NAVEX®

Addressing Cyber & Data Privacy in 2023

A NAVEX EBOOK

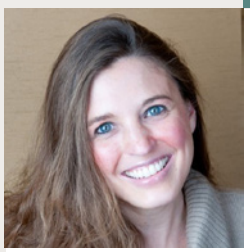
NAVEX®

Table of Contents

Introduction

The ever-evolving landscape of cybersecurity risks and data privacy legislation is a challenge for many organizations to stay ahead of. To help address the growing threat, NAVEX is committed to sharing up-to-date resources to help equip CISOs, IT leaders, and risk and compliance officers with their efforts to protect their enterprise.

This collection of articles covers some of the privacy legislation that is either already in or taking effect soon across the world. The purpose is to give context around cybersecurity, data protection, and compliance with global privacy regulations to help organizations better mature their cybersecurity and data protection posture.



A Recap of U.S. Data Privacy Laws Taking Effect in 2023

BY: JACLYN JAEGER
Freelance Journalist

Last year was a busy one for data privacy legislation across the United States, and with many states' consumer data privacy laws in effect this year, now is the time to reassess where more changes may be needed in order to prepare.

According to an analysis by the National Conference of State Legislatures (NCSL), "at least 35 states and the District of Columbia introduced or considered almost 200 consumer privacy bills in 2022." Comprehensive (omnibus) privacy legislation was the most common type of bill considered, introduced in at 25 least states and the District of Columbia and in almost 70 bills, according to the NCSL.

Comprehensive privacy legislation, as defined by the NCSL, broadly refers to the regulation of the "collection, use, and disclosure of personal information and providing an express set of consumer rights with regard to collected data – such as the right to access, correct, and delete personal information" collected by businesses (data controllers).

To date, five states passed the following comprehensive privacy legislation:

- California Privacy Rights Act (CPRA), a modified version of the California Consumer Privacy Act (CCPA), effective Jan. 1, 2023
- Virginia Consumer Data Protection Act (VCDPA), effective Jan. 1, 2023
- Colorado Privacy Act (CPA), effective July 1, 2023
- Connecticut Data Privacy Act (CTDPA), effective July 1, 2023
- Utah Consumer Privacy Act (UCPA), effective Dec. 31, 2023

By design, these comprehensive consumer privacy laws have many similarities from a big-picture perspective, but they also have a patchwork of subtle differences that companies will need to iron out.

On the next page is a non-exhaustive list of some of those consumer privacy provisions and a brief overview of the similarities and differences between each state's requirements.

Scope of coverage: Among the five states' consumer privacy laws, Utah takes the most business-friendly approach, overall. Like other states, the UCPA applies to any business or data processor who does business in the state or produces a product or service targeted to consumers who are residents of that state.

The scope of the UCPA, however, covers only businesses or data processors that also:

- Have annual revenue of $25 million or more; and
- Satisfies one or more of the following thresholds: during a calendar year, controls or processes personal data of 100,000 or more consumers; or derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

Virginia, Colorado, and Connecticut establish similar 100,000/25,000 consumer thresholds, with some variance regarding the "gross revenue from the sale of personal data" threshold. What makes Utah's multi-tier threshold more business-friendly, however, is that it ensures not only that smaller companies will not be subject to the UCPA, but also that even companies that satisfy the $25 million annual revenue threshold will not fall under the law, unless they also satisfy at least one of the other listed thresholds.

Other than Utah, California is the only other state to include a revenue threshold ($25 million in annual global revenue). Unlike the UCPA, however, the CPRA states that a business that does not make $25 million in annual global revenue can still fall under the scope of the CPRA, so long as it meets one of these other two thresholds: buys, sells, or shares the personal information of 100,000 or more California residents or households; or derives 50% or more of their annual revenue from selling or sharing California residents' personal information.

"Consumer" defined: Subtle differences also exist between how each state defines "consumer." Virginia, Colorado, Connecticut, and Utah define a "consumer" as an individual who is a resident of the state acting only in an "individual or household context." The CPRA, in contrast, goes further by additionally including individuals acting in a "commercial or employment context."

"Sale of personal data" defined: Under the various state consumer privacy laws, the "sale" of personal information triggers many of the requirements, and so understanding the definition of each state law is important. Virginia and Utah define "sale" as the exchange of personal data "for monetary consideration by a controller to a third party." Cookie data for targeted advertising purposes, for example, may not apply. In contrast, California, Colorado, and Connecticut define "sale" more broadly as including "monetary or other valuable considerations."

Utah's Consumer Protection Act has a multi-tier threshold that makes it the most business-friendly.

Personal data defined: Utah, Virginia, Connecticut, and Colorado define "personal data" broadly as any information that is "linked or reasonably linkable to an identifiable or identified individual." Among these states, personal data does not include de-identified or publicly available information.

Scope of exemptions: The scope of exemptions is broad, and in some states more than others. All five states provide exemptions for government agencies, and – except for Colorado – exempt non-profit organizations. Virginia, Colorado, Connecticut, and Utah also provide exemptions for institutions of higher education, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) and – again, except

for Colorado – covered businesses or business associates regulated by the Health Insurance Portability and Accountability Act (HIPAA).

In addition to the type of entities subject to exemptions, exemptions are provided for certain types of data covered by other federal laws. These exemptions vary by state but generally include, for example, the GLBA and HIPAA.

Privacy notices: As companies revise their privacy notices, or create new ones, keep in mind that some states' consumer privacy laws – like Connecticut and Utah – require businesses provide a "reasonably accessible, clear and meaningful" privacy notice. Moreover, the privacy notice must include:

- The categories of personal data that are collected or processed by the businesses
- The purposes for processing the data
- How consumers may exercise their rights, and
- The categories of personal data that's shared with third parties, if any

Some states– for example, Connecticut and Utah – further require that where the business "sells" consumer data to a third party or processes it for targeted advertising, the privacy notice must "clearly and conspicuously" disclose how consumers can exercise their opt-out rights may opt out of such activities.

Universal opt-out mechanisms: California, Colorado and Connecticut each require businesses to recognize universal opt-out mechanisms (GPC signals), which gives consumers the ability to opt-out of the processing of their personal data across multiple websites simultaneously, rather than having to make individual opt-out requests through each website. Virginia does not include such a requirement. Each state also has varying requirements regarding consumer opt-out rights pertaining to the collection of "sensitive" data, as defined by each state, which must also be considered.

The effective date to get into compliance varies by state. Under Connecticut's privacy law, for example, universal opt-out mechanisms must be recognized by controllers as valid consumer requests beginning Jan. 1, 2025.

Service provider agreements: Also important from a legal and compliance standpoint, all five states require businesses to impose contractual obligations on data processors with whom they share consumer data. Colorado, Connecticut, Utah, and Virginia go beyond California by requiring businesses to provide clear instructions pertaining to the processing of personal data; the nature and purpose of the processing; the type of data to be processed; the duration of the processing; and the rights and obligations of the parties.

Data protection assessments: Among the five states, Utah is the only one that does not require businesses to conduct and document a data protection assessment regarding processing activities involving personal data. The scope and level of detail required by each data protection assessment varies greatly by state.

Compliance takeaways

The provisions mentioned above provide only a high-level overview of just a few of each state's key requirements. Using the CPRA as a benchmark when reviewing the company's privacy compliance program, it will be important moving forward to regroup as a cross-functional team and assess where further changes may be needed, depending in which states the business operates, and where its consumers reside.

As a fundamental first step, prudent companies will want to conduct a data mapping exercise that, at a minimum, provides clarity around what personal information the business collects, and how that data is stored, shared and used.

Ensuring compliance with each state's patchwork of consumer privacy laws also requires reviewing and, where necessary, amending privacy notices and ensuring they're easily accessible to consumers, as well as reviewing the company's data retention practices, contracts with third parties, and conducting and documenting a data protection assessment.

The technology-related hurdles are also immense and demand involvement of IT, data security, and cybersecurity experts to ensure do-not-sell/share links are functioning properly, GPC signals are being recognized, and that the business has robust cybersecurity practices in place. For some companies, this is going to be a lot more resource-intensive of an undertaking than for others.

Keeping on top of developments in each state as new guidance becomes available and/or as state rules are revised is important as well. On Dec. 21, 2022, the Colorado Attorney General's office, for example, published revised rules to its consumer privacy act, which make further changes to the draft rules it published in September.

In short, absent a comprehensive federal consumer privacy law, businesses will have to continue reviewing their data privacy compliance obligations state-by-state, and day-by-day.

Ensuring compliance with each state's patchwork of consumer privacy laws requires many steps.

CPRA Regulations & Requirements: Understanding the California Privacy Rights Act

On Jan. 1, 2023, the California Privacy Rights Act (CPRA) will take effect, placing newly enhanced data privacy and notification requirements onto businesses that handle the personal information of California consumers. Understanding its requirements, including the newly modified proposed regulations, may help companies avoid costly financial and reputational harm associated with unintentional CPRA violations down the road.

In 2018, California became the first U.S. state to pass the most stringent and comprehensive data privacy law in the nation, the California Consumer Privacy Act (CCPA), which established privacy rights for California consumers. In November 2020, the CCPA was repealed and further amended when California passed the CPRA.

Businesses subject to the CPRA are those that make $25 million in annual gross revenue as of Jan. 1 of the preceding calendar year; buy, sell, or share the personal information of at least 100,000 consumers or households; or that derive 50 percent or more of their gross revenue from selling or sharing personal information.

CPRA regulations and requirements

Several provisions in the CPRA take inspiration from the EU's General Data Protection Regulation (GDPR). Most notably, perhaps, the CPRA introduces a whole new category of data, "sensitive personal information," and further grants consumers the right to direct a business to limit its use and disclosure. To comply with such requests, businesses must provide a "clear and conspicuous" link on their homepage, titled "Limit the Use of My Sensitive Personal Information."

The CPRA defines sensitive personal information broadly to include the following types of information:

- Social Security number
- Driver's license
- State identification card or passport number
- Financial account information and log-in credentials
- Debit or credit card number and access codes
- Precise geolocation data
- Religious or philosophical beliefs
- Ethnic origin
- Genetic data
- Biometric information for identification purposes
- Personal health information
- Sex or sexual orientation information

New notification obligations

Under the CCPA, businesses are already required to inform consumers about the personal information collected on them and the purpose behind the collection of that data. Under the CPRA, however, businesses must provide even more details, informing consumers if their personal information will be sold or shared, how it will be used, and how long they will retain the data collected.

On Nov. 3, 2022, the CPPA issued modified proposed regulations implementing the CPRA, which revise the initial proposed regulations issued in July. The modified proposed regulations, in part, state that a business no longer needs to identify in its "Notice at Collection" the names of third parties that control the collection of personal information. Removal of this requirement saves businesses the compliance headache of having to continuously revise their "Notice at Collection" every time they change or terminate a third-party contract.

Consumers right to opt-out

Unlike the CCPA, the CPRA gives consumers the right to opt out of having their personal information sold or shared for purposes of "cross-context behavioral advertising," commonly known as "targeted advertising." To comply with this provision, businesses must provide a clear and conspicuous link on its homepage, titled "Do Not Sell or Share My Personal Information."

The modified proposed regulations clarify that businesses must treat an opt-out preference signal as valid request to opt out of sale or sharing for not only that browser or device, but also for "any consumer profile associated with that browser or device, including pseudonymous profiles."

Furthermore, the CPRA grants consumers the right to request that businesses correct inaccurate personal information, or to delete personal information that was sold to or shared with service providers and contractors.

> The CPRA gives consumers the right to opt out of having their personal information sold or shared.

Data minimization requirements

The CPRA's "purpose limitation" provision requires that businesses have a specific and explicit reason for collecting consumers' personal information. The CPRA provides that a business's collection, use, retention, or sharing of a consumer's personal information be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed."

The modified proposed regulations introduce the following five new "factors" for businesses to consider when determining whether their practices satisfy their data minimization requirements:

- The relationship between the consumers and the business
- The type, nature, and amount of personal information that the business seeks to collect or process

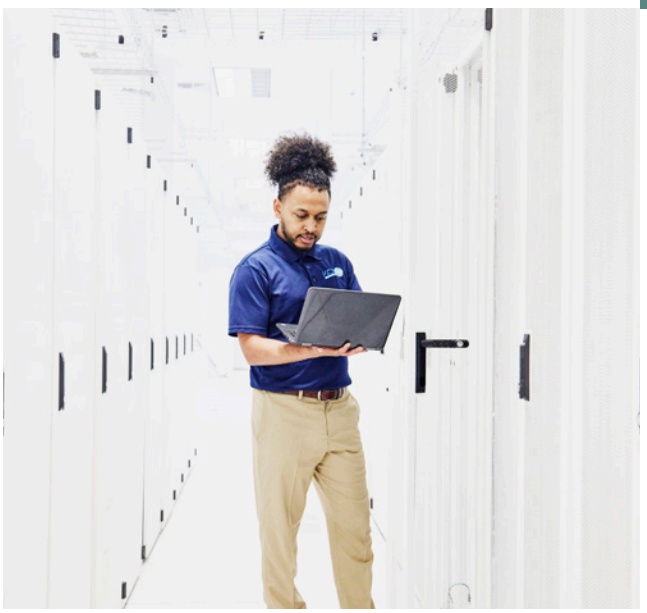
- The source of the personal information and the method for collecting or processing it
- The specificity, explicitness, prominence, and clarity of disclosures about the purpose of collecting or processing it
- The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumers

Additionally, the modified proposed regulations identify factors for determining whether other disclosed purposes are compatible with the context for collecting personal information.

Privacy rights of minors

The CPRA requires that a business with "actual knowledge" that it sells or shares the personal information of a consumer under the age of 13 "shall establish, document, and comply with a reasonable method for determining that the person consenting to the sale or sharing of the personal information about the child is the parent or guardian of that child." Without consent, the business must either wait at least 12 months or wait until the child turns 16 before asking for their opt-in consent again.

The CPRA states that receiving consent for the sale or sharing of personal information is in addition to any verifiable parental consent required under the federal Children's Online Privacy Protection Act. The CPRA further lists six methods for reasonably calculating whether the person providing consent is the child's parent or guardian.



Investigations and enforcement

Implementation, oversight, and enforcement of the CPRA falls under the newly created California Privacy Protection Agency (CPPA), the first data protection authority in the United States. However, the CPRA's enforcement authority for CPRA violations will begin until July 1, 2023, at soonest.

The modified proposed regulations clarify that the CPPA, in deciding whether to pursue investigations of potential or alleged violations, "may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements."

From a regulatory enforcement standpoint, violations of the CPRA could result in civil penalties of up to $2,500 per violation or $7,500 per each intentional violation. Additionally, a business that does not "implement and maintain reasonable security procedures and practices" resulting in the "unauthorized access and exfiltration, theft, or disclosure" of a consumer's personal information faces up to $750 per violation or actual damages, whichever is greater.

The CCPA's five-member board has authority to certify companies deemed to be CPRA-compliant. Businesses that do not fall under the CPRA's umbrella may still voluntarily seek this certification as a demonstration of their data protection practices' high standards.

CPRA compliance message

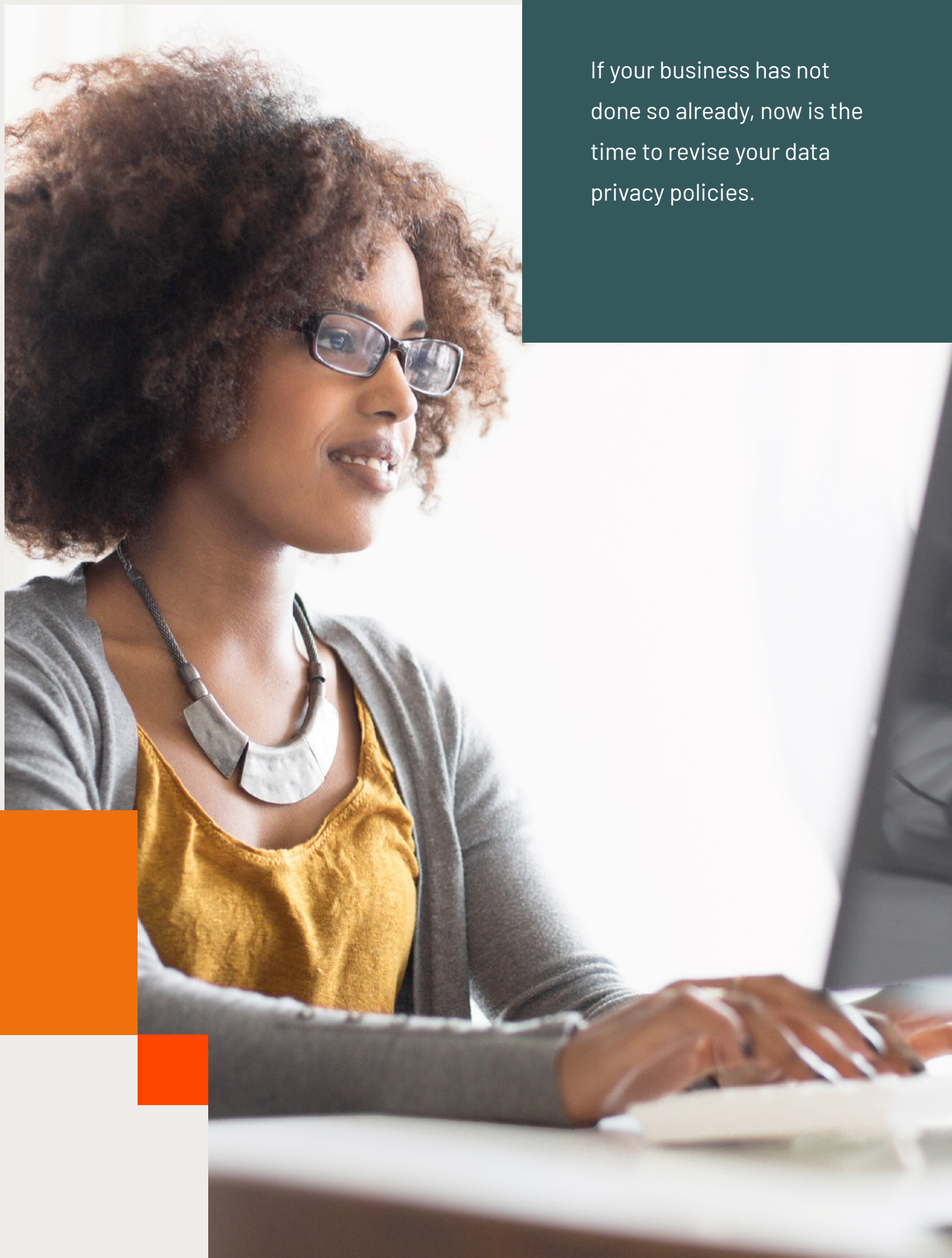
If your business has not done so already, now is the time to revise your data privacy policies and procedures as it concerns disclosure notifications, the more restrictive handling of sensitive personal information, the selling and sharing of consumers' personal information with third parties, as well as reviewing and revising your data retention policies. Prudent businesses also will want to review and update their data collection and storage practices to ensure compliance with the purpose limitation and data minimization requirements.

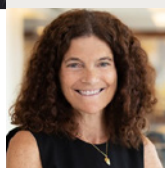
About The Author

JACLYN JAEGER | Freelance Journalist

Jaclyn Jaeger is a freelance business journalist specializing in corporate ethics and compliance matters. Formerly an editor with Compliance Week from 2007-2022, Jaclyn still regularly writes for Compliance Week, in addition to the American Conference Institute's ACI Insights, Anti-Corruption Report, Cybersecurity Law Report, Compliance Chief 360, and numerous other publications. Connect with her on LinkedIn.

If your business has not done so already, now is the time to revise your data privacy policies.





Privacy in 2023 – What to Expect and How to Prepare

BY: **JAMES CASTRO-EDWARDS**
Counsel, Arnold and Porter

NANCY PERKINS
Counsel, Arnold and Porter

U.S. legal trends

Privacy law compliance in the United States today demands resilience, flexibility, and responsiveness. To date, the U.S. Congress has failed to enact broadly applicable privacy standards to govern companies uniformly nationwide. Seeking to fill the gaps in existing privacy regulation, the states are rapidly taking action, with one state in particular, California, leading the charge with a continually expanding set of privacy-related requirements to protect individuals residing in the state. California's initiatives have triggered other states to follow suit. In just the past two years, four other states enacted new consumer data privacy laws, all of which are scheduled to take effect in 2023. However, each state's version of consumer privacy law differs in various ways from the others, and businesses will face an ongoing challenge in juggling privacy obligations under multiple regimes.

Adding to the complexity of the states' different privacy law frameworks, the Federal Trade Commission (FTC), which has broad jurisdiction over for-profit companies operating in the U.S., initiated a potentially far-reaching rulemaking process to address what it perceives to be major gaps in privacy and security protections for consumers. At the same time, the Department of Health and Human Services, which regulates a wide range of entities in the healthcare sector with respect to the privacy and security of protected health information, is poised to amend its privacy regulations. Further, the Securities and Exchange Commission (SEC), which regulates publicly traded companies, proposed new cybersecurity rules, while the federal banking agencies issued new rules for financial institutions and their services providers for notifications of cybersecurity incidents.

For companies doing business in the U.S., this multifaceted privacy law environment can seem daunting. As is the case with most major challenges, a framework for formulating fundamental principles can help make compliance and data strategy more manageable. With limited resources to invest, keeping a realistic focus on significant risks, rather than getting mired in the minutia of detailed requirements, can also prove beneficial. The paragraphs below suggest a conceptual roadmap for streamlining privacy efforts.

Common state law requirements

The five states that enacted broadly applicable consumer privacy laws – California, Colorado, Connecticut, Utah, and Virginia – have all embraced certain fundamental privacy principles and concepts, including many that are at the core of the European Union General Data Protection Regulation (GDPR) (discussed in Section II below). This trend is likely to continue in additional states.

Fueled by concerns that consumers lack knowledge of, and tools to control, how their personal data are being captured (particularly online), used and shared, the five states' laws all contain provisions requiring:

- Consumers be given **notice** (descriptions of what data is collected, and why, and who it is shared with)
- **Privacy rights** (some control over the use, disclosure and retention of their personal information and means to access and amend)
- Companies to implement **privacy by design** (ensuring privacy is considered up front and for specified purposes)
- **Purpose limitations** (forcing companies to collect and use data in accordance with a set of appropriate and lawful purposes)
- **Security** (protection of personal data)
- That companies are **accountable** (through enforcement and complaint mechanisms, documentation requirements, and oversight and auditing requirements)

These same principles are the backbone not only of the GDPR, but also of U.S. federal regulations governing the banking industry, healthcare industry, and industries handling children's information, among others. They thus serve as a reliable framework for designing a privacy program even while the legal goalposts and guardrails for that framework are still under construction.

Following these principles will go a long way in protecting against complaints from individuals or regulators. Key practical steps to implement these principles include:

Adopting a clear, publicly available privacy notice that describes the companies' data practices and individuals' privacy rights

- Making that notice available to individuals before collecting their personal information (wherever collection occurs)
- Adhering, without exception, to the statements in that notice, including to respect people's privacy rights
- Engaging in privacy by design to ensure the ethical collection and use of data (in line with lawful purposes)
- Making third-party recipients of data accountable to follow your statements about data use
- Ensuring an internal privacy program that documents compliance efforts and risk determinations and allows for monitoring and auditing of same
- Maximizing the protection of data in accordance with its sensitivity and the threats thereto

New complexities under the state laws as of 2023

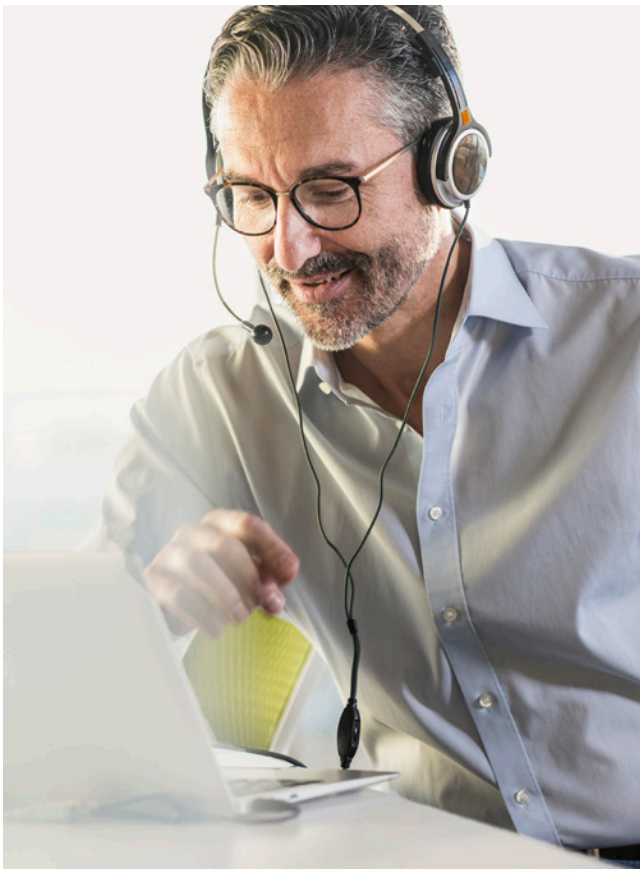
Although the five U.S. states' broad consumer protection laws have fundamental similarities, the scope of California's law, the California Consumer Privacy Act (CCPA), is notably more expansive than the laws of the other four states due to the expiration of the law's previous exemptions for personal information about employees and business-to-business (B2B) contacts (such as customer representatives and vendor contacts). Further, the California Privacy Protection Agency, which was established as a new CCPA administrative and enforcement authority in 2020, recently issued detailed draft regulations implementing the amendments to the CCPA adopted pursuant to the California Privacy Rights Act of 2020 (CPRA). Businesses subject to the CCPA will have significant work to do to ensure compliance with those regulations, the enforcement of which is scheduled to commence in the third quarter of 2023.

As noted, until January 1, 2023, the CCPA exempted from most of its requirements personal information about employees and B2B contacts. Until late August 2022, it was widely anticipated that the California legislature would extend these exemptions. Given these expectations, and because all of the other four states' consumer privacy laws contain permanent exemptions for such information, many companies have designed their privacy programs specifically to protect the personal information of consumers with whom they deal on a **personal or household** basis. Adjusting to the CCPA's new scope covering **employee and B2B** contact information as well will be a challenge for these companies.

In addition, both under the new CCPA regulations and other states' privacy regimes, businesses will need to grapple with restrictions on, among other things:

- Uses and disclosures of "**sensitive personal data**" (as defined in varying ways)
- "**Sales**" of personal data
- Sharing of personal data, including online tracking information, for certain **advertising** purposes
- Collection of personal information of **minors**

The specifics of these restrictions, and the requirements for implementing methods for consumers to opt-in or -out of these types of processing of personal information, may be similar across certain states, and can be handled in a uniform manner, but they **will not be uniform** across all states. Again, this underscores the need for a flexible posture with a focus on areas of highest risk.



EU-UK Legal Trends

Data transfers – the new EU-U.S. Data Privacy Framework

A new EU-U.S. transatlantic data flow agreement is expected to be finalized by the spring of 2023. The EU-U.S. Data Privacy Framework will enable the flow of personal data from 'data exporters' in the EU to 'data importers' in the U.S. who have signed up to the agreement. The Framework offers a flexible alternative to the European Commission's Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), which multinationals with a presence inside and out of the EU must otherwise use to share personal data (absent some small exceptions).

The European GDPR prohibits the transfer of personal data to 'third countries' that do not guarantee an adequate level of data protection. 'Third countries' are countries outside the European Economic Area. The European Commission declared a small number of third countries, such as Switzerland, Canada and Argentina as guaranteeing an adequate level of data protection. Such an adequacy finding means personal data may be freely transferred from EU Member States to the adequate third country. However, the transfer of personal data to third countries which have not been granted an adequacy finding (such as the U.S.) is prohibited, unless appropriate safeguards have been implemented. Currently, the main appropriate safeguards are SCCs and BCRs, which may be onerous to implement or expensive and time consuming, respectively.

More flexible data transfers were available in the form of the Privacy Shield and the Safe Harbor scheme, which were invalidated following the Schrems II and Schrems I decisions in 2020 and 2015 respectively. Multinationals will welcome

the EU-U.S. Data Privacy Framework, which offers a business-friendly alternative to facilitate transatlantic data sharing.

In October 2022, U.S. President Biden signed an executive order, which mandates legal safeguards over U.S. security agencies' use of EU citizens' personal data. This is a critical and long-awaited next step in the progress of the EU-U.S. Data Privacy Framework.

The following step will be for the European Commission to make an adequacy finding, which could take as long as six months. If and when it does take effect, the Framework would operate as a replacement for the Privacy Shield.

However, Max Schrems, founder of privacy non-profit NOYB, already expressed reservations regarding the level of protection guaranteed by the EU-U.S. Data Privacy Framework and a third challenge seems inevitable. If Schrems' third challenge repeats his earlier successes, multinational businesses' access to a flexible EU-U.S. data transfer solution may be short-lived. Only time will tell, as this plays out over the course of 2023.

UK/EU divergence – The data protection and digital information bill

In the Queen's Speech of May 2022, the British government announced its intention to reform U.K. data protection law. The government previously expressed its desire to take advantage of Brexit to realize the apparently conflicting aims of creating

a more business-friendly data regime that promotes growth and innovation, while continuing to protect individuals' privacy rights.

The draft Data Protection and Digital Information Bill was published in July 2022, in an effort to realize the government's intentions. Notwithstanding the government's ambitious claims, the Bill amounted to little more than an evolution of the existing U.K. GDPR, rather than a radical overhaul. However, the changes the Bill would have introduced regarding international data transfers potentially threatened the U.K. adequacy decision the European Commission made in June 2021. The adequacy decision enables the free flow of personal data between the EU and the U.K. following Brexit. However, the European Commission may withdraw the decision if the U.K. data protection regime diverges too far from European data protection standards. Such a withdrawal would mean that organizations in EU Member States would be prohibited from sharing personal data with the U.K., which would be costly and disruptive for multinational businesses with a presence in the U.K. and the EU.

The draft Data Protection and Digital Information Bill looks set to make further progress, following the announcement at the International Association of Privacy Professionals (IAPP) Congress 2022 in Brussels in November by DCMS deputy director Owen Rowland that the latest consultation on the Bill will commence shortly.

The need for reform is questionable; while the U.K. GDPR may not be perfect, it is fit for purpose in striking a reasonable balance between protecting individuals' rights and businesses' interests. The British government may dismiss the GDPR as overly unfriendly to business goals for data use. However, it seeks to give individuals choice and control over how their personal data is used and imposes heavy penalties on organizations that fail to abide by the rules. If the U.K. government pushes ahead with its proposed reform, resulting in a U.K. data protection regime that fails to meet European standards, leading to a revocation of the U.K.'s adequacy finding, companies will face a much-increased burden to enter into an appropriate data transfer solution, as well as carry out a transfer risk assessment, for transfers from the EU to the U.K. The inevitable costs to businesses are likely to absorb at least some of the purported savings (or increased revenues from new data uses) the new legislation would make. Whether the British government will press ahead with its proposed reform remains to be seen, so the best advice to multinational businesses is to watch this space.

2023 prediction

As noted, in recent years the U.S. Congress has considered but failed to pass various forms of federal privacy legislation. The new Congress taking over in 2023 is not likely to put a significantly new face on the prospects for passage of federal privacy legislation. Regulated entities therefore would do well to focus on the trends in the states, as well as the anticipated FTC rulemaking and the agency's ongoing privacy enforcement actions under Section 5 of the FTC Act.

The European Commission's adequacy determination concerning the EU-U.S. Data Privacy Framework is expected imminently; whether or not it survives the almost inevitable Schrems III challenge remains to be seen. Meanwhile, U.K. businesses that trade internationally may well be hoping that the government sees sense and leaves well enough alone, rather than risking the U.K.'s adequacy decision and the free-flow of data with Europe.

About The Authors

James Castro-Edwards | Counsel, Arnold and Porter

James Castro-Edwards provides counsel on global data protection compliance projects for multinational companies, advises on data protection issues, and helps companies respond to data breach situations. He represents a broad range of clients including financial, media and technology organizations, and medical device and pharmaceutical companies. In addition to advising clients on data protection issues, Mr. Castro-Edwards has created innovative data protection support, audit and training programs for clients.

Earlier in his career, Mr. Castro-Edwards was in private practice and served as a Solicitor in the data protection group at PwC Legal. He is widely published in a variety of titles, a regular public speaker on data protection issues and wrote the text book on the EU General Data Protection Regulation (GDPR) for The Law Society.

Nancy Perkins | Counsel, Arnold and Porter

Nancy Perkins focuses her practice on regulatory compliance and consulting on emerging policy issues, with a principal focus on data privacy and security and electronic transactions. Ms. Perkins regularly advises clients on compliance with a wide range of data protection requirements at the federal and state levels, including rules applicable to online communications and transactions as well as all types of uses and disclosures of medical, financial, and other sensitive personal information. She assists clients in structuring their activities, online service offerings, and privacy policies to comply with applicable laws and best practices, taking into account technological and intellectual property issues associated with the expansion of electronic commerce and Internet activities. Among other laws, Ms. Perkins frequently provides counsel on the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act (as amended by the Fair and Accurate Credit Transactions Act), the federal E-Sign Act, the Children's Online Privacy Protection Act, and the Video Privacy Protection Act, as well as state privacy, security, data breach notification, and electronic signature laws.

A framework for formulating fundamental principles can help make compliance and data strategy more manageable.

The SEC Wants You to Do Better at Disclosing Cybersecurity Breaches

BY: MATT KELLY
CEO, Radical Compliance

Compliance and technology executives, we need to talk. Or, more accurately, you need to talk more often – to each other.

In the last 18 months, the Securities and Exchange Commission sanctioned three companies for making misleading disclosures about cybersecurity breaches those companies suffered. In each instance, at least some employees at the company knew the true extent of the breach, but those details weren't passed along to the teams responsible for compiling the company's quarterly SEC filings.

The result: SEC filings that gave investors an erroneous sense of the company's cybersecurity risks. The disclosures either understated the severity of the incident; or framed the incident as a hypothetical threat rather than as something that had actually happened.

Those are failures of internal disclosure processes, and the SEC is not taking kindly to them. The monetary penalties imposed on the offending companies have grown progressively larger, from $488,000 in mid-2021 to $3 million in an enforcement action announced just this month. The heat is only going to get worse, too, since the SEC is likely to adopt even more stringent rules about disclosing cybersecurity incidents later this year.

So how should compliance officers and CISOs approach this enforcement risk? What practices and processes can help with better communication?

Understand the disclosure risk

Federal securities law requires that financial statements disclose all material issues and risks to investors. That means companies need disclosure controls and procedures to capture information about those material issues, and then convey that information completely and accurately to investors.

Companies have spent the last 20 years developing effective disclosure controls and procedures for **financial** items, where accounting and SEC reporting teams work hand-in-glove to confirm every detail that should go into a filing.

The newer, more difficult challenge is to build a similar set of controls and procedures for non-financial issues – including data breaches, ransomware attacks, or other cybersecurity events.

This can be hard for several reasons. First, cybersecurity teams aren't as familiar with disclosure obligations as corporate finance teams usually are. Second, the controls governing financial reporting are well-established, and much more uniform from one company to the next. Cybersecurity practices, on the other hand, evolve all the time; and can differ radically even among companies of similar size or industries.

Hence you can end up with IT teams discovering a breach and not knowing they should report it up the chain of command; or they do report the breach, then discover more information about it but don't report those new details, believing that they'd already done their duty.

For example, in the SEC's most recent enforcement action, the company's IT team discovered a breach in May. By early July, the company disclosed the breach publicly and promised customers that no sensitive data was at risk. By late July, however, the IT team discovered that personal customer data in fact had been breached.

What happened next? The SEC's settlement order says it all:

Although the company's personnel were aware of the unauthorized access and exfiltration of donor bank account numbers and Social Security numbers by the end of July 2020, the personnel with this information about the broader scope of the impacted data did not communicate this to the senior management responsible for disclosures, and the company did not have policies or procedures in place designed to ensure they do so.

That's the real issue for CISOs and compliance officers to watch for. Even if you have solid controls and procedures to report information **out**, from the external reporting team to the 10-Q; you also need controls and procedures that report information **up**, from other parts of the enterprise to those folks who compile the SEC filings.

How to build a better process

Most companies have some sort of in-house disclosure committee to review what should go into the quarterly filings. Start there.

The CISO should already be a member of that committee, and they should be fully briefed by the legal or compliance team about what data needs to be disclosed when cyber incidents happen. Then the CISO needs to assure that controls and processes exist within the IT security function to capture that information about cyber incidents, and then relay it to the external reporting teams.

Critically, those controls and processes need to capture and relay that information **even when the situation has changed** – for example, when you realize the breach is worse than first understood, or that more data was stolen than believed.

That's the risk of relying on manual processes for this work. Too often, people might misunderstand their reporting duties, or record a critical piece of information improperly. For example, you might suffer a "fat finger error" where the employee presses the wrong key and records a high-priority incident as low priority – that actually happened in one of the incidents mentioned above. So the more you can automate this monitoring, capturing and relaying – the better.

Also remember that the SEC has proposed even more disclosure of cybersecurity incidents, which companies will need to file more quickly. Those proposed new rules haven't been adopted yet, but they're likely to come soon. So another part of your disclosure effort might be to map your disclosure controls to those needs.

Clearly the SEC is thinking a lot about how companies should keep investors informed about the cybersecurity incidents you suffer. Your disclosure policies and procedures will need to keep pace with that heightened attention.

Otherwise your company might end up keeping pace with the SEC's monetary penalties for poor cybersecurity disclosure, and they're going up too

Your disclosure policies and procedures will need to keep pace with heightened SEC attention

How CISOs Can Start Talking About ChatGPT

ChatGPT really is a marvelous technology – an artificial intelligence designed to answer just about any question a person might ask it – and yet, somehow, it leaves CISOs and compliance officers with even more questions.

For example, how should companies govern the use of ChatGPT (or any of the other next-generation AI applications rushing onto the market these days) within their own organizations? How are you supposed to guard against new risks posed by others using "weaponized AI" against you? How do you monitor the risks of vendors in your supply chain using AI? Exactly what are those risks, anyway?

Right now, nobody quite knows.

Clearly AI will change the business world, because a technology so powerful and easy to use can't not change corporate operations, risks and governance in profound ways. It's also clear that CISOs (and other risk assurance professionals) will play a crucial role in guiding your organization through those challenges.

Beyond that, however, the answers to the questions mentioned above (and many, many more) are still anyone's guess – and in most cases, the "correct" answer will vary from one company to the next. At this juncture, CISOs simply need to be prepared to find those answers as we move forward into this brave new world.

How so? By asking yourself and your company several more questions.

Do we have the right oversight structures in place?

The fundamental challenge with AI is governance. From the highest levels, your company needs to devise a system that manages how AI is studied, developed and used within the enterprise.

For example, does the board want to embrace AI swiftly and fully, to explore new products and markets? If so, the board should designate a risk or technology committee of some kind to receive regular reports about how the company is using AI.

On the other hand, if the board wants to be cautious with AI and its potential to up-end your business objectives, then perhaps it could make do with reports about AI only as necessary, while an in-house risk committee tinkers with AI's risks and opportunities.

Whatever path you choose, senior management and the board must establish some sort of governance over AI's use and development. Otherwise employees will proceed on their own – and the risks only proliferate from there.

Do we have the right policies in place?

This is the next, more granular step after laying down governance principles for AI. The company then needs to follow up with more precise policies and procedures that your employees and third parties can follow.

For example, if senior management has decided it has big ambitions for using generative AI (say, to automate interactions with customers), you might then follow up with policies that spell out how specific business units can try integrating AI into their operations. If you hail from financial services or some other highly regulated industry, you might want policies that place tight limits on rolling out AI until dedicated teams test those AI systems for security and compliance risks. (Numerous Wall Street banks have already done precisely that.)

This is also where you can start thinking about vendor-related issues more substantively. Do you want vendors to disclose whether they use AI when processing data or transactions on your behalf? Do you want to include a security assessment before purchasing AI systems from a vendor? Those issues will require policies. You'll need to work closely with the procurement team (or whoever is authorized to buy IT services for your enterprise) to be sure those policies are understood and integrated into their operations.

Can we manage AI-enabled work on a routine basis?

This is the people part of the puzzle: have you defined the necessary roles and responsibilities to put these lofty ideas into practice?

For example, if you want to assess the security risks of an AI solution, someone will have to do that. Do you have the right IT audit expertise in-house, or will you need to rely on outsourced help? If you want to use generative AI to develop software code for new products (yes, ChatGPT can do that), someone will need to test that code once it's written. Do you have the right talent for that work? (Especially if you laid off half your coders since ChatGPT is writing the code.)

This part of the AI puzzle could prove especially challenging because you'll be designing new workflows in potentially far-reaching ways. CISOs will need to consult closely with internal audit teams performing risk assessments, and operational teams telling you what is or isn't possible.

'ChatGPT, do we need to panic?'

No, not at all. Fundamentally, artificial intelligence is just another new technology – akin to the rise of cloud-based services in the 2010s, mobile devices in the 2000s, or the internet back in the 1990s. It raises a host of security, operational, and compliance issues we haven't considered yet, but CISOs do have the tools to work through those issues and find answers that fit your company.

You'll need to rely on risk management frameworks (NIST and a few groups have already started developing them for AI), and strengthen capabilities such as policy management, risk assessment, monitoring, and training. You'll also need support from the board, senior management, and colleagues across the enterprise, as you all try to keep your eyes on the proper balls and work toward a common vision.

Then again, hasn't that always been necessary for corporate success? Maybe the issues ChatGPT brings to the fore aren't so new after all.

Final words

ChatGPT will unquestionably change the compliance landscape. Staying ahead of the changes and maintaining an agile program requires a comprehensive software solution. To learn more about how NAVEX can help:

Discover NAVEX One

About The Author

Matt Kelly | CEO, Radical Compliance

Matt Kelly is editor and CEO of Radical Compliance, a blog and newsletter that follows corporate governance, risk, and compliance issues at large organizations. He speaks and writes on compliance, governance, and risk topics frequently. Follow him at @compliancememe or get in touch with him via email.

NAVEX®

NAVEX is trusted by thousands of customers worldwide to help them achieve the business outcomes that matter most. As the global leader in integrated risk and compliance management software and services, we deliver our solutions through the NAVEX One platform, the industry's most comprehensive governance, risk and compliance (GRC) information system.

For more information, visit NAVEX.com and our blog. Follow us on Twitter and LinkedIn.

AMERICAS

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035
United States of America
info@navex.com
www.navex.com
+1 (866) 297 0224

EMEA + APAC

4th Floor, Vantage London
Great West Road
Brentford, TW8 9AG
United Kingdom
info@navex.com
www.navex.com/uk
+44 (0) 20 8939 1650