Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

ACC Guide[SM]

Operationalizing the California Consumer Privacy Act (United States)

Sponsored by:

Association of Corporate Counsel
1001 G Street, NW, Suite 300W
Washington, DC 20001
tel +1 202.293.4103, **fax** +1 202.293.4701
www.acc.com

Operationalizing the California Consumer Privacy Act (United States)

June 2019

Provided by the Association of Corporate Counsel
1001 G Street NW, Suite 300W
Washington, DC 20001 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

This ACC Guide addresses how to operationalize the California Consumer Privacy Act (CCPA). It provides a quick overview of the Act, compares California's requirements to other privacy laws, and points out key program considerations. Next, it details the key activities companies must undertake to operationalize, including specific policies, processes, technology and training. The final section looks at assessing operational maturity.

This material was developed by Contoural, Inc. Contoural is a sponsor of the Information Governance Network and a sponsor of the Legal Operations Network Records Management and Information Governance Foundational Toolkit. For more information about the author, visit their website at www.contoural.com or see the "About the Company" section of this document.

The information in this ACC Guide should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Contoural, Inc. or of the Association of Corporate Counsel (ACC) or any of its lawyers, unless so stated. This ACC Guide is not intended as a definitive statement on the subject, but rather to serve as a resource providing practical information to the reader.

Contoural and ACC wish to thank members of the Information Governance Network for their support in the development of this Guide.

Contents

I. Introduction

On June 28, 2018 the California Legislature passed the California Consumer Privacy Act ("CCPA" or the "Act"). This sweeping and hastily created legislation creates significant new requirements for identifying, managing, securing, tracking, producing and deleting consumer privacy information. This Act will likely serve as a model for other US states, and its effects will be felt well outside California. At the time of publication more than fifteen additional US states have proposed or are considering their own privacy laws with requirements similar to California, and similar proposals are being considered at the US federal level. With a relatively short deadline, coupled with potentially significant penalties, organizations need to start developing a program now.

II. CCPA Quick Overview

While this ACC Guide is not intended to provide an exhaustive review of the entire Act, it is useful to review some of its requirements.

A. CCPA Five General "Rights"

The CCPA takes the position that consumers "own" their privacy information and provides them five general "rights" for their personal information. Under the Act, California consumers will have the right:

1. **To know what personal information is collected about them**
   Consumers will have the right to know, through a general privacy policy or notice (and with more specifics available upon request) what personal information a business has collected about them, its source, and the purpose for which it is being used.

2. **To know whether and to whom their personal information is sold/disclosed, and to opt-out of its sale**
   Companies that provide or make consumer data available to third parties for monetary or other valuable consideration are deemed to have sold the data and will need to disclose this. Subject to certain exceptions, consumers will then have the further right to opt out of the sale of this information by using the "Do Not Sell My Personal Information" link on the business' home page, which is required by the Act. Moreover, those 16 years- old and under must opt-in to have their information sold. Note that the term "sold" is not limited to the actual sale of privacy information but can be interpreted broadly to include sharing of privacy information with other parties.

   Businesses must enable and comply with a consumer's request to opt-out of the sale of personal information to third parties, subject to certain defenses. The Act requires business to include a "Do Not Sell My Personal

Information" link in a clear and conspicuous location on a website homepage. Additionally, businesses must not request reauthorization to sell a consumer's personal information for at least 12 months after the person opts-out.

3. **To access their personal information that has been collected**
   Consumers will have the right to request certain information from businesses, including the sources from which a business collected the consumer's personal information, the specific elements of personal information it collected about the consumer, and the third parties with whom it shared that information. The Act requires that businesses provide specific means for consumers to submit these requests, typically a toll-free number and a web link. Once the request is made, businesses must disclose the requested information free of charge within 45 days, with extensions of time available in certain circumstances.

   A business must comply with a verifiable consumer request and it must respond within 45 days, which is potentially extendable once for another 45 or 90 days on customer notification. Likewise, it must inform the consumer of the reasons for not taking action. Furthermore, it must provide the information free of charge, unless the request is manifestly unfounded or excessive. Consumers may only make information requests twice a year with a 12-month look-back.

4. **To have a business delete their personal information**
   Consumers can request that personal information a business has collected be deleted. Some personal information is exempt from deletion requests, including information under legal hold (until the matter is adjudicated or until the hold is released) and for information that must be retained per legal or regulatory recordkeeping requirements.

5. **To not be discriminated against for exercising their rights under the Act**
   The CCPA gives consumers the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act. As such, businesses may not "discriminate" against consumers for exercising these privacy rights. They cannot deny goods or services, charge different prices, or provide a different quality of goods or services to those consumers. There are some exceptions, however, on the service levels that can be provided. It is expected that this definition of "discrimination" will evolve either from guidance from the attorney general or case law. It should be noted that even though the Act requires the California Attorney General to provide implementation guidelines, he has publicly stated he is reluctant to do so.

B. Who Is Covered?

The Act covers the Personal Information of all natural persons who are California Residents. The Act defines a "resident," as (1) every individual who is in the State for other

than a temporary or transitory purpose, and (2) every individual who is domiciled in the state, but is outside the State for a temporary or transitory purpose. All other individuals are nonresidents. Note that if an individual acquires the status of a resident by virtue of being physically present in the State for other than temporary or transitory purposes, this person remains a resident even though temporarily absent from California. If, however, this person leaves California for other than temporary or transitory purposes, this person is no longer considered a resident.

The Act also places additional restrictions on information about children. The CCPA prohibits selling personal information of a consumer under 17 without consent. Children aged 13 – 16 can directly provide consent, while a parent must provide consent before. Selling personal information about a child under 13 can be requires parental consent. Importantly, protections provided by the US federal Children's Online Privacy Protection Act (COPPA) still apply on top of the CCPA's requirements.

It is important to note that the definition of the word "sell" for purposes of the CCPA is broad and includes, "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or third party for monetary or valuable consideration." This definition includes most uses of personal information sharing between business, even if the personal information is not explicitly sold.

C. Who Must Comply with the Act?

As a threshold, the CCPA applies to for-profit businesses that collect and control California residents' personal information, do business in the State of California, and meet one of these three requirements:

1. Have annual gross revenues in excess of $25 million; or
2. Receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or
3. Derive 50 percent or more of their annual revenues from selling California residents' personal information.

Organizations exempt from the act include public agencies, non-profits, and small companies who do not meet any of the requirements listed above. Also, any information collected while commercial conduct takes place "wholly outside California" is exempt. Note, however, that identifying a consumer in California and then later collecting personal information when that person is outside of California would not be exempt. Note that any entity that controls or is controlled by a covered business or shares a common branding with a covered business, such as a shared name, service mark, or trademark is also subject.

D. What Qualifies as "Personal Information"

The CCPA defines personal information extremely broadly as "information that identifies,

relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." In other words, the State recognizes a "broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information" that can be used to identify an individual. Examples of covered personal information include:

- Personally identifiable information such as name, address, phone number, email address, social security number, driver's license number, etc.
- Biometric information, such as DNA or fingerprints.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available.
- Inferences drawn from any of the above examples that can create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Information collected by federal, state or local government entities that is used in a manner compatible with the purpose for which it was collected above is not covered by the Act. Also note that certain types of privacy data already covered by other regulations are excluded. These include the US Gramm-Leach-Bliley Act (which requires financial institutions to explain their information-sharing practices and to protect sensitive data), the US Driver's Privacy Protection Act (relating to the privacy and disclosure of personal information gathered by US states' Departments of Motor Vehicles), and the California Financial Information Privacy Act.

The Act's broad definition of personal information poses a number of extreme privacy information challenges. For example, if a company conducts video surveillance that records identifiable faces, one could argue that this video contains privacy information under the Act. We expect the definition of privacy to evolve either through clarifications from the Attorney General of California, amendments or case law. Companies are advised to monitor this carefully.

E. Deidentified or Anonymized Data

The CCPA does not restrict a business's ability to collect, use, retain, sell, or disclose consumer information that is deidentified or aggregated (see section below on

deidentification). However, it does set a high bar for claiming data is deidentified or anonymized. Data that has been pseudonymized may still be considered personal information under the CCPA's broad definition of personal information because it remains capable of being associated with a particular consumer or household (See Section IV, Part B, Figure 1. For an example of Pseudonymous data). However, as of this writing the statute does not clearly categorize or exclude pseudonymous data as personal information. There is hope that future guidance from the Attorney General will clarify this.

F. Privacy Notice / Information Right

Unlike General Data Protection Regulation (GDPR), CCPA does not require consumers to "opt in" for the sale or use of their personal information. However, CCPA requires very specific privacy notices as well as providing the right to opt out of the sale or use of personal information. Furthermore, businesses are prohibited from "discriminating" against consumers in the event they exercise these opt out rights.

These notices need to inform consumers about what personal information categories will be collected and the intended use or purpose for each category. The CCPA requires that businesses provide specific information to consumers and establishes delivery requirements. Third parties must also give consumers explicit notice and an opportunity to opt out before re-selling personal information that the third party acquired from another business.

G. What Constitutes "Sale" of Data

It is important to note that as noted at Section B above, the broad definition of the word "sell" for purposes of the CCPA includes most uses of personal information sharing between business, even if the personal information is not explicitly sold.

H. Security and Breaches

Unlike the European privacy requirements under GDPR, CCPA does not directly impose data security requirements. However, it does establish a right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk arising from existing California law. CCPA, like most cybersecurity and data privacy laws, do not define "reasonable security."

I. Penalties and Private Rights of Action

The CCPA establishes a narrow private right of action for certain data breaches involving a sub-set of personal information. However, the Act grants companies a 30-day period to cure violations, if possible. Consumers may seek the greater of actual damages or statutory damages ranging from $100 to $750 per consumer per incident. Courts may also impose injunctive or declaratory relief.

Fines for violations include:

- $2,500 for unintentional and $7,500 for intentional violations of the Act. (These actions must be brought by the California Attorney General.)
- $100-$750 per incident, per consumer- or actual damages, if higher – for damage caused by a data breach. (These actions may be brought by consumers.)

As currently written the law states that a business shall only be in violation of the CCPA if it fails to cure any alleged violation of the CCPA within 30 days after being notified of alleged noncompliance. As the Act is currently written, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. However, the company still may face liabilities from other privacy and breach laws.

While these fines may appear relatively low, it is important to keep in mind they are per violation. It is not uncommon for a privacy incident to affect thousands or tens of thousands of consumers, in which case these fines could reach the hundreds of thousands or millions of dollars. Perhaps most important, CCPA's greatest impact will likely be felt through de facto enforcement from class action litigators. The Act permits a right of private action for instances in which a consumer's nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business's failure to maintain reasonable security procedures. This should be monitored as proposed amendments to the Act call for both expanding the right of private action as well as eliminating the cure period.

J. CCPA Timeline, Amendments and Attorney General Implementation Guidelines

The California legislature has passed several amendments to the CCPA which impacts the implementation timeline. The original legislation called for the Act to go into effect on January 1, 2020. A subsequent September 2018 amendment stipulated that the Act will be in effect immediately but be enforced no earlier than January 1, 2020.

The Act also requires the California Attorney General to adopt implementing regulations meant to "further the purpose" of the law. These may include, for example, clarification on the categories of data considered to be "personal information." The publication of these guidelines will impact the timelines as the attorney general may not bring enforcement of the Act until six months after the adoption of those implementation regulations, or July 1, 2020, whichever is sooner. It is important to understand that the Attorney General "may" publish "general guidance." It is unclear how much utility these updates will provide to businesses, as Attorney General Xavier Becerra has already clarified that his office's goal is to protect consumers, and not in his words to "give out free legal advice" to companies.

In addition to the implementation guidelines, since the September 2019 Amendment, the

California legislature has proposed numerous additional amendments. There are spirited lobbying efforts both by privacy advocates as well as business groups, with advocates pushing for increased requirements and business groups generally looking to weaken the Act or make it easier to implement. It is likely this activity will continue not only through the enforcement date, but also well after.

Finally, despite changes to the law coming from the Attorney General's implementation guidelines as well as amendments, it is expected that core privacy rights and requirements will remain unchanged. Companies need to start preparing today to meet enforcement deadlines, regardless of what parts of the Act may change.

III. Comparing CCPA to GDPR and Emerging State Privacy Rules

While the CCPA has many of the same requirements as the European General Data Protection Regulation ("GDPR"), there are some key differences. Companies that have complied with GDPR will need to update policies, processes and procedures to comply with CCPA. Furthermore, at the time of this publication fifteen additional US States are considering or have proposed privacy legislation. There have also been proposals at the federal level. There are some differences between these proposed laws and CCPA. It is important for companies to understand these differences and build overall personal information management capabilities to comply with all the current and upcoming requirements that apply to them.

A. Similarities and Differences to European GDPR

While there are a number of similarities between California's CCPA and the European Union's General Data Protection Regulation (GDPR), there are also a number of differences. The table below provides a comparison.

	California Consumer Privacy Act	European GDPR (for reference)
Who Must Comply?	For-profit entities doing business in California, or any entity that controls or is controlled by a covered business.	Entities both within and outside the EU that process personal data in the context of activities of the EU establishment, regardless of whether the data processing

		takes place within the EU.
Who Is Covered?	California residents that are either in California for other than a temporary or transitory purpose or domiciled in California but are currently outside the State for a temporary or transitory purpose.	Data subjects which are defined as identified or identifiable persons to which personal data relates
How Personal information Defined?	Defined very broadly as personal information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household. Certain types of information are excluded.	More narrow definition that includes personal data as well as special categories
Rights	Rights to access and deletion broader	Similar right to erasure
Security	Not included but does establish right of action for violations that occur due to reasonable security practices.	Procedures for protecting information
Disclosures	Specific requirements for disclosure	Less prescriptive
Data sharing	More restrictive – but no rules for transfers outside the United States	Restrictions on data transfers outside of specific countries
Privacy by design/default	Not included	Required
Opt-in/out Right	Must enable and comply with consumer's request to opt out, including "Do Not Sell Notice" on website.	Requires residents to "opt in."

Data protection impact assessments	Not included	Required if certain criteria are met
Data protection officer	Not required	Required.
Enforcement	Attorney General and litigators	Country privacy regulators

Table 1. While CCPA has similar requirements to GDPR, there are also key differences.

Companies that have implemented GDPR compliance can leverage parts of these programs to meet CCPA requirements. However, additional program development for CCPA will still be required.

B. CCPA Is a Harbinger for Other States and Federal Legislation

While businesses without a commercial presence in California or that don't engage or sell California consumer information may express relief at not having to comply, these businesses should monitor this law. First, in many cases it may be difficult for companies to segregate California consumers from other consumers, especially in online information gathering. Second, at some point businesses will feel pressured to offer these privacy protections to their non-California customers. It may be difficult for them to justify providing these protections to some customers but not others. Finally, and perhaps most important, other states are likely to follow suit. The first data breach disclosure laws were initially introduced by California in 2003 and many states adopted similar legislation thereafter. It is also expected that many other states eventually will pass legislation similar to CCPA.

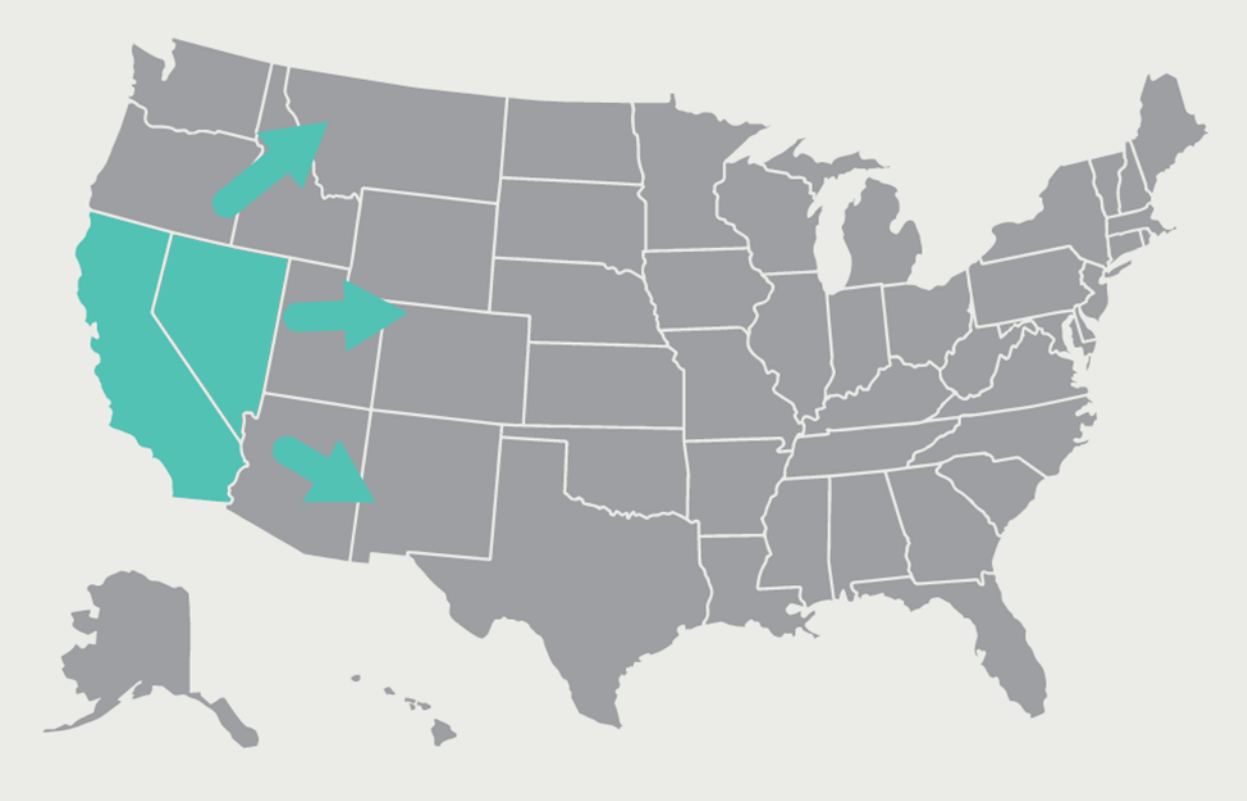

Figure 1. Nevada was the first state to adopt legislation after California. Many other states are expected to adopt legislation similar to CCPA.

C. Additional Privacy Rights and Requirements Beyond CCPA

Both GDPR and emerging US state privacy legislation detail additional rights not enumerated in the CCPA.

Right to Rectification – right for individuals to have inaccurate personal data rectified or completed if it is incomplete.

Right to Restriction – provides individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organization uses his or her data.

Against Solely Automated Decision Making – Prohibits organizations from making decisions based on personal information solely on automated processes, without human involvement. Some argue, for example, that this could outlaw the practice of automated differential pricing in online commerce.

Data Breach Notification – Some newer US state legislation in the proposes stricter notification requirements in the event of a breach.

Risk Assessment – Requires organizations to create a process for identifying and minimizing the privacy risks of new projects or policies.

Purpose Limitation – Requires that data must be collected for specified, explicit and legitimate purposes only (purpose specification), and that data must not be further processed in a way that is incompatible with those purposes (compatible use).

Process Limitation – Similar to purpose limitation, organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.

A quick review of CCPA and other privacy requirements reveal that these laws are effectively still a work in progress. Nevertheless, with enforcement deadlines looming companies can ill afford to wait for more prescriptive legislation. This will require them to create general privacy capabilities that can be updated and modified and new requirements emerge and existing requirements become clearer.

D. Preparing for a Patchwork of State Privacy Requirements

A risk of privacy programs is designing a program to meet a single state's privacy requirements, only to have to update and redesign the program as new privacy laws emerge one-by-one. Instead companies should consider building a baseline privacy capability that can then be more easily adapted as new requirements emerge. We call this baseline capability "Privacy Information Agility". Fundamentally, this agility is characterized by these core capabilities:

Do You Know What You Have and Where It Is? – A key first step is to know what type of personal information lives and flows through the organization, and where it resides.

Is It Managed and Stored Securely? – Does personal information reside in a secure environment

Can You Search for It? – Can you efficiently search for and produce personal information from an individual consumer

Do You Know Where It Goes? – Can you identify with whom this information is shared?

Can You Delete It? – Can you defensibly and easily delete this information upon request?

Nearly all privacy requirements can be met through these core capabilities.

IV. Key Program Considerations

A. Special Information Governance Considerations

While the CCPA allows consumers to request that their personal information be deleted, there are situations where other compliance requirements may override these requests. First, records retention laws and regulations may require companies to retain records for a

certain number of years. These requirements can override consumer deletion requests, even if the record in question contains privacy information. For example, a customer of a financial services company may request his personal information deleted after he closes his account, but recordkeeping rules require that this account information be retained at least seven years in most states. Organizations need to ensure that any deletion request does not run afoul of applicable recordkeeping requirements. As such, organizations need to be up to date and clear on their recordkeeping requirements.

Another area excepted by CCPA is data under legal hold either due to litigation or regulatory inquiry. The obligations imposed by the CCPA do not restrict a business' ability to comply with the law, or exercise or defend legal claims; this would include the obligation to preserve information if it becomes relevant in a legal matter. If a deletion request were made while a legal hold was in effect, the documents and data under legal hold must be retained. Only after a legal hold is released should the pending deletion request be considered and executed if appropriate. To this extent, CCPA compliance processes need to be synchronized both with legal hold processes and the release of these holds.

B. Data Deidentification

In some instances, it may not be practical to delete personal information, or companies want to continue to utilize collected personal information for business intelligence purposes without needing this information to directly relate to specific consumers. This is especially true for personal information stored in relational databases, where deletion of data can break references to other data, compromising "referential integrity." In these cases, organizations may employ a variety of data deidentification techniques (see Figure 1.)

Data Deidentification

Aggregated Plaintext	Data Pseudonymization	Data Deidentification	Data Anonymization
Name: Mark Diamond **City: Los Altos, CA** **Auto: Volvo** **Hobby: Golf**	138357498 Los Altos, CA Auto: Volvo Hobby: Golf	Name: Xygx Ksoe2oc City: Noq Bpoems, QW Auto: Uswiy Hobby: Ipvl	Name: XXXXX City: XXXXX Auto: XXXXX Hobby: XXXXX

Aggregated – Information and data collected from multiple sources is combined. CCPA specifically defines this as information that relates to a group or category of consumers, from which individual consumer identities have been removed

Direct Identifiers – Data that uniquely identifies a person without additional information, e.g. a name.

Indirect Identifiers – Data that identifies may or may not uniquely identify a person but needs additional information to identify an individual.

Pseudonymization – Eliminating or replacing direct data identifiers, but indirect

Figure 2. In many cases it may be easier and more beneficial to de-identify data instead of deleting it.

C. Common Roadblocks to Successful Program Execution and Compliance

As part of good program planning, it is useful to identify potential roadblocks that could either halt or delay program completion. When it comes to implementing a privacy program, some common roadblocks could include:

"Policy-itis": A common roadblock to privacy programs – focusing on the development of a privacy policy to the exclusion of policy execution. This risk is particularly acute for CCPA as the law is expected to be updated by the Attorney General prior to its enforcement. Compliance is achieved not just through having a policy, but by faithfully implementing it as well.

Siloed approaches: Effective privacy takes a team, including privacy, legal, compliance, IT and business units. Any single group that takes on this task by itself is likely to falter.

Manual or unworkable processes: Manually compiling personal information access and deletion requests is likely to become overwhelming quickly. Unlike GDPR which, for many U.S. companies, was low value and manual processes plus policy changes have been

sufficient. For CCPA, organizations need to consider making this an automated, streamlined approach.

Starting too late: The CCPA provides a relatively short time frame before enforcement begins on January 1, 2020. Organizations that start creating their programs too late run the risk of not completing them on time.

All of these pitfalls can be avoided with a smart project start. A well-thought out CCPA Project Plan that engages the right stakeholders and contains a reasonable timeframe goes a long way towards a successful project.

V. Operationalizing CCPA

As with any complex task, instead of executing a series of ad-hoc, one-off steps it is always better to create an end-to-end plan. This is particularly true for privacy as these projects can involve a multitude of policies, processes, technology and training often involving multiple groups addressing different types of media. Especially when facing a tight timeframe, defining upfront what you want to do when, and how much makes these tasks easier. Particularly for a CCPA compliance program, "look before you leap."

The Figure 3 below illustrates typical components of a CCPA Project Plan. While each company's CCPA approach may vary, nearly all will include some or all of these project elements.

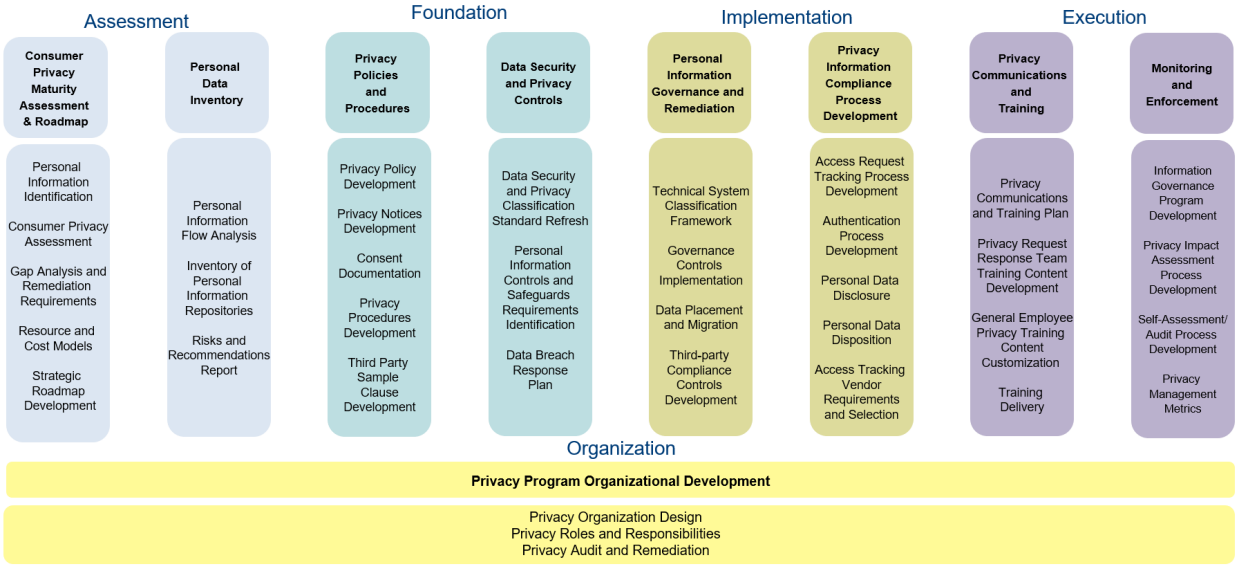

Figure 3. Best practices CCPA and U.S. State Privacy Roadmap. Policy development is a small part of overall compliance.

A. Creating an Assessment and Roadmap

Organizations should start with an assessment process that in turn feeds into a program

roadmap. Through a high-level interview process the assessment discovers the types of personal data an organization collects, how it is managed, how it is protected and the current processes in place to communicate with customers and regulators on privacy compliance, including the reporting of data breaches. The information learned during the assessment can then be used to identify gaps between current state and the required state for CCPA compliance, and a roadmap can be developed to address those gaps. The roadmap should also contain resources required for each step, any new technology that may be required as well as cost information for each step plus include a timeline that achieves compliance well before the deadline. Equally important, the assessment and roadmap process engages a number of key stakeholders required for a successful program early in the project.

Discover	• What personal information do you collect/store? • Where is personal information located? • How do you classify personal information? • For what purposes do you collect/use personal information?
Manage	• What are your current data privacy policies? • How is personal information managed, and for how long? • What are the consumer's rights to their personal information? • How do you manage data privacy risk?
Protect	• How is personal information protected in the organization? • Is privacy considered in technology development? • How does the organization protect against a data breach? • Are employees trained on privacy responsibilities?
Report	• How do you respond to a data breach? • How do you monitor third-party flow of personal information? • What records display compliance with privacy policies? • How do you communicate with customers about privacy?

Table 2. Organizations should conduct an initial assessment to target their required maturity as well as identify gaps.

B. Developing a Personal Information Inventory

Critical to compliance with CCPA is tracking both how personal information is collected and flows through an organization, as well as where it is stored. Companies should create a personal information inventory. This inventory should list all relevant processes that involve the collection and use of personal data. The inventory also should address those who have access to the personal data, to whom the data is transferred outside the company (if anyone), and how long the personal data is stored in each location.

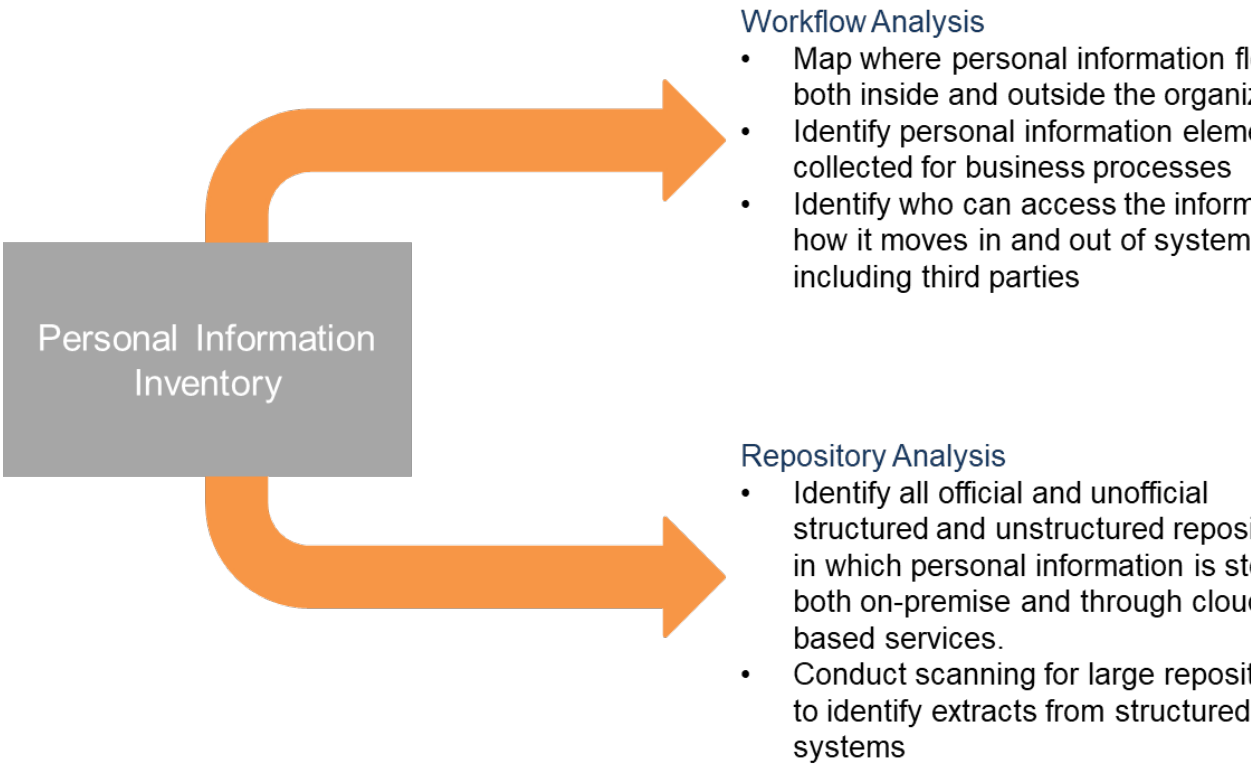

Figure 4. A personal information inventory should take a two-pronged approach reviewing both workflows and repositories.

This personal information inventory process can identify the patterns that may be unique to your business, which can help you identify privacy data. Some of it can be identified through technology that searches for known patterns such as social security numbers, addresses, driver's licenses, "regular expressions" (i.e., XXX-XX-XXXX for U.S. social security numbers where X is a number), etc. Other types of privacy data such as inference data may require more advanced search techniques.

Once the personal data and its respective data flows have been identified, the personal information inventory should also seek to identify all the places personal data is actually stored. This may include databases, email, and file shares, among other locations. Often, employees will take an extract of a database, for example, and store that as a file on their desktop. The inventory should include all designated locations of this data, such as the original source as well as any inadvertent copies.

C. Defining Privacy Policies and Procedures

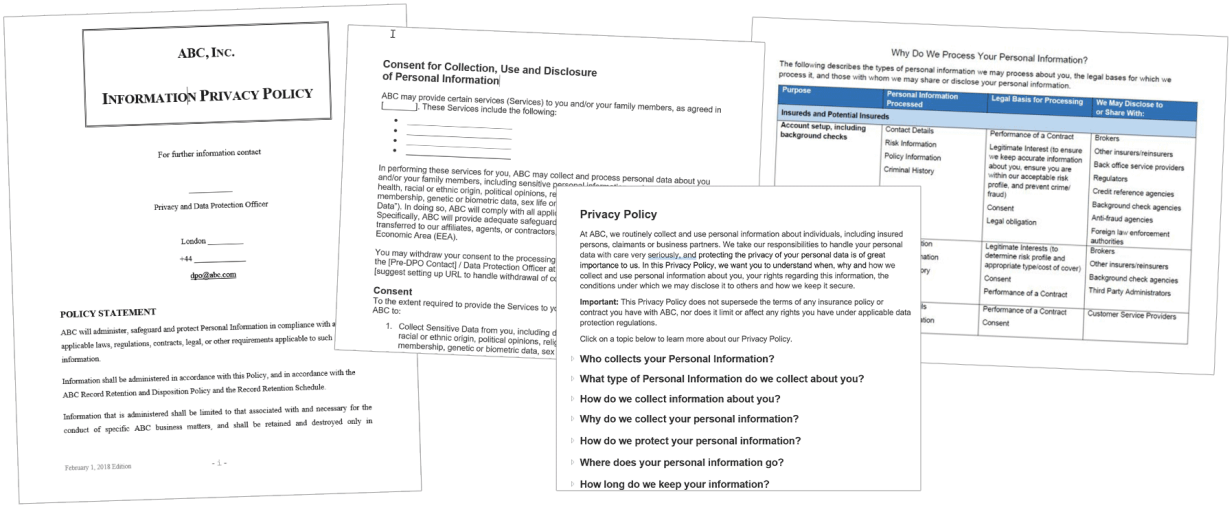

Figure 5. The Act requires that companies make certain at the time the personal data is collected

The Act will require many organizations to update or create additional privacy policies as well as implement a series of privacy procedures, to include the privacy rights recognized in the new law. The types of documents that may need to be created or updated include:

- Updated Privacy Policies
- Privacy Notices
- Consent Notices
- Opt-out (and opt-in) policies, notices and procedures
- Disclosure and Deletion Procedures
- Data Security Classification Standards
- Privacy Impact Assessment
- Data Breach / Incident Response Plans

In some cases, these may be updates of existing privacy policies, and in other cases it may involve the development of entire new processes, such as a procedure to respond to consumer information access requests. The Act also calls for specific processes, such as placing a prominent "Opt Out" button on the website.

The Act requires the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.

Figure 6. CCPA requires at least two methods for California residents to submit opt-out requests.

Consumers have the right to request information collected on them.

Companies will also need to develop new processes for responding to consumer information access requests. CCPA requires two methods for submitting access requests – a typically toll-free number and website link. However, companies should anticipate that consumers are likely to submit these requests through many different channels and develop procedures for funneling these requests into the appropriate workflow.

Upon receipt the business must respond to the requestor within 45 days of the date of request. It will also be important to be able to authenticate the identity of the consumer making the request, to ensure it is not being made by someone who is interested in identity theft. For example, such verification may include steps such as implementing a verification process to ensure the requestor is indeed the person whom he claims he is.

Companies will want to automate and streamline the authentication and data collection process as much as possible, lest this becomes an overwhelming and unmanageable process.

D. Creating Data Security and Privacy Controls

In addition to disclosing what information is collected about consumers, whether and to whom their information is disclosed, and to access information collected, the Act has strong penalties for organizations in the event of a data breach. While there are existing breach laws with penalties on the books, with the enforcement of CCPA and its potential penalties many businesses want to review and strengthen their management and security of personal information. The exact protection measures will depend on the type, medium and location of the personal information. Organizations need to implement data security and privacy controls. Some typical controls include:

- Preventing or controlling movement between repositories
- Tightening access controls
- Securing and encrypting data at rest
- Preventing data from being shared, printed or stored elsewhere
- Scanning repositories for inappropriate data

This step highlights the importance of the previous step: creating a comprehensive personal information inventory that maps out all locations where data is stored is critical as breaches can affect not only repositories of record, but also secondary copies of data in less protected areas.

E. Personal Information Governance and Remediation

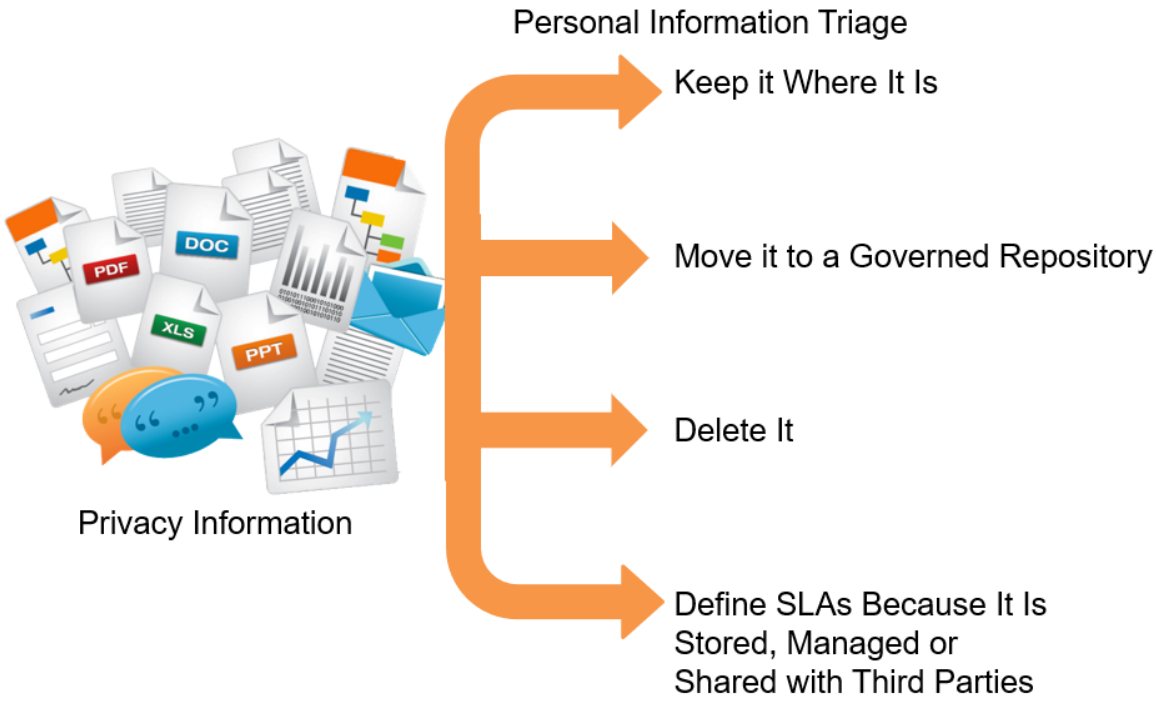

Figure 7. Once personal information is inventoried, companies need to implement information governance or remediation.

It is likely that the Personal Information Inventory will reveal that personal information resides throughout the enterprise, including in databases, but also in unstructured media including files on desktops and file shares. Companies need to engage in a triage process for this personal information:

- Does the personal information already reside in a secured and well-governed repository? Can this information be easily accessed, produced and deleted or de-identified? If the personal information will continue to reside in this repository, have the appropriate data security controls been applied?
- Should the personal information be moved to a more secure and better governed repository?
- Is the personal information either expired and of low or no business value, or is it a copy of information that resides elsewhere, in which case it should be deleted?

- Does the personal information reside in a cloud-based system or other third-party managed repository for which you are the custodian? Does this repository have the appropriate data security controls and Information Governance capabilities?
- Has the personal information been sold or shared with a third party, and you are no longer the custodian of this shared information? Have the information steward requirements been communicated and Service Level Agreements (SLAs) been developed?

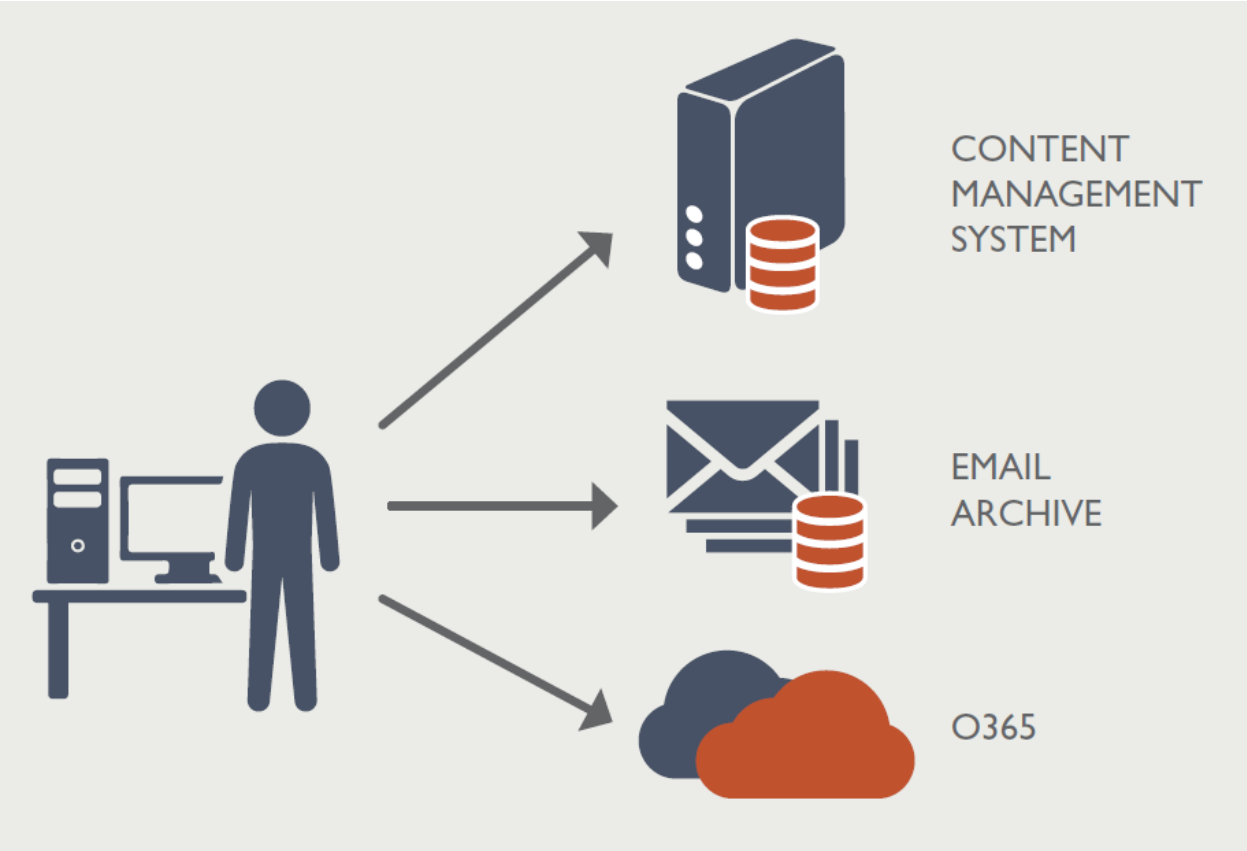

Figure 8. Information stored in cloud-based repositories requires the same protection as any other information or document. These repositories should also have an appropriate file plan and security schema.

Databases containing privacy information should be identified and their access controls tested. For unstructured data, desktops and file shares may not provide adequate protection. This information needs to be moved to more secure repositories such as an enterprise content management or document management systems. This includes developing taxonomies and/or file plans that contain a privacy/security schema, in order to properly organize and classify the information in these repositories.

It is possible that the personal information inventory will identify different locations that contain privacy information. Businesses should not expect to do everything at once. To start, companies should prioritize data stores with large amounts of privacy information. When choosing the appropriate repository to store this information, organizations should look at repositories with built-in, risk-based controls. We recommend that implementation

projects be piloted against smaller data sets and then be rolled out to the larger enterprise.

Do not forget about paper records either onsite or in offsite storage facilities. These documents can and do contain significant privacy information. CCPA disclosure and deletion requirements include personal information of these hardcopy documents.

F. Privacy Information Compliance Process Development

CCPA requires a series of processes to support consumer access, production and deletion requests. These include:

- **Authentication Processes:** To authenticate identifiers of requestors.
- **Search Processes:** As part of compliance, many organizations may need to increase their automated digital search and technical security capabilities. This will help them avoid time-consuming, ad-hoc processes, and reduce the risk of breaches.
- **Production Processes:** To securely produce and deliver requested privacy information. For example, companies will need to produce both databases information for requestors.
- **Disclosure and Deletion Processes:** Defensible and compliant processes for managing disclosure and deletion requests. These processes need to coordinate with records retention and legal hold requirements.
- **Tracking Processes:** To track and manage all inbound requests and requirements.

It should be noted that the more effective the data and information governance capabilities discussed in the previous step, the more efficient and cost-effective deploying these processes will be. Likewise, poor data and information governance may make these processes rather burdensome.

G. Conducting Privacy Communications and Training

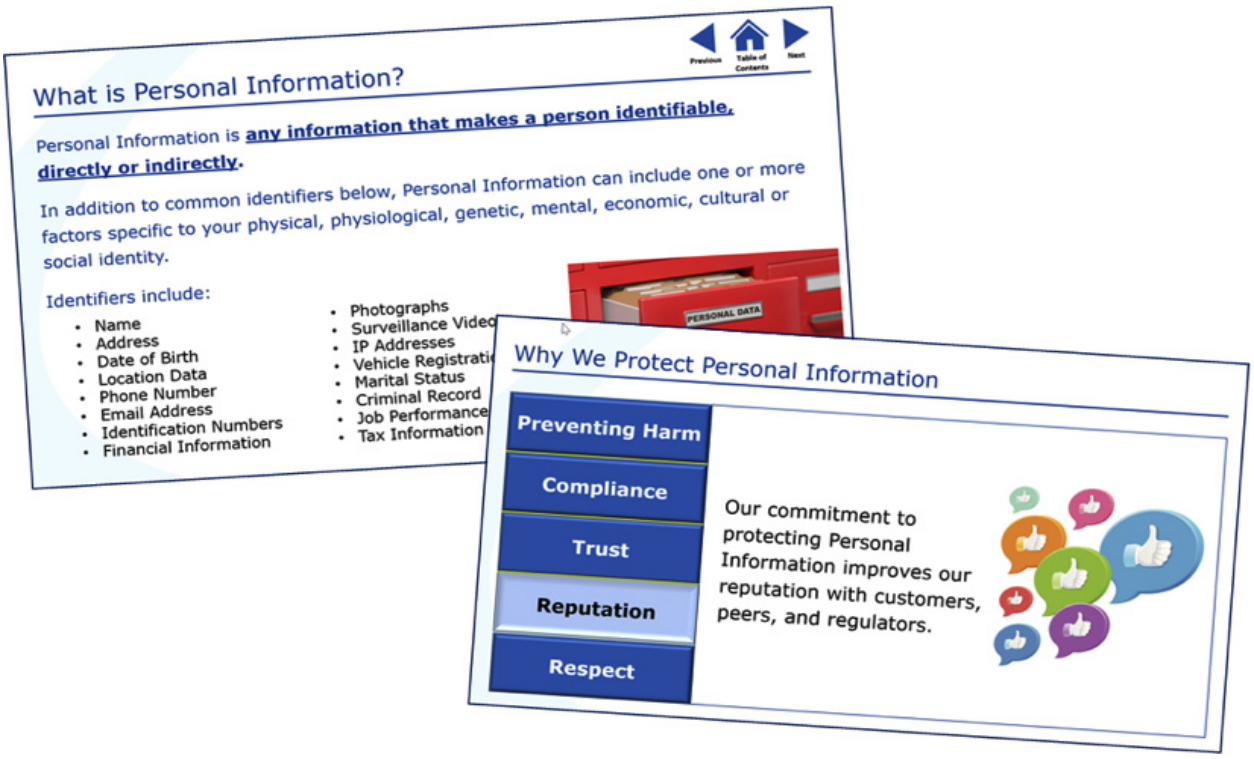

Figure 9. Privacy training should include both targeted training for those with specific privacy-related responsibilities as well as general training for all employees.

Once a company has its roadmap, policies and processes, tools, and technology in place, a critical task remains: employee behavior change management. Change management is a formal discipline that combines messaging, communication, training and auditing to get employees to follow a new process. Often, as part of a revamped privacy program, organizations will implement change management to ensure appropriate handling of privacy information. When organizations effectively apply change management, even stodgy, disinterested and uncooperative business groups will get on board.

A business's CCPA program should train staff with specific responsibilities for handling personal information, as well as employees who are going to be responding to consumer information access requests. Additionally, it is a good idea that *all* employees receive some general privacy training that addresses, for example, why privacy is important and the company's overall responsibilities for handling personal information.

H. Legacy Personal Information Disposition

Holding on to privacy information that is obsolete, expired and not needed for legal, regulatory or business use increases the risk of CCPA non-compliance, and increases exposure should a data breach occur. Likewise, implementing personal data deletion requests in environments with large amounts of legacy data is both difficult and expensive. To that end, privacy and other Information Governance programs should implement

ongoing disposition of old, unneeded documents and data. This legacy deletion should encompass older structured data in databases, unstructured data including files on file shares, desktops and within SharePoint and other content management systems, legacy semi-structured data such as email, as well as inactive data held in backup tapes and onsite and offsite paper records.

I. Developing a Privacy Organization

A privacy project is not a check-the-box operation – it is a living program with ongoing responsibilities throughout the organization. Even when organizing the implementation project, there are questions of ownership, including:

- Identifying the right coordinators
- Identifying the right stakeholders
- Organizing a steering committee
- Identifying who should be part of the steering committee, including executive-level personnel

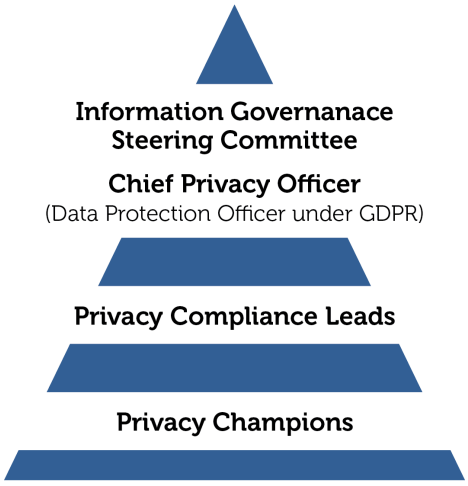

Figure 10. Don't approach CCPA as an army of one. Work with other stakeholders.

The creation or update of a matrix structure of the steering committee will help to drive ongoing privacy activities and maintain organizational compliance, in addition to other information governance responsibilities. The committee should bring together diverse professional viewpoints from various key business functions from across the organization.

It should also:

- Ensure that there is good communication of requisite concepts;
- Promote best practices for the management and control of the organization's sensitive information;
- Establish cross-functional ownership of the privacy program,
- Articulate goals and business benefits; and
- Define ongoing roles and responsibilities for privacy managers, compliance leads, and champions.

VI. Determining Minimal, Required and Best-Practice Activities

As discussed above, CCPA explicitly requires certain activities to be completed in building out a compliant privacy program. Other activities are required to ensure compliance; others, although not directly required, are part of a best-practices approach to reduce program execution costs and risks. The graphic below details minimum program activities required by CCPA, additional baseline activities needed for compliance, and best-practice activities.

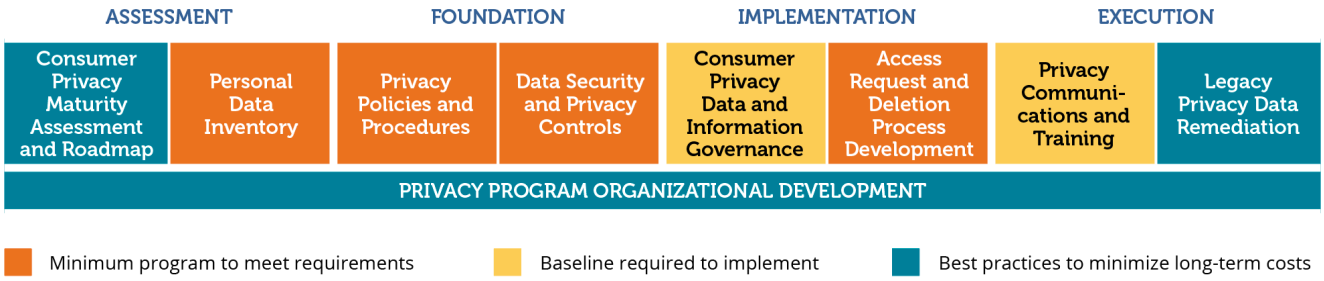

Figure 8. While CCPA only explicitly requires a few program components companies are advised to consider implementing additional program pieces to meet consumer access requests in an efficient manner.

In developing a program, companies will want to pick which of these elements they want to execute. The challenge is balancing speed of execution and program cost vs. ongoing program efficiency. Executing only the orange-colored projects, for example, could make downstream program execution difficult and expensive. Companies are encouraged to think through the entire program, from development to execution. Do they balance investment with risk? Also consider the longer-term costs of execution. Be smart, be efficient and be compliant.

Companies facing these privacy rules need to address some difficult questions: How do we implement a single enterprise-wide program that still meets a patchwork of individual states' requirements? How do we implement a program when many of the requirements are still being defined? If US federal legislation is enacted, will today's efforts be enough? What is defensible and constitutes "good enough"? Are we really ready?

Instead of focusing on meeting each individual US state's requirements as they arise, a smarter approach is to develop general privacy information handling capabilities, and then making minor program adaptations as necessary. There are enough similarities across the various privacy regimes that companies can build some basic privacy capabilities including classification, secure management, production and disposition. These base capabilities – in what we call Privacy Information Agility – will meet most or nearly all of the needs across states. This approach will be far easier in the long run than developing a program hard-wired for a single state, only to have to update the program continuously as new states adopt privacy legislation.

VII. Assessing Your Privacy Maturity

Privacy programs, unfortunately, often face a high failure rate. According to a recent industry survey, most Chief Privacy Officers admitted that their programs were not fully ready to meet GDPR requirements nearly a full year after they went into effect. Privacy programs are also often scrutinized by regulators and courts. Sometimes, in-house counsel believes solely creating a detailed privacy policy will satisfy regulatory requirements. Regulators and courts want to not only see a company's policy, but also that the company is able to demonstrate compliance with the policy. Organizations that can demonstrate compliance with their privacy policies will be more defensible. For these reasons, creating a credible, compliant, and defensible privacy program requires some level of objective demonstration that policies and processes are being followed.

Note: The privacy program maturities summarized in this Guide are detailed in the "ACC U.S. States Privacy Capability Maturity Model" available on the ACC website or from the author.

A. Targeting the Right Privacy Maturity for Your Organization

Different levels of program maturity are required for different companies. Companies vary on the number of consumers whose privacy information they hold, the quantity and breadth of this information, how widely it is shared as well as how this information is stored and managed. A few organizations do indeed need a highly advanced and rather expensive "sports car" level of program maturity; however, most organizations would be better off with a less sophisticated but still fully capable and more cost effective "regular family car" or even "golf cart" level program. It is better to have a well-executed, albeit simpler, approach than a more complex, difficult, and expensive target that needs constant supervision and improvement as opposed to an operationalized program. Savvy privacy professionals know that targeting the right level of maturity is key.

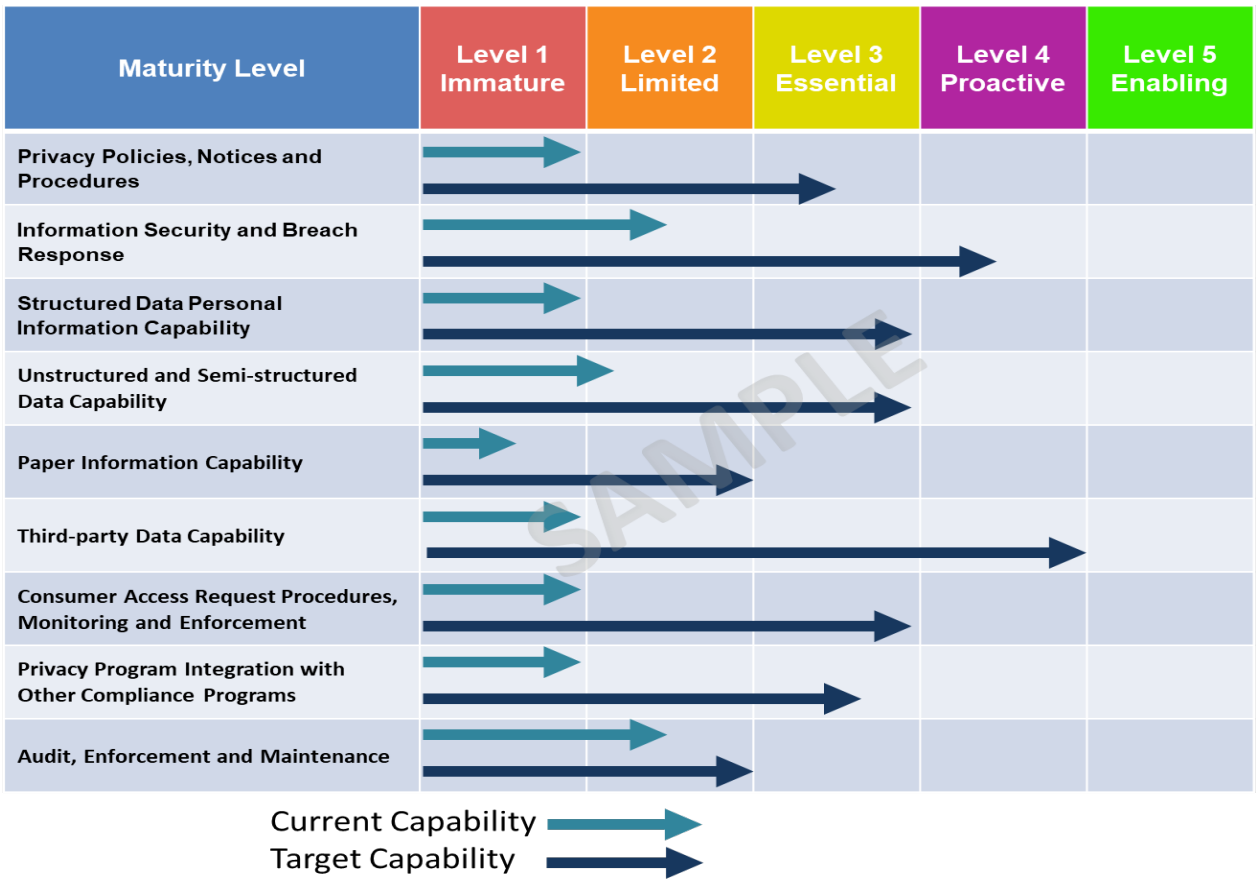

Figure 9. Sample maturity capability model of current capabilities vs. target capabilities. Most organizations do not need to target the highest level of maturity for any given area.

Companies should consciously target a specific maturity level and build their programs to meet that level. Figure 12 displays current vs. target privacy program capabilities. Companies can fail in their privacy efforts by overreaching and trying to create too sophisticated program elements, or by underestimating the needed capability.

Note: The privacy program maturities summarized in this Guide are detailed in the "ACC U.S. States Privacy Capability Maturity Model" available on the ACC website or from the author.

B. Privacy Policies, Notices and Procedures

The new rules will require organizations to either create a privacy policy or update their existing policy. Likewise, they will need to update and add notices, as well as create new processes 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

Table 3. Policy and Notice Maturity

It should be noted that there is an element of risk in updating these policies, in that the policy itself becomes the main program focus and not its execution. Many aspects of the California law as well as other privacy legislation are somewhat non-prescriptive, and the risk is companies will put significant effort creating extremely detailed policies at the expense of execution. The main thrust of the program becomes simply having a policy. In many cases it is wise for a company to create a good policy, and then move on to ensuring they are classifying, securing, managing, and building the capability to access, produce and delete privacy information across electronic and paper media.

C. Privacy Organization and Awareness

A privacy project is not a check-the-box operation – it is a living program with ongoing responsibilities throughout the organization. Even when organizing the implementation project, there are questions of ownership, including identifying and engaging stakeholders, organizing a steering committee and building executive-level support. Likewise, training is critical for building organizational awareness.

Level 1 – Immature	Level 2 – Limited	Level 3 – Essential	Level 4 – Proactive	Level 5 – Advanced
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 ad-hoc 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 on 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

Table 4. Privacy Organization and Awareness Maturity

Execution of a privacy program requires efforts from many different groups and building a cross-functional approach early in the process is important.

D. Information Security and Breach Response

Organizations need to implement data security and privacy controls. The exact protection measures will depend on the type, medium and location of the personal information.

Level 1 – Immature	Level 2 – Limited	Level 3 – Essential	Level 4 – Proactive	Level 5 – Advanced
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

Table 5. Information Security and Breach Response Maturity

Most organizations have some level of information security capabilities already in place. It is important to make sure these capabilities address and are consistently applied to privacy information.

E. Structured Data Personal Information Capability

Significant stores of privacy information live in applications which store their information in structured databases. These databases are part of customer applications. Privacy information often flows from one system to another, sometimes creating many copies of the same data. Companies need to develop capabilities for managing this structured privacy data.

Level 1 – Immature	Level 2 – Limited	Level 3 – Essential	Level 4 – Proactive	Level 5 – Advanced
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

Table 6. Structured Data Personal Information Capability

Privacy requires the capability of not only identifying and securing privacy information in these structured databases, but also producing this information in response to a consumer access request, as well as deleting or "de-identifying" it through pseudonymization procedures.

F. Unstructured and Semi-Structured Data Capability

While privacy information is typically associated with information in databases, large amounts of privacy information exist in files, emails and other types of unstructured and semi-structured information. Many privacy programs do not address this unstructured and semi-structured information, creating real non-compliance issues and risks. Under European, California and other laws this type of information is in scope and can be particularly challenging to manage.

Level 1 – Immature	Level 2 – Limited	Level 3 – Essential	Level 4 – Proactive	Level 5 – Advanced
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

Table 7. Unstructured and Semi-structured Data Capability

G. Paper Information Capability

Paper documents tend to accumulate in both onsite and offsite storage facilities, some of which contain privacy information. The new and emerging privacy laws do not exclude paper, and as such identifying and producing this paper-based information can be particularly burdensome. Hence programs must have the capability of addressing paper.

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 secure destroyed; physical security subject to regular security 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

Table 8. Paper Information Capability

Often paper-based privacy information is either scanned into an electronic format, or even better, -destroyed as soon as its retention period is reached.

H. Third-Party Data Capability

Companies must have the capability to address the privacy information they collect that is either sold or shared with third parties, or likewise they receive themselves. This includes developing the appropriate service level agreements (SLAs) as well as ensuring that these third parties have the capability of complying with the privacy requirements. Many companies are surprised to find out the extent this information is shared.

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 (service level agreements) 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

Table 9. A.Third-party Data Capability

Well-designed third-party capabilities set clear expectations over who is responsible for what. This is always easier to address proactively.

I. Consumer Access Request Procedures, Monitoring and Enforcement

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.

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 plus third-party compliance

Table 10.Consumer Access Request Procedures, Monitoring and Enforcement

J. Privacy Program Integration with Other Compliance Programs and Processes

One of the problems that has emerged from current privacy requirements is the need for these programs to coordinate with other compliance regimes, including records management and eDiscovery and legal holds. CCPA, for example, suspends deletion requests for personal information under legal hold. But these two groups of processes need to be coordinated.

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 Retention 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

Table 11. Privacy Program Integration with Other Compliance Programs and Processes Maturity

K. Audit, Enforcement and Maintenance

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, programs should not be thought of as "one and done," but rather have audit, enforcement and maintenance processes built within them.

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, 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 acknowledgement 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, complaints addressed in timely manner; management monitors noncompliance; risks identified, and formal remediation plans developed on annual basis	+ 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

Table 12. Audit, Enforcement and Maintenance Maturity

VIII. Key Takeaway: Getting Started, Say What You Do, Do What You Say, and Document

New and emerging US Privacy requirements can be both scary and overwhelming. With significant risks and costs for non-compliance, it can be challenging to assess how much maturity is needed for what parts of a program for any given company. Companies start looking for the *perfect* policy, the *perfect* process and the *perfect* tools. We are not ready to start, they tell themselves, because we're not quite there yet. In the meantime, documents and data accumulate, requirements become stricter, and risks increase. *Perfect* becomes the

enemy of "good."

In-house counsel should ask themselves: how much is enough? Privacy is an inherently imperfect process. Fortunately, the courts and regulators do not expect perfection. Rather, they expect reasonable, good faith efforts. 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. No one expects it to be perfect. Start with good and just keep moving forward.

IX. About the Author

Mark Diamond is an industry thought leader in information governance, encompassing records and information management, litigation readiness, control of privacy and other sensitive information, defensible disposition, and employee collaboration and productivity. Mark is a frequent industry speaker, presenting at numerous Legal and IT industry conferences. Additionally, Mark delivers more than 50 onsite Information Governance seminars to internal corporate audiences each year.

Mark is the founder, President & CEO of Contoural, Inc. Previously, Mark was co-founder of Veritas' (OpenVision) Professional Services group, founder and General Manager, Worldwide Professional Services for Legato Systems, Vice President of Worldwide Professional Services at RightWorks, and he has worked as a management consultant. He also served as Chair of the Storage Networking Industry Association customer advisory board on data security. He sits on the board of advisors for high technology companies.

He has a Bachelor's degree in Computer Science from the University of California San Diego. Mark is former President of the UC San Diego Alumni Association, and served as a Trustee of the university's foundation.

Mark welcomes any questions and comments regarding this Guide. He can be reached at mdiamond@contoural.com and for more information, on Contoural's site at www.contoural.com.

X. About Contoural

Contoural is the largest independent provider of privacy, Information Governance consulting services focused on CCPA, GDPR, Records and Information Management, litigation and regulatory inquiry readiness and control of privacy and other sensitive information. Contoural does not sell any products or take referral fees, store any documents or provide any lawsuit-specific "reactive" e-discovery services, serving as a trusted advisor to its clients providing unbiased advice. Contoural has more than 30% of the Fortune 500 as clients, across all industries, as well as federal agencies and local governments. Contoural offers a range of privacy and Information Governance services:

- Data Privacy Maturity Assessment
- Data Privacy Organizational Structure
- Personal Data Inventory
- Data Mapping
- Privacy Policies and Procedures
- Privacy and Security Enhancements
- Records Retention Schedules
- Technology Requirements for Privacy and Security Controls
- Taxonomy & File Plan
- Implement Privacy and Security Controls
- Privacy Communications and Training
- Legacy Data Remediation

XI. Additional Resources

A. ACC Sample Forms, Policies, and Contracts

"ACC U.S. States Privacy Capability Maturity Model," ACC Information Governance Network homepage

B. ACC Guides

"Information Governance Primer for In-house Counsel," (2016), *available at* https://www.acc.com/resource-library/information-governance-primer-house-counsel

"Creating a Modern, Compliant, and Easier-to-Execute Records Retention Schedule," (2017), *available at* https://www.acc.com/resource-library/creating-modern-compliant-and-easier-execute-records-retention-schedules

"Executing Your Records Retention Policy and Schedule," (2018), *available at* https://www.acc.com/resource-library/executing-your-records-retention-policy-and-schedule

C. ACC Docket Articles

"Everybody's Job, Nobody's Job: The Best Way to Create an Information Governance Program Without Going Crazy," Patrick Chavez and Mark Diamond, *ACC Docket* (April 2019) *available at* https://www.accdocket.com/articles/resource.cfm?show=1500001

"Privacy Trends: The California Privacy Act is a Harbinger of New Regulations," Tim Sesler and Mark Diamond, *ACC Docket* (March 2019) *available at* https://www.acc.com/sites/default/files/resources/20190314/1497947_1.pdf

"Upgrading Your Traditional, Paper-centric Records Program to Be More Modern, Compliant, and Useful," Andrea Meyer and Mark Diamond, *ACC Docket* (December 2018) *available at* https://www.acc.com/resource-library/upgrading-your-traditional-paper-centric-records-program-be-more-modern-compliant

"Building a Business Case for Information Governance," Annie Drew and Mark Diamond, *ACC Docket* 32, no. 8 (Oct. 2014): 26-40, *available at* https://www.accdocket.com/articles/resource.cfm?show=1377595

"Privacy Trends: The California Privacy Act is a Harbinger of New Regulations," ACC Docket March 2019, *available at* https://www.accdocket.com/articles/resource.cfm?show=1497947

D. ACC Legal Quick Hits

"Personal Data Inventory and Data Mapping Strategies," *Legal Quick Hit,* (2019), *available at* https://acc.inreachce.com/Details/Information/69ebaee4-c3bd-4447-81ff-d1e092461af1

"Creating a California Consumer Privacy Act Action Plan," *Legal Quick Hit,* (2018), *available at* https://acc.inreachce.com/Details/Information/754e132b-57c5-4b62-a2f5-1863747dcc82

"Three Ways to Stop Bleeding Money on Paper Storage Costs," *Legal Quick Hit,* (2018), *available at* https://acc.inreachce.com/Details/Information/46a5d942-6a3e-4019-91d7-b39e726834f1

"Preventing Employees From Hoarding Documents," *Legal Quick Hit,* (2018), *available at* https://acc.inreachce.com/Details/Information/FAA4D598-2313-4693-B408-2E5C09CB94C3

E. ACC – Webcasts

"IG 101: Information Governance for In-House Counsel Parts 1 and 2," *Webcast* (2019), *available at* https://acc.inreachce.com/Details/Information/3a9b3a20-d3dd-42fd-bb70-863dd70542d7

"Legal Operations Maturity Model Series - Information Governance & Records Management," *Webcast* (2019), *available at* https://acc.inreachce.com/Details/Information/a0edf21b-3014-4676-b70b-cd5a1398637b

"First Year Student Orientation: Launching or Updating Your Records Management Program," *Webcast*, (2017), *available at* http://learningcenter.inreachce.com/viewer_v9/?eid=cd1c2a44-53fc-41b0-be84-979208d88970&oid=acc&uid=0

"Information Governance: Getting a Program Started," *Webcast,* (2017), *available at* https://acc.inreachce.com/Details/Information/88a31407-7ff2-42df-8d59-6da965f96de1

F. ACC – Information Governance Network Resources

"California Consumer Privacy Act Project Plan," *Quick Overview*, (2019), *available at* https://www.acc.com/chapters-networks/networks/information-governance-network

"California Consumer Privacy Act (CCPA) - Similarities and Differences to European GDPR at a Glance," *Sample Forms, Policies, & Contracts*, (2019), *available at*

https://www.acc.com/resource-library/california-consumer-privacy-act-ccpa-similarities-and-differences-european-gdpr

"Information Governance – Glossary of Terms," *Sample Forms, Policies, & Contracts*, (2019), *available at* https://www.acc.com/resource-library/information-governance-glossary-terms

"Employee Behavior Change Management Programs for Information Governance," *Quick Overview*, (2017), *available at* https://www.acc.com/resource-library/employee-behavior-change-management-programs-information-governance

"Creating a Data Classification Standard," *Sample Forms, Policies, & Contracts*, (2017), *available at* https://www.acc.com/resource-library/creating-data-classification-standard

"Data Map Design Strategies," *Sample Forms, Policies, & Contracts*, (2017), *available at* https://www.acc.com/resource-library/data-map-design-strategies

"Data Map Population Strategies," *Sample Forms, Policies, & Contracts,* (2017), *available at* https://www.acc.com/resource-library/data-map-population-strategies

"Data Map Use Cases," *Sample Forms, Policies, & Contracts,* (2017), *available at* https://www.acc.com/resource-library/data-map-use-cases

"Creating Discovery Response Processes," *Article*, (2017), *available at* https://www.acc.com/resource-library/creating-discovery-response-processes

"Defining Effective Legal Hold Processes," *Article,* (2017), *available at* https://www.acc.com/resource-library/defining-effective-legal-hold-processes

G. Contoural Whitepapers

"Creating a California Consumer Privacy Act Action Plan," *White Paper,* (2019), *available at* www.contoural.com

"Reducing Your Offsite Storage Risk and Cost," *White Paper,* (2019), *available at* www.contoural.com

"Defensible Disposition: Real-world Strategies for Actually Pushing the Delete Button" *White Paper,* (2014), *available at* http://www.contoural.com/whitepaper_summary.php?id=31

"Metrics Based Information Governance," *White Paper,* (2013), *available at* http://www.contoural.com/whitepaper_summary.php?id=28

"Stop Hoarding Electronic Documents," *White Paper,* (2012), *available at* http://www.contoural.com/whitepaper_summary.php?id=32

"Email Classification Strategies That Work," *White Paper,* (2012), *available at* http://www.contoural.com/whitepaper_summary.php?id=29

"Seven Essential Storage Strategies," *White Paper*, (2015), *available at* http://www.contoural.com/whitepaper_summary.php?id=1