TLP: WHITE

THE RETAIL AND HOSPITALITY CISO'S GUIDE TO PREPARING FOR THE

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY ISAC

CONTENTS

1 Summary

2 Key questions and insights

2 Understanding key terms and applicability

4 Complying with retailer & hospitality obligations

5 Planning for the future

8 References

SUMMARY

The world has woken up to the significance of data privacy on a global scale. Advancements in digital technologies make it possible for global retail and hospitality companies to tap into new synergies that deepen customer relationships and enrich product and service offerings. This evolution has given rise to a new sense of urgency regarding how companies view data privacy and security.

California is one of several states to lead the way on consumer privacy and security protections, including passing the California Consumer Privacy Act (CCPA) in 2018. According to a joint publication released by DataGuidance and Future of Privacy Forum, CCPA "aims to guarantee strong protection for individuals regarding their personal data and applies to businesses that collect, use, or share consumer data, whether the information was obtained online or offline."

At a high level, CCPA ensures the following rights, subject to certain limitations, to privacy for California consumers:

1. The right of Californians to know what personal information is being collected about them.
2. The right of Californians to know whether their personal information is sold or disclosed and to whom.
3. The right of Californians to say no to the sale of personal information.
4. The right of Californians to access their personal information.
5. The right of Californians to equal service and price, even if they exercise their privacy rights.

The RH-ISAC has partnered with its members and leading industry experts to produce this guide as a source for relevant and actionable insights to help cybersecurity leaders in retail and hospitality improve their understanding of and ability to prepare for CCPA compliance. The guide focuses on relevant articles and sections from the CCPA to maximize usability, and is not intended to be used as a substitute for legal advice. Contents of this guide are based on the version of the CCPA law enacted on June 28, 2018.

KEY QUESTIONS AND INSIGHTS

The RH-ISAC has highlighted key questions and insights pertaining to the following three areas for inclusion in this guide:

1. Understanding key terms and applicability
2. Complying with retailer obligations
3. Planning for the future

UNDERSTANDING KEY TERMS AND APPLICABILITY

What is the CCPA's definition of personal information ('PI')? (1798.140(o)(1)
Personal information is described 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." While the definition of "household" is not defined in the law, it is reasonable to assume that a household may include individuals living at a common address and who may or may not be related.

Readers should note that this description is much broader than the common definitions of Personally Identifiable Information (PII), which includes information that relates to, describes and is capable of being associates with a particular consumer or household. Unique identifiers may also include:

- Real name
- Alias
- Postal address
- Unique personal identifier
- Online identify
- Internet protocol address
- Email address
- Account name
- Social security number
- Driver's license number
- Passport number
- Education information
- Professional or employment-related information
- Geolocation data
- Devices

Companies should also consider inclusion of personal information as commercial information including products or services purchased, obtained or considered, or other data unique to purchase or consumption histories.

Consumers

What is the definition of a "consumer" under this law?
A "consumer" is defined as non-temporary residents of California.

Does a company have to provide information on the following?:

- PI of company employees, retirees, job applicants, contractors, etc.?
- PI of employees of corporate customers (e.g. phone numbers, emails, etc.)?
- PI of employees of company vendors?
- Employees of vendors or corporate customers who are not California-based?

Yes, as long as the individual(s) referenced falls within the definition of a "consumer" under the law. A consumer refers to a natural person who is a California resident as defined by Section 17014 of Title 18 of the California Code of Regulations, as the section read on September 1, 2017 and however identified, including by any unique identifier.

Companies

What are the key criteria that make CCPA applicable to retail and hospitality companies as business entities under the law?
There are two triggers that are likely most common for retail and hospitality companies who are considered a business entity under the law. Those triggers are that the company a.) does business in California and b.) has annual gross revenue in excess of 25mm.

What "specific pieces of information" must a company be able to provide to a requestor? (1798.110(c)(5))
There are two rights which drive this requirement: transparency and portability. Regarding transparency, CCPA grants the right to know what information has been collected as well as what information has been shared within the past 12-months.In reference to portability, the law provides that data subjects that exercise their right to access, must receive the data "by mail or electronically and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transit this information to another entity without hindrance."

What is considered a third party? (E.G. 1798.110(A)(4), (C)(4))
Any party that receives PI is considered either a business or third-party, unless otherwise defined as a service provider. A service provider is a company who contractually cannot use PI for any use(s) outside of satisfying the contracted service requests – they may not share or otherwise use data for other benefit or purpose.

Some RH-ISAC members recommend contract language which stipulates that any selling of PI to a third-party precludes that third-party from selling the PI again unless the consumer has received explicit notice and has been provided the opportunity to exercise their right to opt-out.

Is an academic researcher or governmental entity considered a third-party?
Academic researchers and/or government entities would be considered a third-party, unless there is an associated business purpose as defined by the law with related contract/arrangement.

COMPLYING WITH RETAILER & HOSPITALITY OBLIGATIONS

What is the deadline for a company to have the ability to provide information on categories of personal information it collects about consumers?
Jan. 1, 2020. However, CCPA has a 12-month lookback period.

Does a company need to provide detailed information to a consumer and is internal use of data required to be disclosed?
Companies must provide detailed information to consumers with the purpose for which the data was collected and used, referred to as "commercial purpose of collection." A company must also disclose a description of a consumer's rights and two or more designated methods for submitting requests. Addition disclosure requirements include a list of categories of personal information the company has collected about consumers in the preceding 12 months that most closely describe the personal information collected. This information should be included in the online privacy policy and should be updated every twelve months.

How can a company obtain consent under different conditions for different behaviors while minimizing customer friction?
CCPA is an opt-out paradigm for collection (cookies and tracking technologies), selling and sharing of Personal Information. Based on learnings thus far, some companies will expand on cookie opt-out functionality to go beyond Interest Based Advertising/Online Behavioral Advertising in order to obtain consent. Companies will also have to implement the "Do Not Sell My Data" button on website home pages, along with the necessary backend processes, to fulfill this requirement.

Does a company need to segregate information received from the data subject (to which the deletion right attaches) from information about the data subject?
Companies must manage what Personal Information will be provided in response to an Access Request, and what Personal Information it can delete upon request that does not violate any other requirements, such as contractual or regulatory requirements. There are, however, different requirements. Deletion applies only to the information collected from a consumer.

Does the company also need to be able to flow down this requirement to its vendors in contract?
Yes, deletion requests must flow down to vendors.

Our company does not, today, "sell" information within the meaning of the law. (§1798.140(t)(1)(2)) How does it stay within the "service provider" exception to the definition of "sale"? (§1798.140(t)(2)(C))
Companies may be considered a third-party even in the absence of sales transactions. A company must meet the criteria outlined in 1798.140(t) and (v) of the law to be considered a service provider.

Can we clarify the requirements related to the right to opt-out? ((§1798.135)?
Businesses need to provide a clear and conspicuous link on the internet homepage titled "Do Not Sell My Personal Information," to an internet web page that enables a consumer to opt-out of the sale of the consumer's personal information. The business cannot require consumers to create an account for them to exercise their right to opt-out.

Does the fact that a company does not "sell" consumer information mean that its consumers have no opt-out right? (1798.120)
There is no opt-out right to sell consumer information if the company does not sell consumer information. However, that might not mean that the functionality doesn't have to be offered. The law is somewhat unclear on this.

Does a company need to report consumer-authorized data release of data under CCPA?
Yes, if it is to a third-party.

Does a company have to disclose information shared with a regulatory or government entity of ongoing compliance, such as the Employment Development Department (EDD) and/or the Occupational Safety and Health Administration (OSHA)?
Yes, for those companies which classify government agencies as third-parties.

Academic researchers do not fall within the meaning of "sale" (no valuable consideration) or business purpose. If this is the case, why do we need to disclose this sharing upon consumer request?
An academic researcher can be considered a third-party.

Regarding employee information, do companies have to disclose internal use of employee information (e.g. payroll)?
Yes, in some cases.

Currently, the company has geo-trackers in company vehicles. Does that constitute tracking of a 'consumer'?
Yes

What kind of customer notice must we provide? Can it be high level like Gramm-Leach-Bliley Act? (GLB or GLBA)?
High-level customer notice may be appropriate in limited cases, but not with all. Companies must update Privacy Policies to describe a consumer's rights as they relate to the CCPA and how individuals can exercise them.

Companies should be aware that the common practice of embedding Privacy Policies within "terms of use," often used in mobile environments, is not acceptable.

PLANNING FOR THE FUTURE

What steps can a company take now to prepare for compliance?

1. Conduct process-centric data mapping exercises that encompass the following:

    - Identify all internal and external business processes that process personal data.
    - Use diagrams and/or tables to document details including types of data collected, mechanism collection, business applications and data flows across the process.
    - Identify underlying technology behind business applications and process flows.
    - Complement the exercise with a supply-chain based approach to data mapping, including identifying external entities that supply and/or consume personal data.

2. Use data mapping information to create a privacy-centric data inventory

    - Identify and document privacy-relevant details such as special categories of data, data elements, legal basis for processing, retention requirements, storage geographic locations, 3rd party processors involved, any international transfers, and any other parties with whom the data is shared and for what purpose.

3 Develop and maintain Data Flows of Personal Information in and out of the company recording the business purpose, retention schedule and contractual elements need to determine if a 3rd party is considered a Service Provider.

4 Identify potential gaps in privacy-relevant processes by understanding the following:

- Are existing processes designed to satisfy relevant data subject requests?
- Do existing technologies allow for timely deletion/modification of personal data for a given subject across all instances?
- Are all data transfers backed by appropriate privacy agreements?
- Are there any data residency concerns?

5 Increase your company's likelihood of success:

- Establish a governance program
- Involve stakeholders from all relevant departments, including Privacy, Compliance, Legal, Information Technology (IT), Cybersecurity, Human Resources (HR), Sales/Marketing, Development/Engineering, Management, Research and Development (R&D) and any other relevant parties
- Use Governance Risk Compliance (GRC) tools or purpose-built privacy tools if possible to facilitate information gathering and documentation of data maps
- Gain buy-in by emphasizing the additional benefits of performing a data mapping/inventory beyond privacy (i.e. better data management, operational/process improvements, etc.)
- Assign ownership and develop processes to ensure mapping/inventory is maintained
- Evaluate and make any necessary expansion to cookie opt-out processes for non-interest-based advertising technologies
- Develop processes to offer and handle Request to Access and Delete Personal Information
- Develop processes to offer and handle "Do Not Sell My Data" requests
- Develop Awareness and Training programs
- Evaluate staffing requirements to address estimated volume of Requests

How can a company estimate potential liabilities resulting from Data Subject Access Requests (DSARs)/Data Subject Deletion Requests (DSDRs)?

At the time of this publication, DSAR/DSDR enforcement issues reside with the California Attorney General (AG). Estimates should take company and industry-specific considerations into account. Some example considerations include the following:

- What data do we hold from consumers and what benefits do consumers get from requesting access?
- How easy it is to make requests? This will impact how many people are willing to go through the process.
- Are there any social or other activists that may try to use DSARs/DSDRs as a means of imposing hardship on the company?
- Are there any other factors that may draw public and/or attorney interest in our company when the regulations come into effect?

It should be noted that the deletion requests can only be made by a consumer regarding data collected from the consumer. The deletion right is subject to a number of specific exemptions, as well as the general exemptions from the law such as those related to compliance with legal obligations, to detect security incidents, etc.

Which departmental leaders will be responsible for monitoring a company's ongoing CCPA compliance program?

The RH-ISAC polled its CISO members to gather more information in response to this question. Based on the most common responses, for most companies the Chief Information Security Officer (CISO) and head of legal will share joint responsibility for monitoring CCPA compliance on an ongoing basis. Three of ten total respondents indicated that the Data Protection Officer (DPO) position required for GDPR compliance already existed within their organization, and that this individual would also assume responsibility for CCPA compliance.

	Legal (Privacy Attorney/General Councel)	Corporate Compliance	Chief Information Security Officer (CISO) or equivalent	Chief Information Officer (CIO) or equivalent	Chief Privacy Officer (CPO)	*Also designated Data Protection Officer (DPO) for GDPR
Company A	X					X
Company B				X		X
Company C			X			
Company D	X		X			
Company E			X			
Company F	X					
Company G		X				
Company H					X	X
Company I	X					
Company J			X			

Which department(s) have companies charged with "owning" responses to Data Subject Access Requests (DSARs)/Data Subject Deletion Requests (DSDRs)?

Based on responses to the above mentioned poll, ownership will vary by company. Some member responses include the following:

- The privacy office will receive requests and respond to those with a systemic solution. For all other requests, Marketing will respond to those that are customer-generated and Human Resources will respond to Employee requests.
- Our privacy attorney in California is "accountable" for DSAR completion, but there are several responsible parties in the work flow that actually complete the tasks required to fulfill a DSAR. The attorney & privacy analyst on her team will monitor and escalate if needed to ensure that the 30-day response requirement is met.
- DSAR requests belong to the customer relations team, but are reviewed by members of the CISO's team for validation & metrics tracking.
- Our legal privacy department is leading our compliance with CCPA. They also coordinate our DSARs but there are multiple teams including IT involved in the process.
- Our Privacy team is ultimately responsible for ownership of all Data Subject requests from start to finish. All requests are funneled to the Privacy team for evaluation/approval and are then routed to appropriate business and technology groups to address.

What types of technologies are being evaluated to assist with fulfilling requirements under CCPA?
Members reported that their companies are evaluating various technology solutions to support compliance. Some responses include:

- Leveraging/expanding existing Cookie opt-out implementations
- Tools used to inventory and map data flows, applications and 3rd parties for GDPR

CONCLUSION

RH-ISAC members offer an array of services, goods, and experiences such as shopping, entertainment, dining, hospitality and gaming. In a world of shifting consumer expectations, these companies must constantly adapt to better protect consumers, employees and brands. The CCPA was enacted to support consumer privacy and as we look forward into 2020 and beyond, companies can anticipate a continued focus on privacy from a legislative perspective. It is important for companies to take steps now that support preparedness. Along with key recommendations included in this Guide, the RH-ISAC encourages its members to share additional strategies and best practices within the membership community through the CISO and legal email lists, virtual community discussions, and at in-person meetings and events.

ABOUT THE RH-ISAC

The RH-ISAC operates as a central hub for sharing sector-specific cyber security information and intelligence. The association connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other—all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC currently serves companies in the retail, hospitality, gaming, travel and other consumer-facing entities. Follow us @RH-ISAC on Twitter or visit our website at https://www.rhisac.org.

RETAIL & HOSPITALITY ISAC

REFERENCES

"Comparing privacy laws: GDPR v CCPA," DataGuidance and Future of Privacy Forum. https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

CCPA articles. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

CONTACTS/AUTHORS

Andrew Serwin
Partner & Co-Chair, Global Data Protection, Privacy and Security Practice
DLA Piper
andrew.serwin@dlapiper.com

Rocco Grillo
Managing Director, Global Cyber Risk Services
Alvarez & Marsal
rgrillo@alvarezandmarsal.com

Jennifer McGoldrick-Stenberg
Vice President, Membership and Operations
RH-ISAC
Jennifer.mcgoldrick-stenberg@rhisac.org