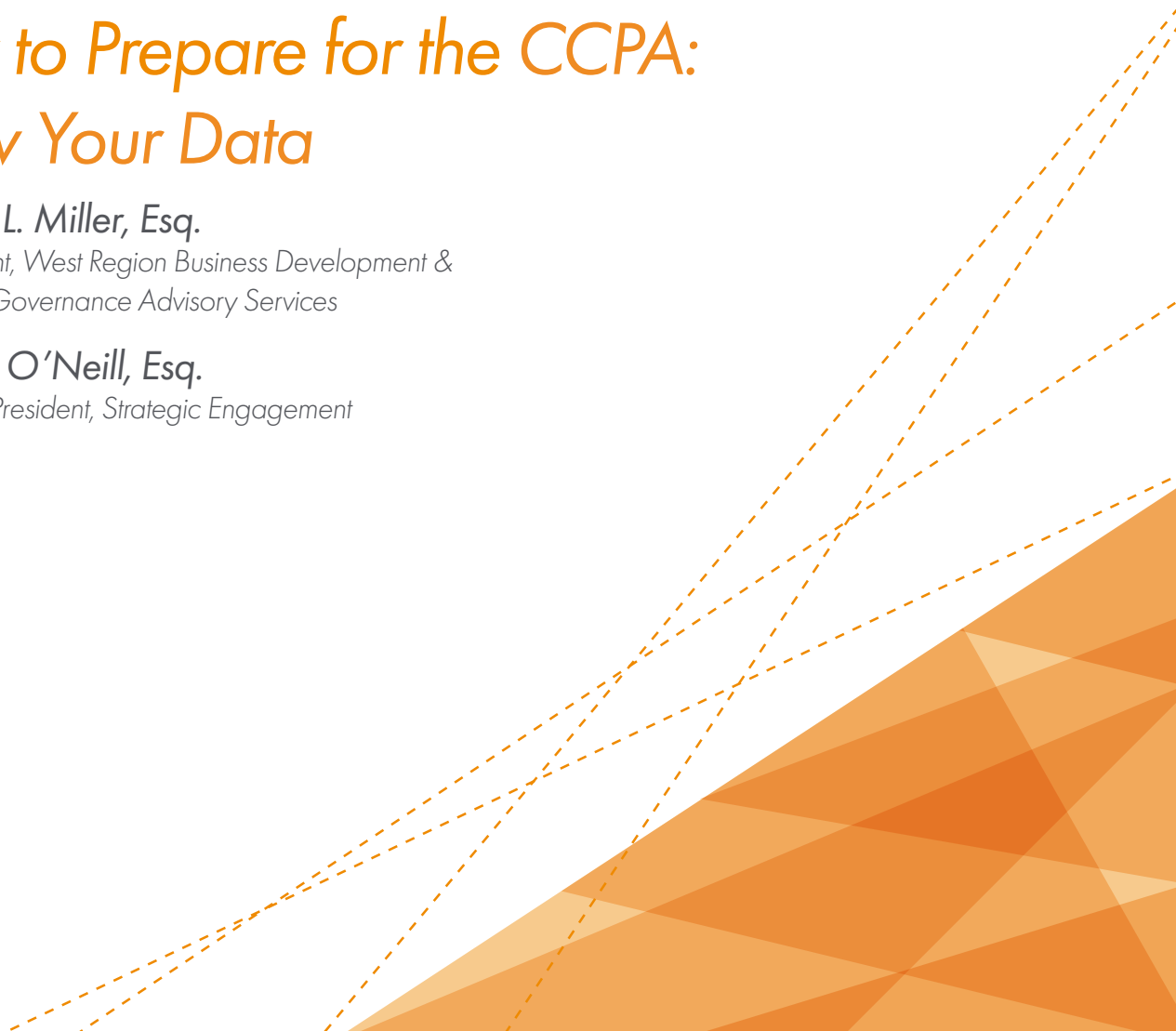
Consilio®

Global Leader in Consulting & Legal Services

How to Prepare for the CCPA: Know Your Data

Matthew L. Miller, Esq.
Vice President, West Region Business Development & Information Governance Advisory Services

Maureen O'Neill, Esq.
Senior Vice President, Strategic Engagement
CIPP/US, CIPP/E



How to Prepare for the CCPA: Know Your Data

In a highly globalized market where big data proliferation has run unchecked, organizations are increasingly vulnerable to mismanagement of their information assets. In response, data privacy regulation has been on the rise over the last few years. The law with the most impact to date has been the European Union's General Data Protection Regulation (GDPR). The GDPR sent organizations around the globe into a panic as they attempted to bring their policies into compliance before the law went into effect. Even now, well after its effective date, many organizations are still struggling to comply with the GDPR, placing them at risk of significant fines and penalties—up to 4% of global revenue for the most serious violations.

Now, organizations have another reason to be concerned. The latest data privacy compliance challenge comes not from Europe, but from the United States—in the California Consumer Privacy Act of 2018 (CCPA), the broadest law of its kind in the U.S. Inspired by the GDPR, and in response to a number of recent incidents that "highlighted that our personal information may be vulnerable to misuse when shared on the Internet," the CCPA aims to give consumers more control over their personal information so that they can avoid the misuse of their data.

With the January 1, 2020, effective date of the CCPA approaching fast, organizations need to act now to prepare for compliance. As the law's requirements make clear, it all starts with knowing your data.

What does the CCPA require?

The CCPA gives California residents four distinct data privacy rights, with corresponding obligations on businesses to respect and protect those rights. The scope of the CCPA is sweeping, extending to businesses well beyond California's borders and defining protected "personal information" expansively.

The first right set out in the CCPA is the "Right to Know." Businesses must notify consumers, through a publicly posted privacy notice or in answer to a consumer's request, about what information they collect, how they collect it, and how they plan to use it, including whether they plan to disclose or sell that information. The second right is the "Right to Opt Out." All consumers have the right to opt out of allowing businesses to sell their personal information to third parties; consumers under the age of 16 must affirmatively opt in for their information to be sold, and consumers under 13 must have consent from a parent or guardian. The third right grants consumers the "Right to Delete" their personal information (subject to certain exceptions). Lastly, the "Right to Equal Treatment" protects consumers from discrimination when they exercise their personal information privacy rights.

The CCPA is not limited to businesses physically located within California's borders. Rather, it applies to any for-profit entity that does business in the state and which meets any one of three threshold tests: (1) has gross revenue of more than $25 million; or (2) annually buys, receives, sells or shares the personal information of 50,000 or more California consumers, households or devices; or (3) derives 50 percent or more of its annual revenue from selling California consumers' personal information. The CCPA also extends to any entity that controls or that is controlled by a business that meets the criteria above and that shares common branding with that business.

The CCPA's definition of personal information is unprecedented. The law defines personal information 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." The definition includes the following details, so long as they are not publicly available:

- any identifying information, such as names, aliases, addresses, unique personal identifiers, online identifiers, IP addresses, email addresses, account names, Social Security numbers, driver's license numbers and passport numbers;

- any protected characteristics under California or federal law, such as race, sex, age, disability status and many more;
- commercial information, including "records of personal property, products or services purchased, obtained or considered or other purchasing or consuming histories or tendencies";
- biometric information;
- internet and electronic network activity information, such as browser history;
- geolocation data;
- audio, electronic, visual, thermal, olfactory or similar information;
- professional or employment-related information;
- education information; and
- inferences drawn from any of the above information to create a profile "reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes."

The law also expands the definition to include any information that could be "associated with" or "reasonably linked, directly or indirectly" to a particular consumer or household.

In the current iteration of the law, violations proven by the California Attorney General are punishable by civil penalties of up to $2,500; the fine rises to $7,500 if the violation is shown to be intentional. The law also creates a private right of action for individual consumers if their unencrypted personal information is accessed, stolen or disclosed as a result of an organization's failure to employ reasonable security procedures. Damages can range from $100 to $750 per consumer, per incident, or can extend to actual damages, whichever is greater. Given the significant scale of many recent data breaches, it's easy to see how these statutory damages can quickly add up to liabilities of tens—if not hundreds—of millions of dollars.

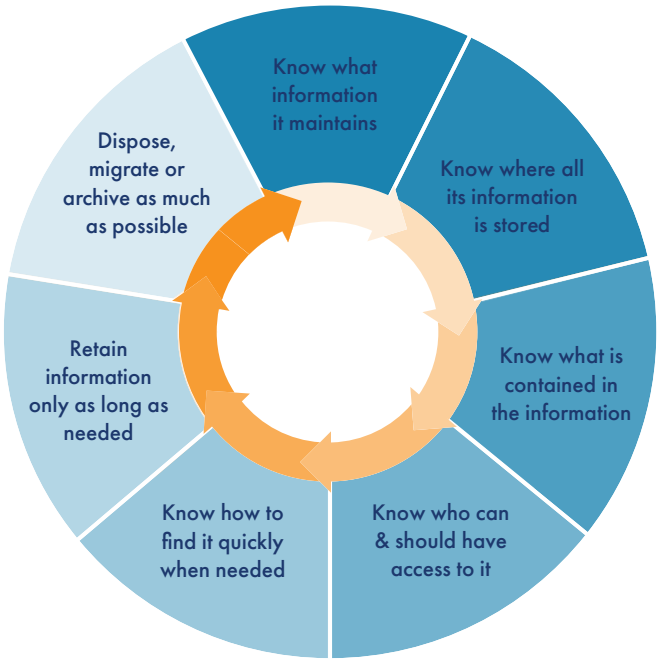
In light of the complexities of the law and the potential stakes of its violation, businesses should start preparing for the CCPA now. This is especially true due to a provision in the law mandating that responses to data access requests must cover the previous 12 months of data—even for the 12 months preceding the law's effective date, all the way back to January 1, 2019. For most organizations, the best way to get started with a compliance program is to "know your data."

What does it mean to "know your data"?

Knowing what data you have and where it exists is a gargantuan task in today's corporate environment.

Every day, employees create, use and interact with various data stores within an enterprise, including workstations, file shares, databases and email, in the course of performing critical business functions. Companies already have a hard time tracking this information, given the rapid pace of data growth and transfer. Given data's fluidity, it is hard to know precisely what information organizations have, where that data is located, what it contains, who can and should have access to it, and how to find specific data within a reasonable timeframe—and even harder to have confidence that what you have found is both the right data and all of the right data. This graphic illustrates the various aspects of truly "knowing your data"—

Does your organization...



Organizations that do not have a good grasp of their data will be unable to comply with the CCPA, particularly the category-centric required disclosures and consumer requests for specific pieces of personal information. Locating sensitive personal data with a reasonable degree of accuracy is challenging to the point of impossibility in the absence of proper data identification and classification.

And with the size of most organizations' data populations, it can be difficult to find specific data without indexing the entire corporate network, an endeavor for which few organizations have the people, processes, technology, time or budget required. Fortunately, there is a better way.

Where do you start?

To determine the optimal place to start, conduct an information governance maturity assessment, evaluating your organization's people, process and technology assets. Begin by benchmarking your organization's current state. For example, do your employees keep every bit and byte of data that they create, with no structure to the methods and locations of storage? Or have you implemented—and enforced—a comprehensive enterprise retention schedule, along with tight controls on the devices used to create and store data? Or does your organization fall somewhere in between these extremes?

Next, identify any applicable risks, including the CCPA, that your current state of information governance maturity implicates. Define the gaps in your approach to your information in light of these risks, and make recommendations for remediating them. Finally, establish goals, a road map and a timeframe in which you'll achieve your desired maturity level.

Understand what data you have

Once you know where you stand with your policies and practices, take an inventory of your organization's data. Create or re-vamp an existing global data map. Make sure you capture all sources of data, including servers, computers, cloud-based applications and other software, as well as archival systems and mobile devices. Be vigilant about searching for shadow IT—non-sanctioned, unsupported hardware and software applications that employees have started using without notifying IT.

Understand how your data flows

The next step is to assess how data moves through your systems. Create a map of critical and sensitive data as it flows from place to place, showing what data you're collecting. In light of the CCPA, pay particular attention to all the various types of personal information collected from "consumers" as defined by that law. Indicate the source of each type of data and determine where it is stored, including the locations of any copies of that data. Also record everyone that you share the data with or sell the data to, and denote who has access to it, both inside and outside your organization. And make note of the purported business purpose for collecting the data.

Understand what data you need—and what you don't

The final step is to distinguish your organization's critical business data from data that is redundant, obsolete or trivial (ROT)—which offers minimal, if any, business value. ROT can constitute anywhere from 25 percent to 75 percent of the average organization's unstructured data storage footprint—but fortunately, it is often possible to identify ROT based on its metadata alone.

Sampling methodologies, data analytics and scanning technologies can help you study the large-scale unstructured information assets on your organization's network to determine data classifications and percentages of content composition. Armed with this intelligence, you can prioritize which repositories you should target for classification as ROT, critical business data, or sensitive data such as personal information or protected health information for identification and further review.

Once you've isolated the ROT, dispose of it following your records retention protocol. If you don't have a formal records retention schedule, there's no time like the present to implement one. And, if you find that your organization is collecting more personal information than is necessary for your business operations, mitigate your CCPA risk by ceasing those extraneous collections.

Conclusion

If your organization diligently prepared for the GDPR, don't be lulled into thinking that you're magically in compliance with the CCPA. The two laws offer consumers some similar rights, but they differ markedly in the requirements they impose on businesses. A better approach is to view the CCPA as its own beast—and as a harbinger of U.S. privacy laws to come. Therefore, it might make sense for many organizations doing business across multiple jurisdictions to start treating all data—whether of California residents or anyone else—as potentially subject to the privacy requirements of the CCPA.

Doing so not only sets in motion a paradigm that ensures your compliance with the law and enables you to respond confidently to regulatory inquires but, can also demonstrate your organization's commitment to data privacy and security. Such a commitment can serve as a competitive advantage that sets you apart from your peers, and which inspires greater trust with your clients.