




# Operational Privacy

For the California Consumer Privacy Act of 2018

January 2020

*by Barry Weber*  
*Privacy Practice Leader*  
*Assured SPC*



The California Consumer Privacy Act of 2018 (CCPA) has generated significant discussion, clarification and legal opinions in business and legal communities, across the U.S. and internationally. But what has been largely missing from that discussion has been useful information about the specific activities that businesses need to institute and manage their responsibilities under the law. This guide will, at a high level, layout *how* businesses must respond to the law – what processes need to be created, what current business activities may need to change and who in the business may need to take on new accountabilities and responsibilities.

## Overview - California Consumer Privacy Act of 2018

The new California privacy act has been discussed and clarified since 2018. But this activity is not complete. In the Fall of 2019, some amendments were signed into law and the State Attorney General’s (AG) office released a draft of regulations to clarify details of the law that will be used in enforcement actions. The AG will finalize regulations in 2020, but it is required to begin enforcing the law once those are completed or July 1, 2020, whichever comes first.

There are restrictions to CA consumer rights regarding their personal information (PI). *These restrictions won’t be highlighted here for the sake of brevity.*

At a high level, the law provides California consumers rights to their personal information (PI) that include:

1. A right of protection – businesses must implement “reasonable procedures and practices” to protect consumer’s PI from misuse, inappropriate access and loss.
2. Rights to know how their PI is acquired, used, transferred and rights to restrict what businesses do with their PI
  - a. Right to Know – when requested, businesses covered by the CCPA must respond to consumer requests about how the business acquired their IP, from whom, how it is used, if it was transferred or sold, to whom it was transferred or sold and what specific PI the business has collected.
  - b. Right to Opt-out of sale of PI – Businesses must comply with this request with restrictions
  - c. Right of Deletion – Businesses must comply with this request from a consumer with some restrictions.
3. Businesses must deliver equal service and equal pricing to consumers after they have exercised their rights (with some allowance for discounted services, in exchange for business use of PI)

## Operational Privacy – Business Requirements and Objectives

Privacy becomes operational when all business requirements have been met. The business requirements below are a combination of those it must deliver for consumers and those it must implement to minimize its own risk. Effective implementation of Operational Privacy can only be done within the structure of a formal program. Such a program ensures that requirements are satisfied by meeting measurable objectives, the program is managed beyond the initiation phase and businesses can prove they have taken action to be compliant with the regulations. Meeting requirements can be translated into 10 specific objectives.

### Objectives

1. **Governance** – Implement privacy governance including identified roles for accountability and responsibility, objective and process reporting
2. **Data Mapping** – Create and maintain a detailed list of what PI the business collects including the sources, transferees, where it is stored and how it is protected. This includes PI that may be in structured repositories like databases and PI that may be in less structured repositories like file directories of spreadsheets, documents and emails.
3. **Policies** - Create or update external and internal Privacy and Cookie Policy and manage versions over time
4. **Vendor Management** - Ensure that Third Party contracts are updated to ensure that service providers accept responsibility to use consumer PI appropriately and to protect it. Implement annual vendor security review procedure to protect the business
5. **Minimize Consumer PI** – Consciously reduce the PI the business collects and stores to minimize the risk to the business and the risk to the consumer
6. **Risk Management** - Implement an information security risk management program to regularly update the threats, probabilities and impacts to business assets associated with consumer PI and other risks to information security. The risk management process needs to include identification of protections to mitigate the risks and the plan to implement those protections
7. **DSR Workflow** - Implement a trackable Consumer Access Request/Data Subject Request (DSR) workflow and record keeping procedure
8. **Cookie Banner** - Implement a cookie banner and Do Not Sell option on the business website to inform consumers about capture of technical PI and “sale” of the PI to third parties associated with the business website
9. **Incident Management** - Implement a PI incident management procedure that is activated when an incident has occurred
10. **Employee Training** - Train employees and contractors on new policies, standards and procedures related to CCPA

## Benefits of Risk Management

Implementing and operating a risk management program may seem like extraneous effort to organizations that don't currently do this. On the contrary, a risk management program provides some significant benefits to businesses. These benefits include:

### Identification, prioritization and budgeting and scheduling

Many businesses have not budgeted for the effort to architect, license, implement or operate controls required to protect PI or operate a DSR workflow procedure. Information security controls and procedures cannot be implemented overnight. They take time to define, architect, implement and operationalize. A risk management program can help to identify the priorities and timing of controls. This provides the rationale for business leaders and boards of directors to justify priorities of budget and scheduling.

### Proof of compliance

Courts and compliance enforcement organizations recognize that major activities such as implementing a privacy compliance program cannot be done overnight. Business activities that include assessing risks, defining the schedule of a risk treatment plan and taking action on schedule, as outlined in a risk treatment plan, is proof that the organization takes compliance seriously. This is considered if there is a lawsuit by the state AG or consumers exercising their private right of action.

### Proof that the business has not been negligent

Risk management has been historically focused on risk to the business. There is case law that shows that if businesses do not consider the risk to others, in this case to CA consumers, they could be negligent. The same case law shows that courts understand that there are reasonable limits to the expense and effort that a business employs to deal with risk to others. And there are risk assessment methodologies that consider both addressing the question of negligence and limits to expense and effort. It is wise to employ one of these risk assessment methodologies when doing information security risk assessment to address consumer rights.

## How Assured SPC can help

Assured SPC has expertise in the lifecycle of information security and privacy programs. We assist organizations with requirements for compliance including HIPAA, the California Consumer Privacy Act (CCPA) and GDPR to implement "reasonable security procedures and practices" and to implement the requirements and objectives of privacy laws.

Assured SPC teams have deep experience as IT Leaders in addition to credentials and years of experience driving information security and privacy programs. We regularly help organizations prepare for AICPA SOC2 audits and HITRUST CSF assessments. We also offer virtual c-level leadership for SMB businesses, including Chief Information Security Officers (vCISO), Chief Information Officer (vCIO) and Privacy Officer services.

©Assured SPC 2020 all rights reserved