The Cyber Regulatory Landscape Entering 2023

December 2022

LOCKTON®

Cyber insurance is generally known for its first-party incident response coverage. An often overlooked yet critical component, however, is its regulatory liability coverage.

As the world has become more connected to the internet, the need for laws governing the storage, processing and handling of personal data has been amplified. This has resulted in the proliferation of federal, state and international data privacy laws.

Beyond the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) and sector-specific laws — such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act, which regulates the use of data by financial institutions — several new data privacy laws and regulations have emerged in the United States and internationally in 2022. These proposed and enacted laws and regulations have familiar elements, but also reflect the continued evolution of language to suit the present landscape of storing and selling sensitive personal data.

In this report, Lockton's Cyber & Technology Practice summarizes key developments across the cyber and data privacy regulatory landscape in 2022.

U.S. Federal Laws

American Data Privacy and Protection Act (ADPPA)

Despite attempts to create bipartisan support and agreeable language for a national data privacy framework, the U.S. has yet to enact a law analogous to the EU's GDPR. In June 2022, however, the American Data Privacy and Protection Act was introduced in the House of Representatives and has since gone through several iterations.

The ADPPA — in its current form — takes a different approach from past privacy bills: It focuses on data minimization rather than consent, would apply to a range of organizations that collect and hold data, including nonprofits, and would extend to information that identifies or is linked (or reasonably linked) to an individual. Further, the bill does not specifically enumerate protection for employee data but does preclude certain defined entities from collecting, processing or transferring covered data unless it is limited to what is reasonably necessary and proportionate to achieve a specified legitimate purpose. The bill designates the Federal Trade Commission (FTC) as its the enforcement authority, responsible for issuing clear guidance regarding what would qualify as being reasonably necessary and proportionate.

Unlike many enacted and proposed state data privacy laws, the ADPPA would create a limited private right of action; awards are limited to attorneys' fees, injunctive relief and compensatory damages, and both the FTC and a state attorney general must be advised that a suit is being filed and given 60 days to review for possible intervention.

Although passage with bipartisan support remains a challenge, the ADPPA has more support than previous federal data privacy law attempts. As it would be the first nationwide data privacy-specific law, the issue of preemption will be key to its viability. In its current form, the ADPPA would preempt some state data privacy laws — including the California Privacy Rights Act (CPRA) and Virginia Consumer Data Privacy Act (VCDPA) — but not others, such as the Illinois Biometric Privacy Act (BIPA). It would also not preempt state breach notification requirements or criminal laws pertaining to identity theft or fraud.

Despite the lack of a federal privacy law in the U.S., the FTC still protects consumers against unfair and deceptive trade practices, including those related to data privacy and security. The FTC has historically exercised its enforcement authority against entities that fail to impose reasonable data security measures or transfer personal information to an acquiring entity without express disclosure of a consumer data privacy policy. It has also implemented more stringent data privacy requirements for auto dealerships and higher education institutions.

U.S. State Laws

California Privacy Rights Act of 2020 (CPRA)

SIGNED INTO LAW: DEC. 16, 2020 | **TAKES EFFECT:** JAN. 1, 2023

California was the trendsetter for U.S. state data privacy laws when the CCPA was enacted and signed into law in June 2018. The CCPA provides consumers with protections against their personal information being collected, sold or used by a covered business. In 2020, California residents voted to approve passage of the CPRA, which amended the CCPA and created the California Privacy Protection Agency (CPPA) to replace the California attorney general as the law's enforcement body.

The CPRA will continue to apply to for-profit entities doing business in California, that collect California consumers' personal information and that meet specified thresholds. Under the CPRA, those thresholds will include:

- Exceeding $25 million in revenue;
- Buying, selling and/or sharing the personal information of at least 100,000 or more California consumers or households; and
- Deriving 50% or more of their annual revenue from sharing consumer personal data.

Covered entities are subject to myriad requirements related to the retention of data, purpose limitation and deletion requests to service providers and third parties that have received information.

Critical additions in the CPRA include not only the creation of the CPPA, but also the removal of the mandatory 30-day cure period, which will make strict compliance with the law even more important. In short, the CPRA is clearly an enhancement for consumers, and will be far more arduous and complex for businesses to comply with than the CCPA and other state laws.

The CPRA will not be enforced until July 1, 2023, giving businesses six months to achieve compliance.

For more information, read Lockton's previously published report on the CPRA.

Virginia Consumer Data Protection Act (VCDPA)

SIGNED INTO LAW: MARCH 2, 2021 | **TAKES EFFECT:** JAN. 1, 2023

The VCDPA is the first wide-ranging state privacy law enacted after the CCPA. Businesses are required to comply with the VCDPA even if they are not incorporated or based in Virginia if either:

A. The entity conducts business in Virginia; or

B. Markets its products or services there; and

   i. Data of at least 100,000 residents of Virginia;

   ii. Derives more than 50% of its gross revenue from selling personal data and controls or processes the personal data of 25,000 Virginia residents.

The law requires businesses to comply with certain enumerated consumer rights, including the ability to delete or access personal data, correct inaccuracies and opt out of the sale of personal data, among others. Importantly, the VCDPA will also require businesses to employ appropriate data security controls and practices and limit the data being processed to only those pieces needed for a specific purpose.

A key difference from the CCPA is that the VCDPA will not extend to Virginians a private right of action. Instead, the Virginia attorney general is charged with enforcement, with organizations having a 30-day cure period.

Colorado Privacy Act (CPA)

SIGNED INTO LAW: JULY 8, 2021 | **TAKES EFFECT:** JULY 1, 2023

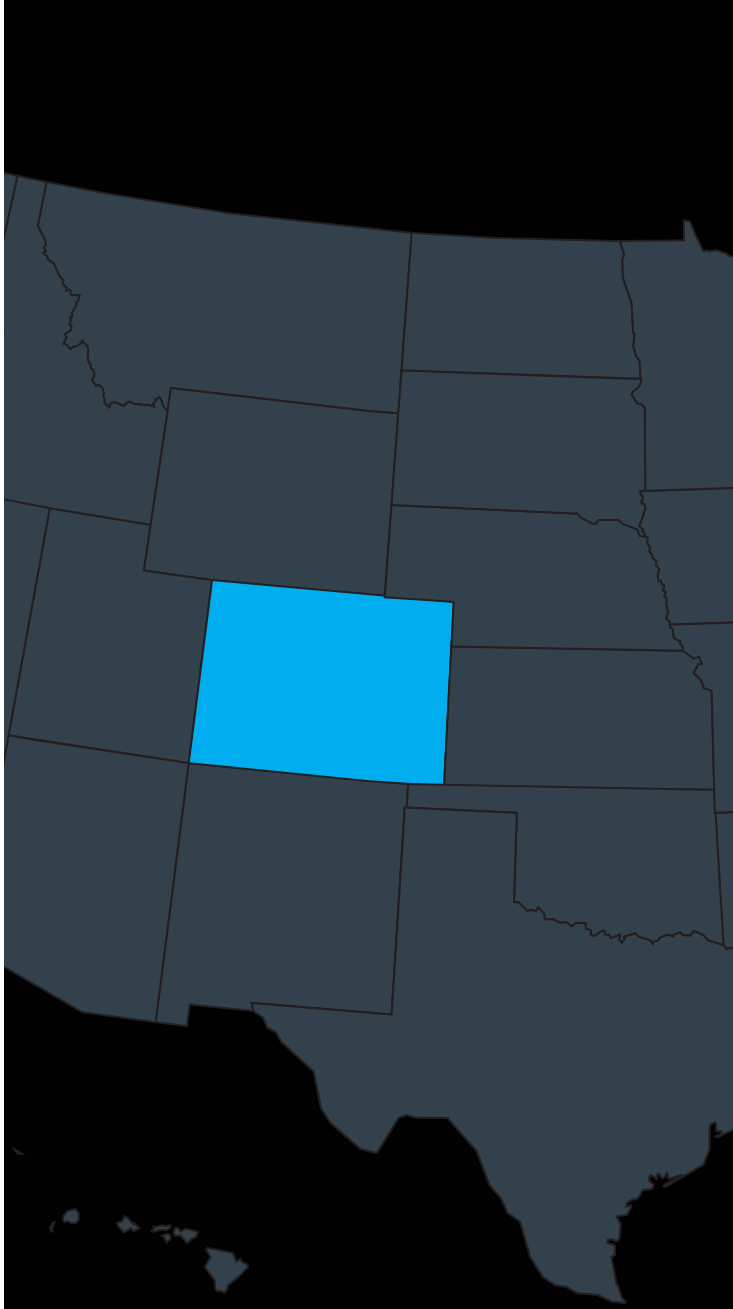
The CPA effectively is an amalgam of the GDPR, the CCPA and the VCPDA. Like the VCPDA, the law will apply to those either conducting business in Colorado or targeting the sale of products and services to Colorado residents. The CPA includes triggering language similar to the VCDPA: An entity must also control or process the personal data of 100,000 or more consumers or derive or receive discounts from the sale of personal data and control the data of at least 25,000 consumers to be subject to the law.

The CPA, however, is stricter than the VCDPA in that it does not include a revenue threshold amount or percentage when selling personal data that must be breached before compliance becomes mandatory.

If the above criteria are triggered, the CPA will require businesses to abide by and make available access to consumer rights such as the right to opt out, access data and correct/delete data. The CPA will also require that businesses complete data protection assessments when processing or selling sensitive personal data that presents heightened risk of consumer harm.

Additionally, businesses will need to provide consumers with a reasonably accessible and clear privacy notice and limit personal data collection to only that which is relevant and "reasonably necessary in relation to the specified purposes for which the data are processed."

Again, like VCDPA, there will not be a private right of action; the Colorado attorney general's office is charged with enforcement. The CPA, however, will be more flexible — at least until 2025 — by allowing for a 60-day cure period.



For more information, read Lockton's previously published report on the VCPDA and CPRA.

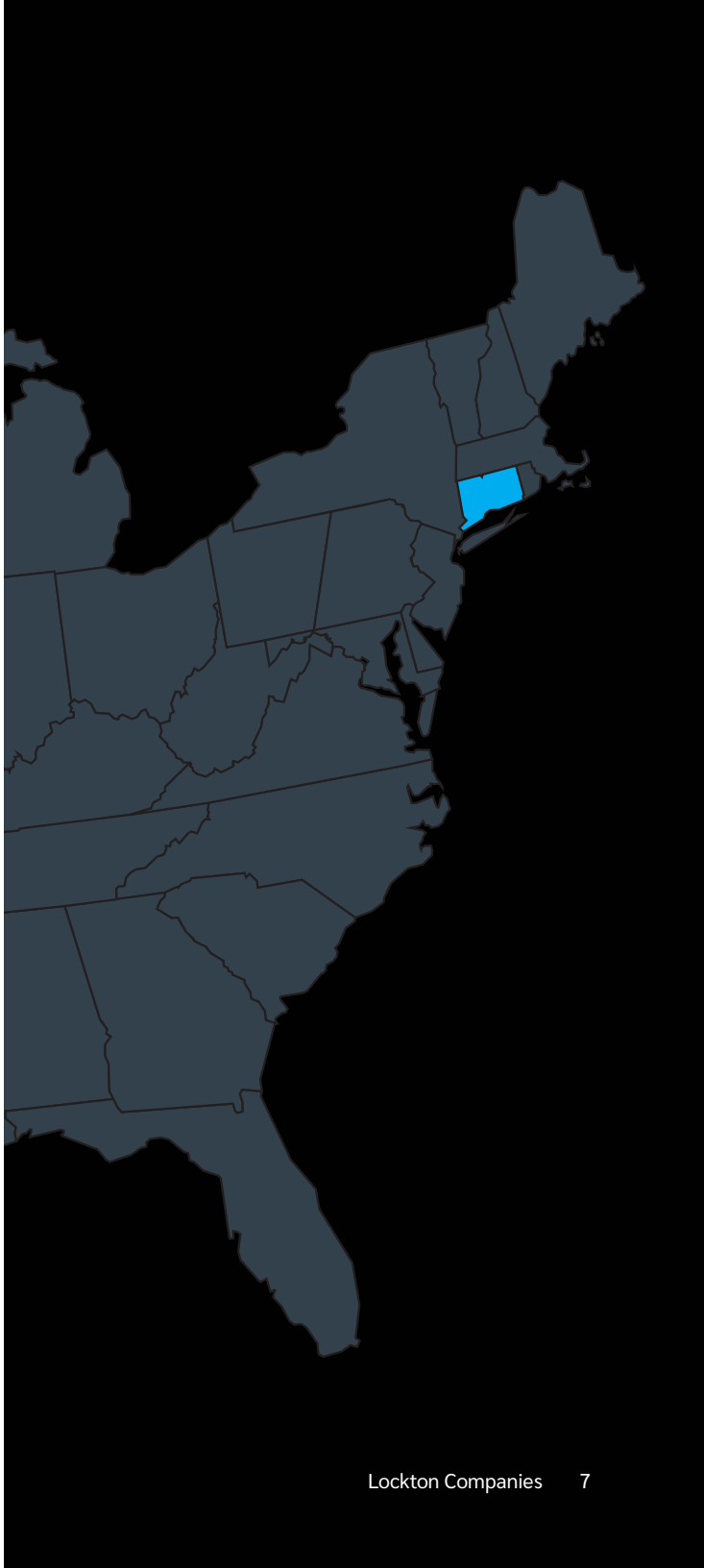
Connecticut Data Privacy Act (CTDPA)

SIGNED INTO LAW: JUNE 17, 2022 | **TAKES EFFECT:** JULY 1, 2023

The CTDPA will apply to Connecticut businesses or those offering products and/or services to Connecticut residents that either (i) control or process data of more than 100,000 Connecticut consumers or (ii) derive 25% of their gross revenue from the sale of personal data and control or process more than 25,000 consumers' data.

The law excludes personal data processed solely for payment transactions. Therefore, an entity processing payment transactions for the purpose of completing a sale will not be subject to the CTDPA's requirements.

The CTDPA will provide consumers with various new rights, including the ability to confirm processing, access/correction and deletion, and prohibits discrimination by businesses against consumers for exercising their rights under the act. The law also allows consumers to opt out of the sale of personal data or targeted advertising.



Utah Consumer Privacy Act (UCPA)

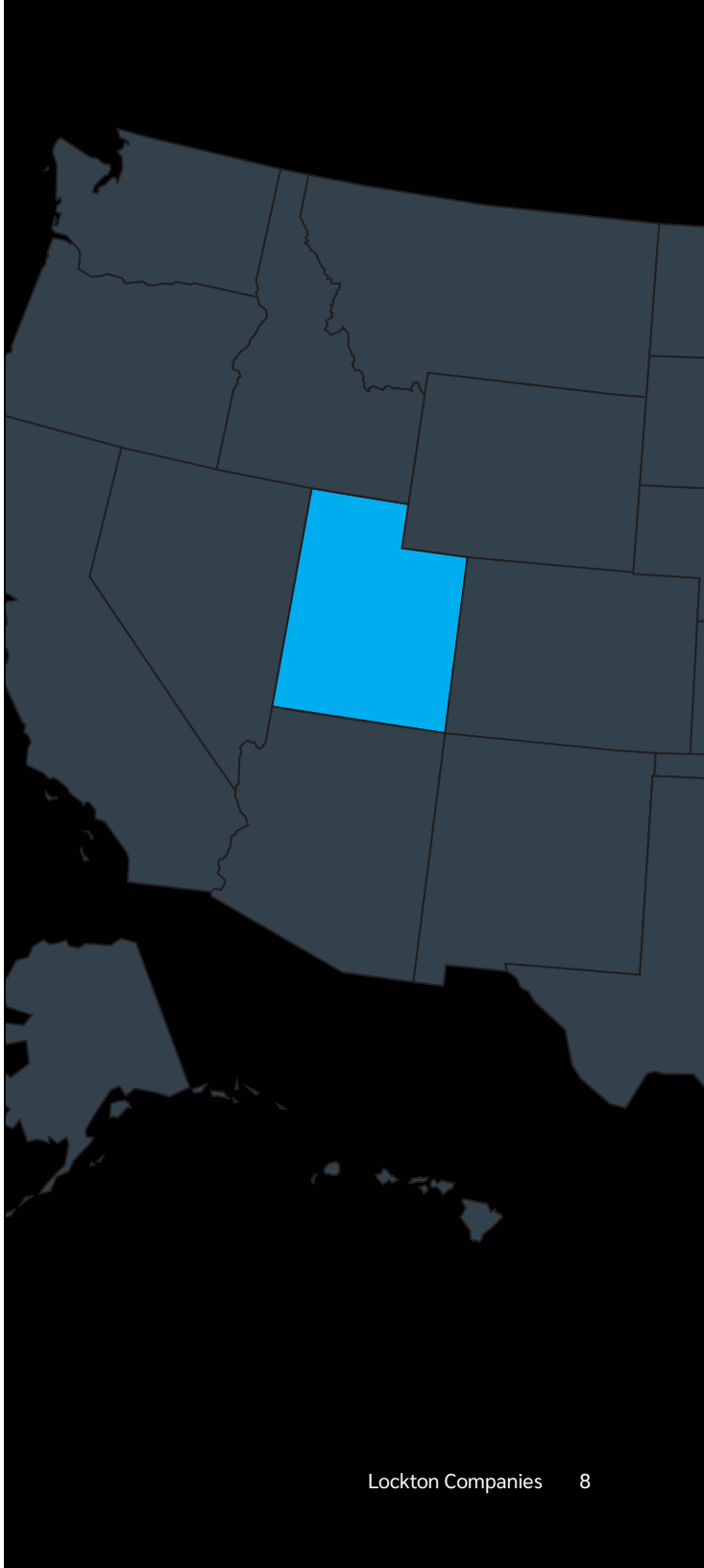
SIGNED INTO LAW: MARCH 24, 2022 | **TAKES EFFECT:** DEC. 31, 2023

The UCPA will apply to organizations with $25 million or more in revenue that conduct business in Utah or offer products and services to Utah residents. Organizations that control or process the data of 100,000 or more Utah consumers or process the data of 25,000 or more Utah consumers and derive more than 50% of their annual revenue through the sale of personal data will also be subject to the law.

Like other state laws, the UCPA requires that data be linked or reasonably linkable to an identifiable individual and will provide consumers with rights related to access/deletion, data portability, opting out of the processing of personal data by businesses for targeted advertising or sale, and nondiscrimination.

Other state laws

Over the last two years, legislators in Louisiana, Massachusetts, Michigan, New Jersey, New York, North Carolina, Ohio, Pennsylvania and Rhode Island have proposed bills modeled on the CCPA, CPRA, VCDPA and/or CPA. As more and more states introduced consumer privacy laws, it will be critical that companies continue to monitor their progression and be prepared to comply with them.



International Laws

International privacy laws and regulations continue to proliferate and have become increasingly broad. While the GDPR is the most well-known and scrutinized, several other international laws and regulations illustrate the global trend toward consumer protection.

EU Network and Information Security Directive 2 (NIS2)

In November 2022, the Council of the European Union approved legislation to replace the existing Network and Information Security Directive (NIS) with NIS2. The NIS2 directive establishes baseline cyber risk management and reporting requirements for organizations in regulated sectors, meaning those that provide essential services.

Whereas the NIS directive allowed EU member states to determine what essential services organizations would be subject to it, NIS2 applies to organizations based on their size. NIS2 also streamlines reporting requirements for organizations.

EU Cyber Resilience Act

The Cyber Resilience Act is a proposed law that tightens cybersecurity obligations in EU member states, including from a reporting and information sharing perspective. The law would apply to essential sectors, including energy, banking, healthcare, digital infrastructure and transportation. It would also establish a framework for information sharing and cooperation with authorities and EU member states, with the goal of creating a European vulnerability database. The law includes multiple requirements and will have strict penalties — separate from the GDPR — for failure to comply.

Australia Privacy Penalty Bill

The Australian Federal Privacy Act 1988 regulates the handling of personal information by relevant entities, including through investigations and civil penalties. While the act has been in effect for more than 30 years, in November 2022, Australia's parliament approved the Privacy Penalty Bill, which increases penalties for repeated or severe privacy breaches resulting from the failure to adequately safeguard customer data.

The new legislation increases maximum penalties to the greater of three times the value of benefits obtained through the misuse of data, AUS$50 million, or 30% of a company's adjusted turnover in the relevant period. The legislation will become effective the day after the bill receives royal assent from King Charles III.

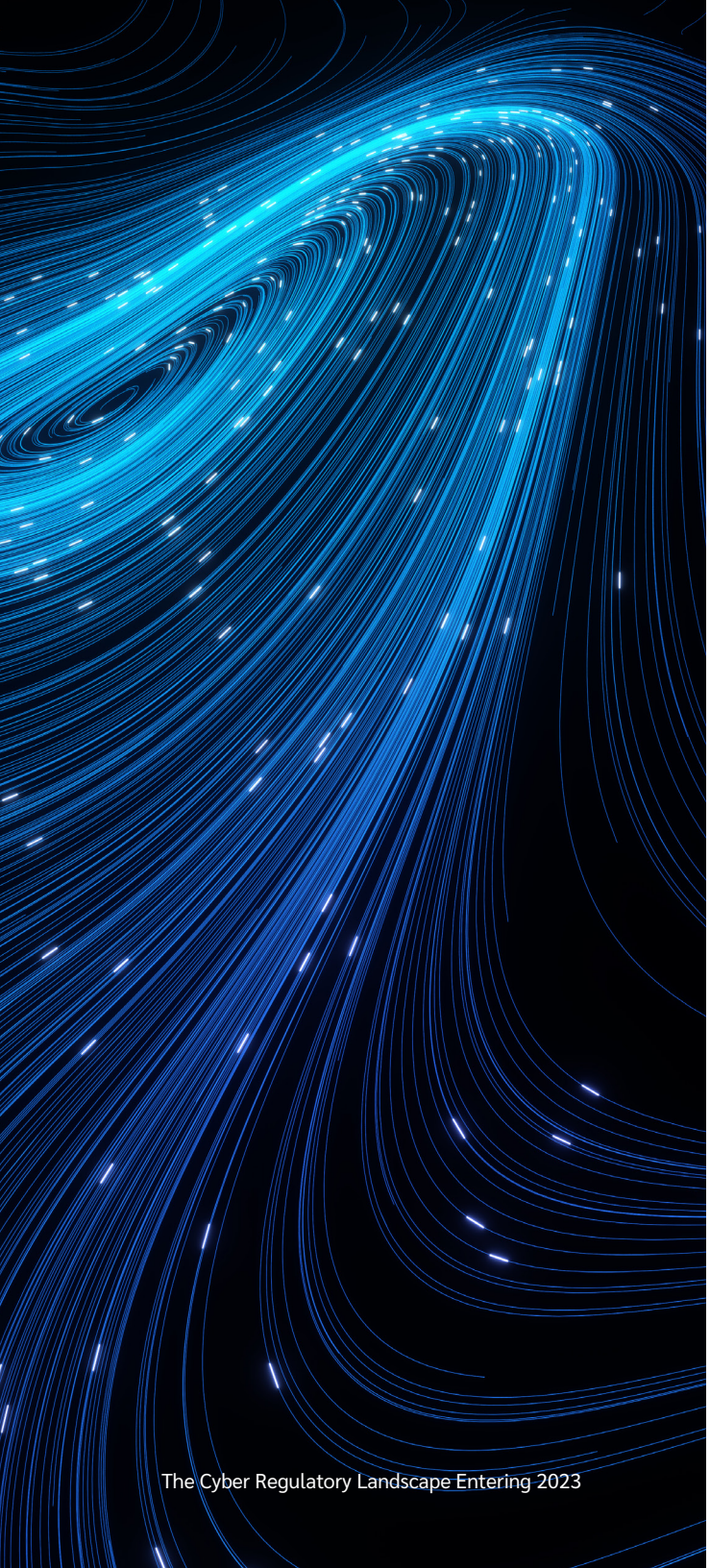
Brazil General Data Protection Law (LGPD)

The LGPD went into effect on Sept. 18, 2020, and generally follows the GDPR. The law includes provisions applicable to the processing of personal data of individuals located in Brazil and data used to offer goods or services to individuals in Brazil or collected or processed there.

China Personal Information Protection Law (PIPL)

The PIPL took effect on Nov. 1, 2021, adding to and enhancing China's prior Cybersecurity Law and Data Security Law. The PIPL applies to both the public and private sectors and to data processed both within China and for the processing of Chinese citizens' data in other countries for the purpose of providing products or services to them.

For more information, read Lockton's previously published report on the PIPL.



South Africa Protection of Personal Information Act (POPIA)

The POPIA went into effect on July 1, 2020, and applies to any company, person or organization processing personal information in South Africa, domiciled in South Africa or utilizing automated/non-automated data processing in South Africa.

The POPIA classifies personal information as that related to a natural person or "juristic person," such as independent legal entity. It is enforced by an independent regulator; violations can lead to fines of up to ZAR10 million or imprisonment up to 10 years.

The act confers multiple rights upon individuals, including to request access to personal information, be notified if their personal information is collected, and request deletion or destruction of personal information.

Enforcement

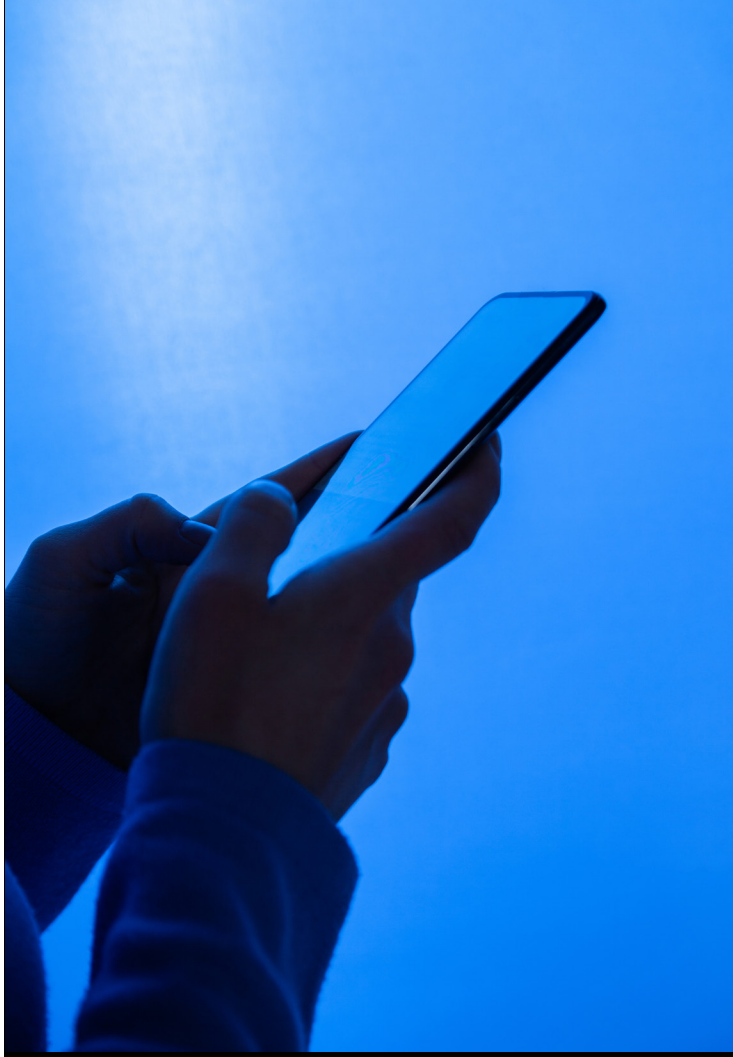
Given the novelty of privacy laws, the frequency and severity of enforcement remains to be seen across the landscape. There have, however, been some recent enforcement actions of note.

Earlier this year, California's attorney general filed suit under the CCPA against Sephora, a personal care and beauty products retailer, alleging the company failed to disclose to consumers that it was selling their personal information. In August, the allegations were resolved with a $1.2 million penalty amount — the first settlement under the CCPA — and several other requirements, including that Sephora enhance online disclosures and privacy policies to include clear representations around the sale of personal data.

Also in the U.S., biometrics have been a significant area of focus:

- In October, Texas's attorney general Ken Paxton sued Google for the alleged unauthorized collection of biometric data, seeking $25,000 per violation.
- In Cothron v. White Castle System, Inc., the Illinois Supreme Court is examining whether damages under the Illinois Biometric Privacy Act (BIPA) accrue per individual violation or if the first instance of a violation constitutes the full claim under the act. This decision is expected to an enormous impact on the scope of BIPA fines moving forward as it would substantially change how much plaintiffs can recover.

Overseas, during the past few years, EU data protection authorities have also issued substantial fines under the GDPR, including a €746 million fine against Amazon Europe for not complying with general data processing principles and €225 million fine against WhatsApp Ireland insufficiently informing consumers about the company's data practices. In the U.K., meanwhile, British Airways was fined over £20 million for a compromise of personal data after user traffic from its website was diverted to a fraudulent site where attackers harvested users' personal details.



More recently, in November 2022, the Irish Data Protection Commission issued a €265 million fine against Facebook, which followed a €405 million fine against Instagram in September. Instagram and Facebook are owned by the same parent company.

Regulatory compliance and staying informed about the continued development and augmentation of data privacy laws and regulations is an increasingly important facet of cyber risk management. Fortunately, if a cyber event affects your organization and regulators take an interest, a strong cyber insurance program will cover costs associated with a regulatory investigation and will include coverage for fines and penalties assessed.

AUTHORS

Neel Desai
VP, Cyber & Technology
Lockton Companies
404.460.3656
ndesai@lockton.com

Richard J. Bortnick
Of Counsel
Wilson Elser
619.881.3334
richard.bortnick@wilsonelser.com

UNCOMMONLY INDEPENDENT

C | 21297271222