Quick Overview: Operationalizing the California Consumer Privacy Act (CCPA)

Mark Diamond, CEO & Founder, Contoural, Inc.

On June 28, 2018 the California Legislature passed the California Consumer Privacy Act (“CCPA” or the “Act”). This sweeping legislation creates significant new requirements for identifying, managing, securing, tracking, producing and deleting consumer privacy information. This Quick Overview presents key steps toward complying with CCPA. For further developments, please check out the ACC Guide on Operationalizing the California Consumer Privacy Act (2019).

As with any complex task, 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. When facing a tight timeframe, defining upfront what you want to do when, and how much makes these tasks easier.

The Figure 1 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.
1. Creating an Assessment and Roadmap

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, cost information for each step, and 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.

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

Table 1. Organizations should conduct an initial assessment to target their required maturity and identify gaps.

2. Developing a Personal Information Inventory

Track 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 2. A personal information inventory should take a two-pronged approach reviewing both workflows and repositories.

3. Defining Privacy Policies and Procedures

Figure 3. 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 documents may be updates of existing privacy policies. In other cases, they 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.

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 and verify the identity of the consumer making the request, to ensure it is not being made by someone who is interested in identity theft.
4. Creating Data Security and Privacy Controls

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; and
- Scanning repositories for inappropriate data

Breaches can affect not only repositories of record, but also secondary copies of data in less protected areas. It is thus critical to create a comprehensive personal information inventory that maps out all locations where data is stored.

5. Personal Information Governance and Remediation

Figure 5. 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 6. 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. Starting an implementation project on smaller data sets will help your group perfect the process before rolling it 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.

6. 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.

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.
7. Conducting Privacy Communications and Training

Figure 7. 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 reluctant business groups will get on board.

8. 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. 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.
9. Developing a Privacy Organization

A privacy project 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; and
- Identifying who should be part of the steering committee, including executive-level personnel.

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.

Conclusion

Operationalizing CCPA requires a combination of effective policies, applying technology and developing robust processes. Getting a good start is both important and often difficult. It is easy to become overwhelmed. As with tackling any complex task, break it into pieces. Create a plan and a schedule. Track your progress to the plan and make adjustments as necessary. Most important, keep moving forward. Although at times it may not feel like it, you will get there.

Additional Resources

ACC Guides
- Operationalizing the California Consumer Privacy Act (2019)
- Creating a Modern, Compliant and Easier-to-execute Records Retention Schedule (2018)
- Executing Your Records Management Program (2018)

Maturity Models
- ACC US States’ Privacy Maturity Model (2019)
- ACC Records Management Program Maturity Model (2019)

Other Articles
- California Consumer Privacy Act (CCPA) - Similarities and Differences to European GDPR at a Glance (2018)

The information in any resource collected in this virtual library should not be construed as legal advice or legal opinion on specific facts and should not be considered representative of the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical advice and references for the busy in-house practitioner and other readers.