynndalco's role in the transaction ran afoul of the BIPA, including by capturing, collecting, receiving, storing, disclosing and/or using biometric identifiers and biometric information without complying with the BIPA's statutory requirements and/or profiting from the plaintiffs' biometric identifiers or biometric information in the Clearview app.

[12] *Citizens Ins. Co. of Am. v. Wynndalco Enters., LLC*, ---F.4th--- (7th Cir. 2023).

Citizens Denies Coverage for the BIPA Lawsuits

Wynndalco tendered the BIPA lawsuits to its business liability insurer, Citizens, for coverage. Citizens denied coverage on the ground that the lawsuits fell within a catch-all provision in the policy's "Violation of Statutes" exclusion. That exclusion bars coverage for "personal and advertising injury" arising out of any act or omission that actually or allegedly violates the Telephone Consumer Protection Act, the CAN-SPAM Act of 2003, the Fair Credit Reporting Act or the Fair and Accurate Credit Transaction Act (and amendments thereto), as well as the subject catch-all provision that states "[a]ny other laws, statutes, ordinances, or regulations, that address, prohibit or limit the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information."

Thereafter, Citizens filed suit against Wynndalco in the U.S. District Court for the Northern District of Illinois seeking a declaratory judgment that Citizens has no duty to defend or indemnify Wynndalco in the BIPA lawsuits. Wynndalco counterclaimed, seeking a declaration to the contrary and damages for breach of contract.

The District Court Enters Judgment for Wynndalco

On the parties' cross-motions for judgment on the pleadings, the district court entered judgment for Wynndalco. After considering the policy language, case law and canons of construction, the court found that the "Violation of Statutes" exclusion was "intractably ambiguous" and could not be enforced against Wynndalco. As a result, the district court concluded that Citizens had not met its burden of establishing that the claims against Wynndalco were excluded from coverage and held that Citizens had a duty to defend Wynndalco in the BIPA lawsuits.

The Seventh Circuit Affirms

On appeal, the Seventh Circuit affirmed. At the outset, the court rejected Citizens' argument that the exclusion should be enforced as written, reasoning that a literal reading of the exclusion's catch-all provision would effectively eliminate coverage for a number of statutory injuries expressly included in the definition of "personal and advertising injury" that the policy purports to cover. For that reason, the Seventh Circuit agreed with the district court that the exclusion is ambiguous.

The Seventh Circuit then turned to canons of construction in an attempt to resolve the ambiguity, but to no avail. The court rejected Citizens' argument, in reliance on the canon of *ejusdem generis* (a Latin phrase meaning "of the same kind"), that because each of

the statutes expressly enumerated in the exclusion regulate privacy in some way, the court should construe the catch-all provision to reach only statutes that likewise regulate privacy, such as the BIPA. The court reasoned that the provision contained no mention of privacy and that only if one "looked beyond the facially expansive sweep of the catch-all provision ... might it be possible to arrive at the narrowing privacy gloss for which Citizens advocates."

Unable to resolve the ambiguity, the court construed the ambiguity against Citizens and in favor of the insured, stating "as the catch-all provision says nothing about injuries arising from statutes regulating privacy interests, and the policy defines a covered 'personal and advertising injury' so as to include an injury arising out of the '[o]ral or written publication, in any manner, of material that violates a person's right of privacy' ... we conclude that the injuries alleged in [the BIPA lawsuits] at least potentially fall within the coverage of the Citizens policy. Citizens thus owes its insured, Wynndalco, a duty to defend it against those complaints."

Key Takeaways

As the *Wynndalco* opinion illustrates, the coverage landscape for BIPA claims continues to evolve. While the *Wynndalco* decision is a win for policyholders, ultimately the policy language will dictate coverage for BIPA claims. Thus, it is important for policyholders and insurers alike to carefully review coverage grants and exclusionary language to ensure they accurately reflect the parties' intent with respect to coverage for BIPA liabilities.

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Nicole L. Grimm
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000