ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Are You Really Ready for the New Privacy Laws?

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***As goes California.*** The California Consumer Privacy Act (CCPA) served as a model for 15 other US states to construct their own privacy legislation.
- ***Privacy maturity.*** One way to assess your organization's privacy capability is to measure your current and desired target on a scale of preparedness, with one being "immature" and five being "enabling."
- ***National guidelines.*** All 50 US states contain data security breach notification laws with penalties. Organizations would be wise to review and strengthen their programs in conjunction with the state laws.
- ***Third parties.*** Companies must have the capacity to address personal information they gather that is either sold or shared with third parties. This can be done with appropriate service level agreements outlining data handling expectations and restrictions.

Are you ready? Led by California, a new wave of privacy legislation is likely to have significantly more impact and cause more difficulty for organizations than any other US compliance requirements seen within the past decade. These new rules will create new obligations and privacy challenges for organizations. Companies will need to rethink the concept of Personally Identifiable Information (PII) and implement new policies, processes, and technology to develop a dedicated privacy plan. For organizations subject to these requirements, the key to avoiding substantial risks and costs associated with these new requirements is by being properly prepared. This article details key strategies and capabilities organizations should be prepared to implement to meet emerging privacy requirements.

On June 28, 2018, the California Legislature passed the California Consumer Privacy Act (CCPA). Similar to the data breach legislation initially passed in California in 2003 that served both as a model and was a catalyst for multiple states adopting similar laws, the 2018 CCPA is also expected to be copied by many other states and even perhaps spur the passage of federal privacy legislation. Recently both Nevada and Maine also passed somewhat less restrictive privacy laws. While the CCPA is expected to go into effect on January 1, 2020, in what appears to be a wave of new legislation at the time of publication, at least 15 other states are considering or have proposed their own privacy legislation.

Pending privacy legislation

STATE	BILL	COMMON NAME
CONNECTICUT	RB 1108	
HAWAII	SB 418	
ILLINOIS	HB 3358	Data Transparency and Privacy Act
LOUISIANA	HB 465	Internet and Social Media Privacy and Protection Act
MARYLAND	SB 613	Online Consumer Protection Act
MASSACHUSETTS	SD 341/S 120	
MINNESOTA	HF 2917/SF 2912	
NEW JERSEY	S2834	
NEW MEXICO	SB 176	Consumer Information Privacy Act
NEW YORK	SB S5642	New York Privacy Act
NORTH DAKOTA	HB 1485	
PENNSYLVANIA	HB 1049	Consumer Data Privacy Act
RHODE ISLAND	S0234	Consumer Privacy Protection Act
TEXAS	HB 4518 / HB 4390	Texas Consumer Privacy Act/ Texas Privacy Protection Act
WASHINGTON	SB 5376	Washington Privacy Act

In general, these new and proposed state privacy laws are designed to provide consumers a broad set of rights over the use and retention of their personal information. The CCPA gives consumers broad rights to access and control their personal information and imposes technical, notice, and financial obligations on affected businesses. In addition, it will expand the definition of personal information to include types of data not traditionally considered personal information in the United States. Under the CCPA, personal information encompasses any information that could be reasonably linked, directly or indirectly, with a particular California consumer or household.

The CCPA is designed to provide consumers and eligible employees with five explicit rights. These include the right to opt-out of the sale of personal information (or opt-in for consumers under the age

of 16), right to access, right to deletion, right to portability, and the right to nondiscrimination.

As more states adopt their own privacy legislation, it is entirely possible that new requirements distinct from either the CCPA or the EU General Data Protection Regulation models will emerge. Perhaps most importantly, CCPA and other states' laws will be enforced by both regulators and through a right of private action, potentially spurring significant lawsuits, from class action suits to one-off lawsuits.

Organizations subject to CCPA compliance requirements and other new privacy laws must address some difficult questions: How do we implement an enterprise-wide privacy program that meets the patchwork of individual state (and potentially federal) requirements? How do we implement a privacy program when many of the requirements are still being defined and modified? How do we build organizational literacy and compliance programming that accounts for ambiguity within the CCPA? What is defensible and sufficient for CCPA compliance? Are all levels of the organization ready to operationalize CCPA?

Instead of focusing on meeting each state's requirements as they arise, the more strategic approach is to develop general privacy policies and personal information governance and handling processes. Once the organization has a solid program in place, it can make program adaptations as necessary to account for additional privacy requirements. There are generally enough similarities across all the various existing privacy regimes that organizations can build basic privacy capabilities around classification, information security, production, and disposition. These basic privacy capabilities — or what can be referred to as privacy information agility — should meet most or nearly all of the organization's compliance needs across states. While the ability to adapt to the regulatory environment may be necessary. This approach will be far easier in the long run when compared to developing a privacy program hardwired for a single state, only to have to update the program continuously as states adopt new or additional privacy legislation.

Will there be a federal privacy law?

Shortly after California passed its privacy law, both privacy advocates and companies have been calling for a federal privacy law that would supersede a patchwork of state laws. Privacy advocates want to ensure that such a law would be as strict as the state laws it would be replacing. Likewise, companies see a federal law as one of their last chances to enact less restrictive requirements. Most privacy experts believe that the US federal government will pass such a law, but its timing at this point is uncertain.

Key characteristics of privacy information agility

Designing a privacy program to meet a single state's privacy requirements may increase the risk of substandard compliance across the regulatory environment in which an organization operates. The organization will have to update and redesign their privacy program each time new privacy laws are enacted. The smarter approach is for organizations to consider building baseline privacy protocols that can be easily adapted for changing requirements. This baseline capability is called privacy information agility. Privacy information agility is characterized by these core capabilities:

Do you know what personal information you have and where it is? A key first step is knowing what type of personal information is collected, how personal data flows through the organization (both internally and externally), and where it resides. Consider a data mapping initiative to understand how personal data is processed within your organization.

How is the personal information managed and stored? Determine where the personal information resides and evaluate if it is in a secure environment.

Can you search for the personal information? Establish best practices and develop the process to efficiently search for and produce personal information from an individual consumer or employee.

Do you know where the personal information goes? Review vendor contracts and identify all parties with whom the personal information is shared.

Can you delete it? Evaluate your retention policies and determine whether or not you can you defensibly and easily delete this information upon request?

Many privacy requirements can be met through a focus on developing these core capabilities.

Eleven ways to assess your organization's privacy capability

1. Target the right privacy maturity

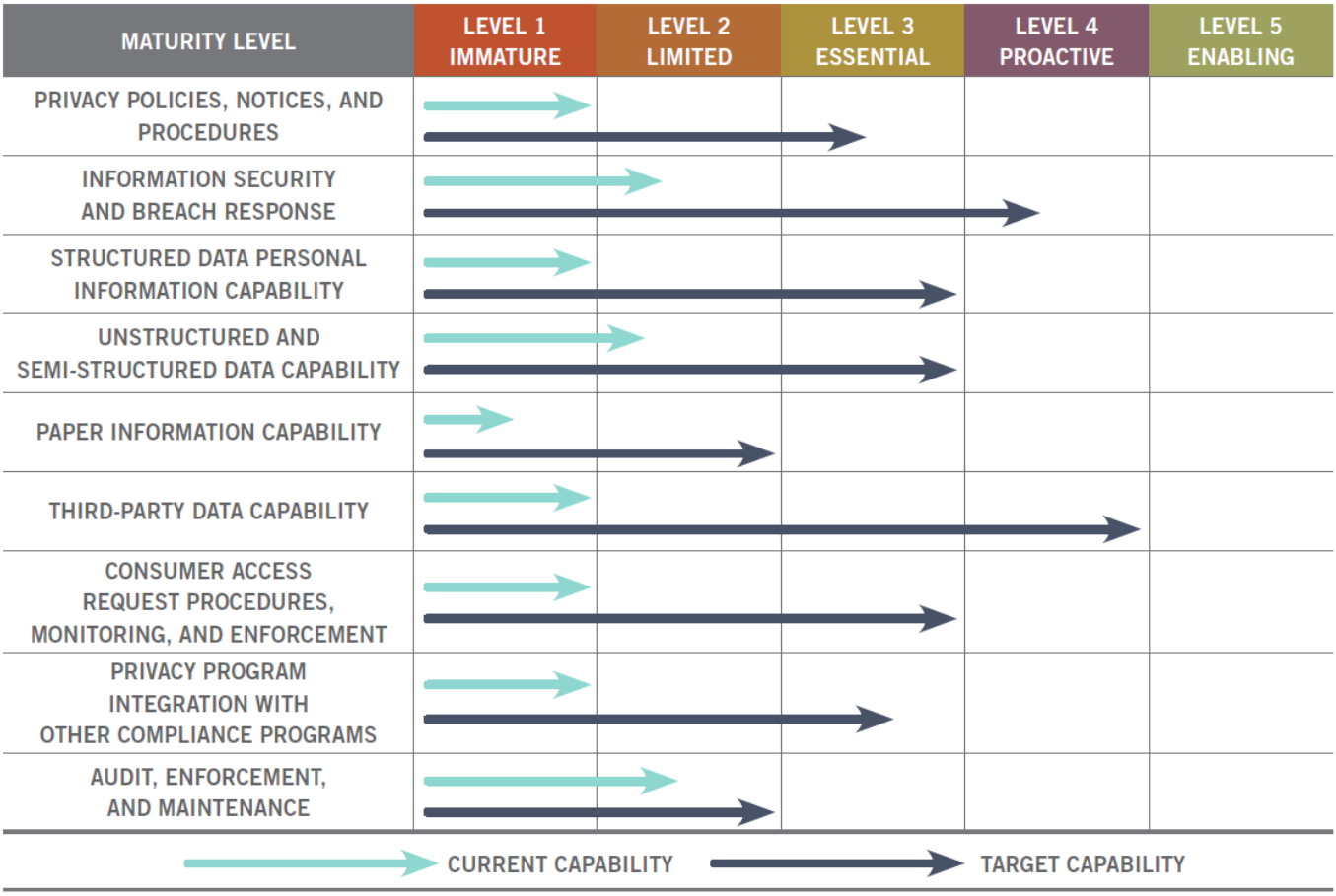


Figure 1. Sample maturity capability model of current capabilities vs. target capabilities. Many

organizations do not need to target the highest level of privacy maturity for any given area in order to achieve compliance with many privacy laws.

Privacy maturity is the concept of reviewing your current capabilities in various privacy areas against your desired target capability. The goal is to measure your current and desired target capability on a scale of preparedness, usually where level one is an “immature” rating all the way up to a level five rating of “enabling.” Savvy privacy professionals know that targeting the right level of privacy maturity is key. Each area in your privacy program may not need to be at the highest level to perform successfully, address vulnerabilities within existing processes, and comply with privacy laws. Utilizing a maturity capability model allows the organization to determine the best level of preparedness for their specific privacy concerns. Organizations should consciously target a specific maturity level and build their programs to meet that level. Figure 1 displays a maturity capability model showing current versus target privacy program capabilities.

Different levels of privacy program maturity are required for different organizations. Organizations vary on the number of consumers whose personal information they collect or process, what they do with that personal information, the quantity and breadth of this information, how widely it is shared, and how this information is stored and managed. A few organizations will indeed need a highly advanced and rather expensive “sports car” level of privacy program maturity; however, many organizations can be better off with a fully capable and more cost-effective “sedan” or even “golf cart” level of privacy program maturity. It is better to have a well-executed, albeit simpler, approach than a more complex, difficult, and expensive “sports car” target maturity that spends more time in the repair shop than being driven.

Organizations fail in their privacy efforts by overreaching and trying to create target capabilities that are too sophisticated or unmanageable for the long term.

2. Privacy policies, notices, and procedures

Figure 2. Privacy policies, notices, and procedures

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ADVANCED
Privacy policy is either informal or non-existent; notices not provided on a timely, comprehensive, or legally sufficient basis; information provided on choice and consent inconsistent with requirements	Privacy policy is either not fully documented or incomplete or exists only for a single regulation; no attempt has been made to customize the policy to meet the organization’s current requirements; notice not easily understood; consent not always documented per requirements; all forms of sharing not fully disclosed	Privacy policy exists and is documented; policy addresses and covers all applicable regulations and has been customized to fit the organization’s current and specific requirements; notice is provided timely, in plain and simple language, with types of information collected and shared fully disclosed	Policy is regularly reviewed and updated; policy includes any specific regional requirements or emerging regulations; notices regularly reviewed and updated; individual choice and consent preferences are documented, tracked, and audited	Fully integrated policy across all geographies, jurisdictions, and emerging regulatory frameworks; continuous improvement to all notices based on changes in law, business practices, and third-party relationships

The CCPA will require affected organizations to either create a privacy policy or review and update their external privacy policy and notices. Organizations will also need to update and add notices, as well as create new processes and procedures.

Keep in mind that the development of the privacy policy is as important as the execution of the

privacy policy. Many aspects of the CCPA, as well as other privacy legislation, are nonprescriptive, and a risk is that an organization will put significant effort into creating an extremely detailed privacy policy at the expense of its execution. The main thrust of the privacy program becomes simply having policies. To avoid this, it may benefit an organization to develop a solid privacy policy, and then dedicate resources to focus on ensuring they are executing and operationalizing that policy by classifying, securing, managing, and building the capabilities to comply with CCPA.

3. Privacy organization and awareness

Figure 3. Privacy organization and awareness

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ENABLING
There are no resources dedicated to privacy activities, or are provided on a limited ad hoc basis; no coordination across departments; business units have little exposure; no formal privacy training	Privacy is owned and managed by individual departments or business units with adhoc coordination on privacy issues; limited privacy training	Resources are authorized to provide privacy support throughout the organization; key stakeholders engage through a steering committee; formalized privacy training	Privacy organization exists, with dedicated privacy owner; participation in steering committee from business units; dedicated privacy coordinators conduct training for all employees	Executive management reviews privacy functions annually; privacy coordinators meet regularly; privacy awareness leads to strong privacy culture

Depending on your organization, anticipate that compliance with CCPA and similar privacy regulations may be a culture shift on several levels. A single person serving as the organization's privacy officer and updating a privacy policy once a year will not be sufficient. A well developed privacy program should not be viewed as a check-the-box operation — it is a living program with ongoing responsibilities throughout the organization. A successful privacy program must identify and engage stakeholders from throughout the organization. It should not be seen as something that only the legal department takes on or only the IT department implements. It often includes organizing a cross-functional privacy steering committee, creating and conducting privacy awareness training, and building executive-level support. Compliance with the new privacy regulations such as CCPA will not be a one and done matter. You will need to implement a long-term plan. Your organization is constantly changing — and your privacy program must follow suit.

4. Information security and breach response

Figure 4. Information security and breach response

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ENABLING
No or limited information security program; access controls inconsistent/ incomplete; no incident monitoring in place; no breach response or business continuity plans; no security for data transmission	Limited or only partially implemented information security program; no documented data security classification policy; ad hoc incident monitoring; limited breach response / business continuity plans; limited security for data in transmission	Comprehensive, enterprise-wide information security program including documented data security classification policy; formalized and documented incident monitoring program and response; documented procedures for breach response, access controls, business continuity	Annual review of privacy risk and practices based on privacy requirements; continuous monitoring of all access controls and incident logs for continual improvement; regular walkthroughs of breach management plan	Annual review of security program for effectiveness; formal risk management program relating to privacy; monitoring includes utilizations of advanced security technology; formalized and systematic analysis of breach, access attempts and response activities

The CCPA and similar privacy laws have strong penalties and enforcement measures for organizations in the event of a data breach. There are already existing data security breach notification laws with penalties on the books in all 50 states. With the enforcement measures and penalties prescribed under new privacy laws, organizations should review and strengthen their data security programs, including their breach response policies and procedures. It will also be important to review the data security practices of third parties and service providers that you provide, sell, or share personal information with. Most organizations have some level of information security program already in place. The exact security program your organization needs will depend on the type, medium, and location of the personal information.

5. Structured data capability

Figure 5. Structured data capability

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ENABLING
Personal information is not identified in databases or other structured systems; no procedures for access or security controls of personal information; no procedures for production or deletion under data privacy requirements	Basic data classification of personal information identified across major systems; no workflows mapped; processes exist for access and authentication of personal information in structured systems, but not documented; ad hoc procedures for deletion of structured data for access requests under data privacy requirements	Personal information specifically identified, classified and inventoried in all structured enterprise systems; workflow of personal information across structured systems identified; systems comply with security policies; documented procedures for production privacy information; documented; approved procedures for deletion of structured data for access requests that maintain referential integrity; internal privacy information access controls	Personal information identified and inventoried in departmental databases or systems; structured systems subject to regular security monitoring and testing; documented procedures for production of structured data for access requests for departmental systems; older, expired, unneeded older privacy information routinely deleted from structured systems; records of deletion retained	Formal system change management process identifies personal information as new systems are deployed or retired; structured systems personal information monitoring and security testing for newly deployed systems and change management for existing systems; easily executable and scalable production and deletion processes for all personal information in all relevant structured systems

Significant amounts of personal information may live in applications that store that information in structured databases. These databases are often homegrown applications within the organization or third-party applications that the organization has contracted to use. Personal information often flows from one system to another, sometimes creating many copies of the same data. Organizations need to develop capabilities for managing this structured personal information.

Privacy compliance requires the capability to identify and secure personal information in these structured databases, and also the capability to produce personal information in response to a consumer or employee access request, as well as deleting or “de-identifying” it through pseudonymization procedures.

6. Unstructured and semi-structured data capability

Figure 6. Unstructured and semi-structured data capability

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ENABLING
Personal information is not systematically identified in file systems, desktops, email systems, offline or desktop email storage, or other unstructured or semi-structured repositories; limited or no application of data security processes; no procedures for access, production, or deletion of data for access requests under data privacy requirements	Basic categories of personal information identified in specific locations within larger unstructured repositories and email; ad hoc processes exist for access, authentication, production, and deletion of personal information in unstructured systems, but not documented	Personal information identified and inventoried for all unstructured and semi-structured data, including email servers, repositories, and desktops; unstructured and semi-structured systems and repositories have access and security controls implemented and monitored; documented procedures for production and deletion of unstructured or semi-structured data for access requests for enterprise and departmental systems	Personal information in unstructured or semi-structured media; unstructured and semi-structured systems subject to regular security testing; documented procedures for access, production, and deletion of unstructured or semi-structured data for access requests for departmental systems, including individual information stores; older, expired, unneeded older privacy information routinely deleted from structured systems	Change management process identifies and disposes personal information as new systems are deployed or retired; unstructured and semi-structured systems security testing incorporated into change management for newly deployed systems; easily executable and scalable production and deletion processes for unstructured semi-structured systems

While personal information is typically associated with information in structured databases, large amounts of personal information may exist in unstructured and semi-structured formats. Examples of unstructured or semi-structured data can include shared file drives, email messages, word processing documents, videos, photos, audio files, and other kinds of common documents. Many organizations fail to address unstructured and semi-structured data, potentially creating risk for noncompliance issues. Under the CCPA and other privacy laws, personal information stored in unstructured or semi-structured formats or locations is in scope and can be particularly challenging to manage. Consider identifying sources of unstructured and semi-structured data and consider end user access controls and data handling best practices to account for the type of information stored in these locations and focus on employee training and improving visibility of these sources.

7. Paper information capability

Figure 7. Paper information capability

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ADVANCED
Personal information is not systematically identified in either onsite or offsite paper records or documents; little or no physical security applied to documents containing personal information; no procedures for production and secure destruction of paper-based personal information under data privacy requirements	Personal information identified in paper documents in some locations on a limited, ad-hoc basis; physical security applied to some onsite or offsite paper document storage, but not consistently; ad hoc procedures for production and secure destruction of paper-based personal information under data privacy requirements	Paper-based personal information identified and inventoried for all onsite and offsite locations; physical security applied to all paper documents containing personal information; consistent, documented processes for production and secure destruction of paper-based information	Paper-based personal information routinely converted to electronic format, and paper copy is securely destroyed; physical security subject to regular testing; scalable and efficient processes for production and secure destruction of paper-based privacy information	Paper-based personal information classified upon initial creation or receipt; full physical security and access controls applied to entire lifecycle of paper documents containing personal information; fully scalable production and secure destruction of paper-based privacy information

In most organizations, paper documents tend to accumulate in both onsite and offsite storage facilities, some of which will most likely contain a significant amount of personal information. CCPA and other new privacy laws do not exclude paper records, and as such identifying and producing this paper-based information can be particularly burdensome. Hence, an organizations privacy program

must address paper documents and third-party storage.

Often paper-based personal information is either scanned into an electronic format or ideally destroyed as soon as its organization-prescribed retention period is reached.

8. Third-party data capability

Figure 8. Third-party data capability

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ADVANCED
Personal information stored, shared or sold to third parties not identified; third party service level agreements (SLAs) contain no provisions regarding production, deletion, retention, or handling of personal information; no communications with third parties on privacy requirements	Limited identification of personal information stored, shared or sold to key third parties; SLAs provide for the discovery and production of information to meet personal information requests; SLAs do not address the unauthorized sale, retention, use, or disclosure of personal information; privacy requirements communicated	All personal information stored, shared, or sold to all third parties identified; SLAs provide the capability to discover, produce, and delete personal information upon request; SLAs require third party to delete a consumer's personal information upon request, as well as fulfilling other consumer access requests; agreement covers re-use, enrichment, retention, and disposition	Third-party personal information tracked throughout lifecycle, from creation through transmission, data enrichment, retention, and disposition; SLA sets a specific retention period for personal information; SLAs require the use of specific security measures (e.g., encryption, anonymization) to protect personal information	Formal system change management process identifies all data flows for all third personal information as new systems are deployed or retired through entire lifecycle; SLA allows for a specific retention period for personal information to be set to match the retention period of the company at an individual content level

Organizations must have the capability to address the personal information they collect that is either sold or shared with third parties, or likewise that they receive themselves. This includes developing the appropriate Service Level Agreements (SLAs) that outline data handling expectations and restrictions as well as ensuring that all third-parties have the capability of complying with the privacy requirements. Many organizations are surprised to find out the extent to which personal information may be shared by third parties.

Well-designed third-party capabilities set clear expectations over who is responsible for what. This is always easier to address proactively. Developing clauses to promote data handling in compliance with privacy laws and obligations should help minimize misuse or lack of insight into how personal data is managed once it is shared externally.

9. Consumer access request procedures, monitoring, and enforcement

Figure 9. Consumer access request procedures, monitoring, and enforcement

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ADVANCED
No method of authenticating identity of consumer; consumer access requests are not tracked; no procedures in place to audit access request process	Some ad hoc processes in place for verifying identity; tracking of consumer access requests is manual and inconsistent; basic guidelines in place to audit consumer access request process, but not routinely followed	Identity authenticated via use of ID and password used for account; access request tracking is centralized; audit procedures are well defined and published; audits are ad hoc in nature	Identity verified through use of industry-recognized authentication standards; access requests are automatically logged, including workflow to respond to the request; full records retained of requests; access request process is routinely audited	Authentication mechanism regularly monitored and audited for effectiveness; continuous improvement of access request tracking processes, audit processes, and technology use

CCPA and other proposed laws require a series of processes to support consumer access, production, and deletion requests. These include authentication processes, search processes, production processes as well as deletion processes. Furthermore, these processes need to be tracked and monitored for compliance.

10. Integration with other compliance programs and processes

Figure 10. Integration with other compliance programs and processes

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ADVANCED
Privacy processes are not integrated with records management policies and schedules, records processes, or data classification standards; privacy processes are not integrated with legal discovery processes	Privacy only addressed in Records Policy but not the Records Schedule or data classification standards; privacy disposition request suspended if in conflict with legal hold	Privacy information inventory cross-referenced with the Records Schedule; privacy deletion requests are synchronized with retention requirements; routine consumer request destruction processes fully suspended for groups of documents under legal hold	Records management and privacy classification occur as a single process; automated records destruction processes fully suspended for individual privacy information under legal hold	Automated controls prevent the premature deletion of records containing privacy information; release of legal holds automatically invokes resumption of pending privacy deletion requests

One of the problems that has emerged from the CCPA and similar privacy laws is the need for the privacy program to coordinate with other existing compliance regimes within the organization, including records management, compliance with other existing privacy laws (e.g., HIPAA, FERBA, GLBA), as well as eDiscovery and legal holds. The CCPA, for example, would not require requests for deletion of personal information under an organization's legal hold, but these two groups of processes need to be coordinated.

11. Audit, enforcement, and maintenance

Figure 11. Audit, enforcement, and maintenance

LEVEL 1 IMMATURE	LEVEL 2 LIMITED	LEVEL 3 ESSENTIAL	LEVEL 4 PROACTIVE	LEVEL 5 ADVANCED
No privacy procedures in place; privacy-related issues or concerns are addressed informally; no process to address inquiries, disputes, or complaints; no formal compliance program; ad hoc remediation on specific issues/ individuals; no change control process applied to policies or processes	Privacy procedures established in certain areas, but not well understood or consistent across the organization; processes are in place to monitor for changes, address disputes, inquiries and complaints, and measure compliance, but are not fully documented; policy acknowledgment tracked and can be escalated; policies and processes are updated on an ad-hoc basis; changes to privacy processes are handled in an ad hoc manner	Privacy procedures are well-defined and published; documented policies are in place to address changes, disputes, inquiries, complaints, and monitor compliance; risks identified and communicated on a regular basis; policies and processes updated minimally every 12 to 18 months; trainings are also updated concurrent with the program update; audit results are feedback into a change control process	Well defined and published privacy procedures are reviewed and updated and published on a regular basis; established process for monitoring privacy environment; disputes, inquiries, or complaints addressed in timely manner; management monitors noncompliance; risks identified and formal remediation plans developed annually	Privacy procedures are routinely audited for compliance and fully integrated into the organization; continuous monitoring and analysis used to improve privacy process; non-compliance results in training and disciplinary action; internal audit findings communicated to key stakeholders for remediation plan

Finally, privacy laws and the resultant programs are hardly stagnant. New laws are being enacted

and current legislation is subject to amendments as well as implementation guidelines. To this end, privacy programs should not be thought of as “one and done,” but rather have audit, enforcement, and maintenance processes built within them.

Final thoughts

New and emerging privacy requirements like the CCPA can be both daunting and overwhelming. With significant risks and penalties for noncompliance, it can be challenging to assess what level of privacy maturity is needed for any given organization’s privacy program. Organizations should avoid the desire to start looking for the perfect policy, the perfect process, or the perfect tools. Additionally, organizations should avoid the mentality that they are not ready to start the CCPA compliance process because they are not at 100 percent in their privacy program. In the meantime, documents and data accumulate, privacy requirements become stricter, and the risks increase. Perfect becomes the enemy of good.

You may be asking: How much is enough to comply with CCPA and other similar privacy laws? Privacy is an inherently imperfect process. Fortunately, the courts and regulators generally do not expect perfection. Rather, they expect reasonable, good faith efforts to comply. In your policies, declare what will be done. Execute those policies with processes, technology, and training. Demonstrate that policies are being complied with through training and audits. Show that a plan has been developed. Show that the plan is being executed. Audit the results and remediate any shortfalls. Not perfect? That is OK. Start with good and keep moving forward.

ACC EXTRAS ON… Privacy regulation

ACC Docket

This Week in Privacy: Finding the Best Privacy Control Framework (Sept. 2017).

Articles

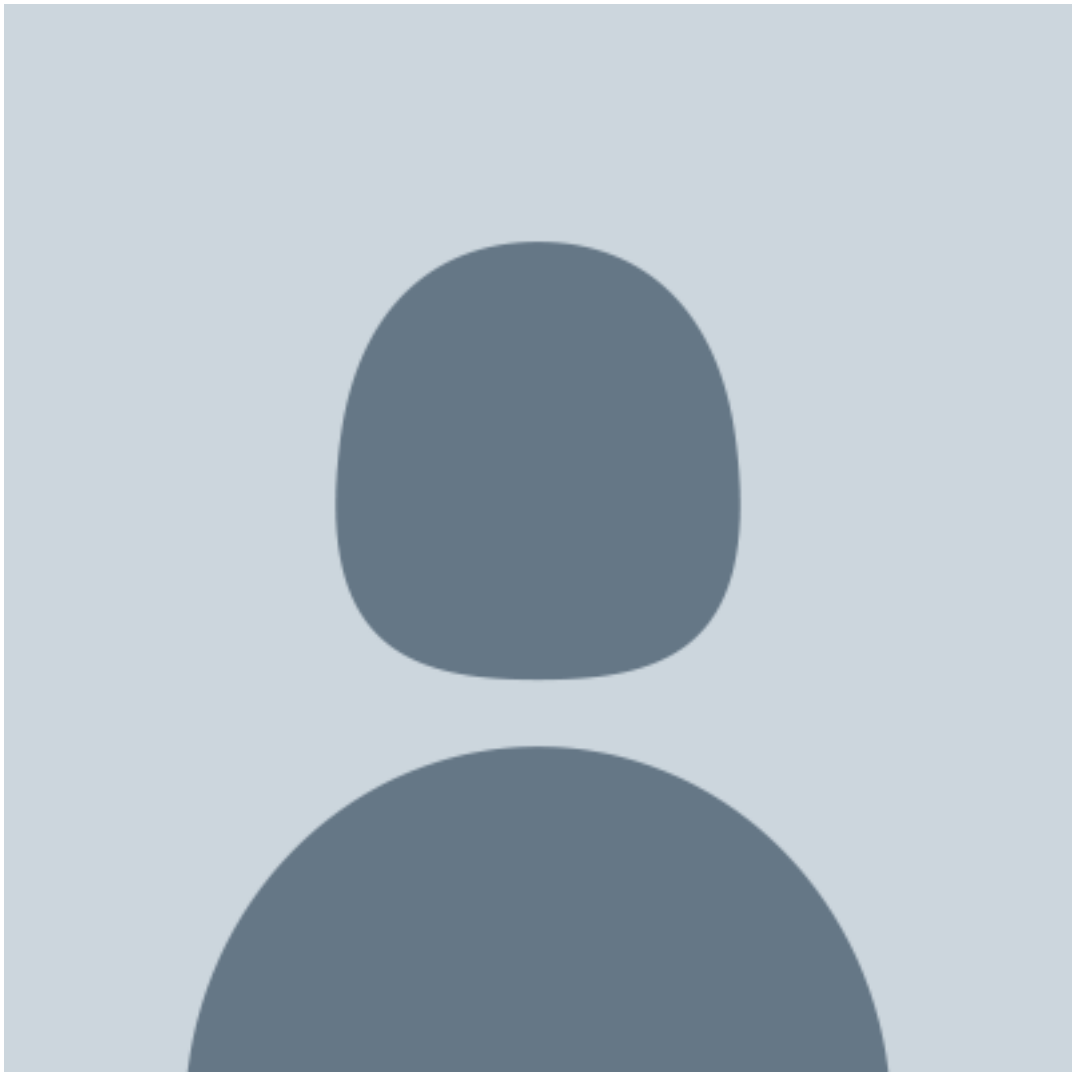
Operationalizing the California Consumer Privacy Act (United States) (June 2019).

Overview of Data Privacy Laws in India and Aspects of Data Protection That Your Company Should Take into Account When Establishing a Business in India (Feb. 2017).

Sample Forms, Policies, and Contracts

ACC US States’ Privacy Capability Maturity Model (April 2019).

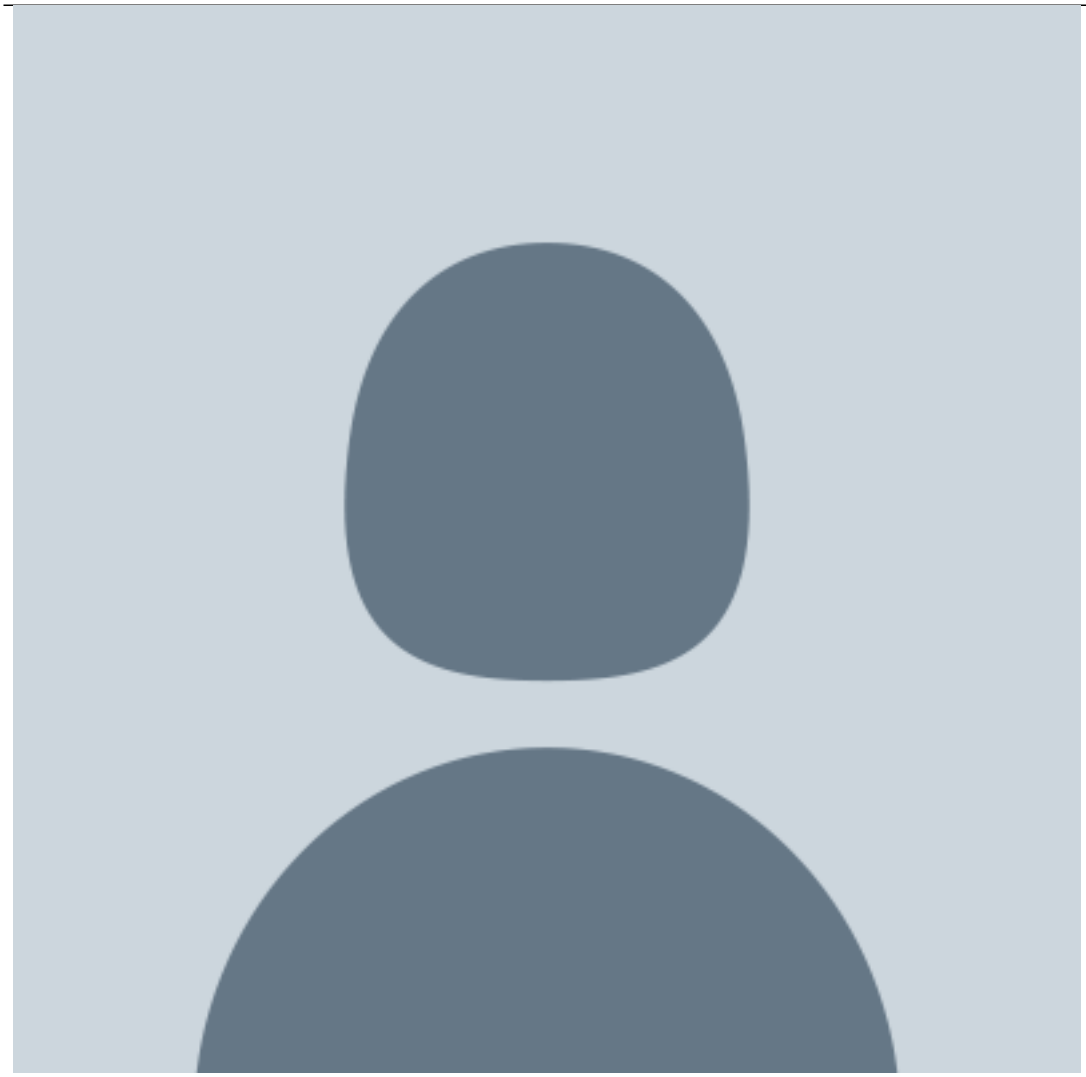
Robin Shapiro



Corporate Legal Counsel

Career Education

Justin Allen



Assistant General Counsel

TCS Education System

Mark Diamond

CEO and Founder

Contoural Inc.

Mark Diamond is the CEO and founder of Contoural Inc., an independent provider of information governance consulting services. His company works with more than 30 percent of the Fortune 500, plus many mid-sized and smaller companies.