Data privacy, retail and consumer goods: Meeting the needs of CCPA, consumers, and the bottom line
**Introduction**

What drives every retail and consumer oriented business model these days? Personal data. It’s flowing from in-store and online transactions, store technology, loyalty programs, social media, as well as mobile operators and other providers. Driven by competitive pressures from digital natives, and by the value that hyper-personalized shopping and marketing offers, many consumer-facing companies are making data gathering and insight a core competency.

As consumer data and its monetization potential grows in significance, so do the privacy challenges. A new set of regulations is almost here: the California Consumer Privacy Act (CCPA), which was passed in June, is scheduled to go live on January 1, 2020.

Privacy regulation may sound onerous, but it doesn’t have to be. With the right approach, retailers and consumer-packaged goods (CPG) companies can deploy the latest data gathering and analysis tools, meet or exceed customer expectations for personalization and privacy, and comply with regulatory demands.

To do all that, enterprises need to move quickly and they need a plan.
Data privacy, retail and consumer goods: meeting the needs of CCPA, consumers, and the bottom line

April 14, 2016
EU adopts GDPR

June 28, 2018
California adopts CCPA

May 25, 2018
GDPR goes live

January 1, 2020
CCPA goes live
With a compliance deadline of January 2020, the clock is ticking on CCPA. The legislation is complex, and some ambiguity remains, but here are a few of the highlights:

• Increased transparency. At or before the point of collection, organizations must indicate to consumers the categories of personal information they collect, disclose or sell. Planning to track transaction information for personalized marketing? You’ll have to let consumers know.

• New consumer rights. Customers will have the right to see what personal information of theirs organizations are collecting, disclosing, or selling. They will also be able to request that companies delete their data or stop selling or disclosing it. Organizations will have 45 days to satisfy these requests.

• Limits on differential treatment. Enterprises won’t be able to give consumers who share their personal information better prices or services than they give to consumers who exercise their privacy rights—unless the difference in price or service is a direct result of value provided to the consumer from his or her personal information. There’s a lot of ambiguity around this requirement but, for example, special offers based on loyalty program data could pass muster. Charging higher prices across the board to a user who opts out of location tracking probably won’t.

• Data lifecycle management and rights processing. To meet the above demands, organizations will need to know where consumer data comes from, how it is used, and where it’s going, with special tracking of any selling of personal information.

• Third-party risks. Retailers will have to ensure that suppliers, vendors, and other third parties with which they share consumer data can also respond to consumer requests to delete or stop selling their data.

• Information security. California consumers will have a new private right of action in certain cases when “non-encrypted” or “non-redacted” personal information is compromised. Potential statutory damages will range from $100 to $750 per consumer incident and up to $7,500 per CCPA violation.

• Partial grace period. Under an amendment passed August 31, 2018 (SB 1121) by the California legislature, the California Attorney General cannot enforce the CCPA until six months after the publication of final regulations or July 1, 2020, whichever is sooner. That likely provides a six month grace period, during which companies won’t face CCPA-related state enforcement actions. However, SB 1121 does not delay the new consumer private right of action if personal information is compromised. Under the current schedule, companies may still face such actions starting January 1, 2020.
GDPR and CCPA: Several big differences

One difference lies in the definition of personal data. For GDPR, personal data is anything that an organization could use to identify you: factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity. Name, government identity numbers, fingerprints, IP addresses, and cookie identifiers are a few examples.

The CCPA broadens this definition to include any information that identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. That may include identifiers such as consumer browsing history and tendencies, products or services purchased, and inferences drawn from any personal information.

It’s worth emphasizing here the CCPA’s inclusion of household as well as individual data. This dynamic potentially adds another layer of complexity to compliance. Certain data types that won’t identify individuals could be linked to a particular household.

Another difference is how the CCPA allows consumers to opt out of the sale of their personal information. Under the CCPA, data “selling” means not just selling but also renting, releasing, disclosing, disseminating, making available, or transferring orally, in writing, or electronically, consumer personal information to a third party for monetary or other valuable consideration. GDPR, by contrast, only enables consumers to restrict “processing” of data, and that only under certain conditions.
The need to adapt data tools

CCPA’s coming rules are a big deal for retail and CPG companies’ data practices. Here are just a few of the current or emerging tactics and technologies that enterprises may have to modify:

### Personal device tracking
Beacons allow retailers to track smartphone MAC IDs that enter their store.

### Loyalty programs
Consumers share personal information when they sign up for loyalty programs.

### Biometrics
Facial recognition and behavioral biometrics can identify a consumer.

---

<table>
<thead>
<tr>
<th><strong>Personal device tracking</strong></th>
<th><strong>Loyalty programs</strong></th>
<th><strong>Biometrics</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>It's common for retailers to track MAC IDs of smartphones that enter their stores. Through the use of beacons, retailers may use this tracking for proximity marketing: they could, for example, know that a consumer is in the “back to school” supplies aisle and send a suitable ad or coupon. Some may take personalization even further. For example, a consumer may look at certain items on a retailer’s website, and even place them in their online shopping cart but not complete the purchase. When a retailer sees that consumer’s MAC ID enter a store, it can push marketing for those specific items. However, under the CCPA, a MAC ID may become protected personal information if it is capable of reasonable association or linkage to a person or household, so the customer may have to explicitly agree to this kind of marketing.</td>
<td>Retailers and CPG companies like to reward loyal customers—and part of the deal is that loyalty program members, when they sign up, share certain personal information. But the CCPA establishes certain limits on special prices or services for those who share personal information, compared with those who don’t. Enterprises whose loyalty programs offer special benefits, as most do, may need to make changes: they may not, for example, be able to require data sharing as a condition of joining the program. These retailers might then have to look at third party services, synthetic populations, and other advanced analytics techniques to fill in gaps in data sharing.</td>
<td>Enterprises are increasingly using facial recognition as well as behavioral biometrics: the way people touch, tap, and hold their devices is unique and can identify them. For now, most enterprises that use this data are doing so to crack down on fraud and other crimes—but some are considering it for marketing. That would put it squarely in the sights of the CCPA, which considers biometrics (including behavioral biometrics) protected data. Consumers who permit retailers to use their biometrics to protect them against fraud may still refuse to allow them to use this data for marketing.</td>
</tr>
</tbody>
</table>
When an enterprise builds a brand around privacy, consumers aren’t just more likely to think fondly of that enterprise (and perhaps consider its products more favorably); they’re also more likely to let that enterprise gather, process, and even sell their data. To build that trust, the enterprise should embed three principles. These principles will also foster a culture that will make it easier to comply with CCPA, GDPR, and other state or federal privacy regulations that will surely appear in the coming years.

1. **Transparency.** No one likes surprises in how their personal data is used, and hardly anyone has time to read all the fine print in disclosures and consent agreements. To inspire confidence in consumers, offer concise, easy-to-understand, constantly updated information on how the organization will collect, use, and share their data.

2. **Protection.** It’s not enough to use your customers’ data in line with their wishes. You must ensure that you don’t allow anyone else—whether malicious actors or third parties—to abuse this data. Rigorous cybersecurity along with enhanced privacy technology such as data minimization, encryption, and pseudonymization can provide strong defense.

3. **Value for value.** Your customers’ data is valuable to you—give your customers something valuable in return: a personalized experience with relevant content and promotions (so long as these extra benefits comply with CCPA.) Make your customers valued members of a community from which they too benefit.
Next steps

GDPR is already here. CCPA goes live in 2020 and other regulatory mandates may be forthcoming from other jurisdictions. Enterprises need to move quickly to create the right culture and a repeatable framework for compliance—at the same time they continue to pilot and roll out new tools and processes to gather, analyze, and potentially monetize data.

Every enterprise is different, but here are five steps that retail and CPG companies should consider as the countdown to 2020 begins.

Step 1. Discover and analyze

What parts of the business and what back office functions have to do in order to comply with CCPA? For most retailers and CPG companies, it is a complex question to answer.

Enterprises will need a system to track all business processes, third parties, products, devices, and applications that process California residents’ personal information—and to keep up with any changes.

This system should start with a data inventory, covering all categories of personal information as defined under CCPA. This inventory should also flag the source of personal information, the business purpose for processing, and wherever personal information is sold or shared with a third party as personal information collected before January 1, 2019 may be exempt from certain CCPA requirements.

Retailers and CPG organizations should use this exercise to help build processes to keep only the data they need. As the business value of data grows, so do the risks and liabilities of improper data handling. Unnecessary data can lead to unnecessary risks and liabilities.

Step 2. Assess and recommend

After establishing an understanding of your personal information footprint, retailers and CPG organizations can then assess their privacy and data related program capabilities against the key requirements of CCPA. Take future needs into account, too. Planning to start using facial recognition to track shoppers? You’ll need to plan for suitable compliance capabilities.

The goal is to capture the compliance gaps and build a plan to close them, in line with the company’s business goals and risk profile.

Aim to take advantage of privacy and data governance tools and capabilities that the enterprise already has in place. Common examples which, if properly scoped and leveraged, can support CCPA compliance include:

- templates for records of processing
- systems and technologies to triage and respond to consumer rights requests, or that could be leveraged in such a manner
- privacy impact assessments (PIAs)
- privacy-by-design techniques
- third party risk management processes
Set the implementation strategy

With cross functional teams and a “compliance map” in place, it’s time to decide on the big picture. There are two main approaches to achieving CCPA compliance in a way that keeps costs reasonable, builds the brand with customers, and meets the business’s needs.

1. Expand existing programs. If you already have a robust privacy program designed to meet GDPR’s requirements, you may want to expand and adapt the program to cover domestic operations subject to CCPA.

2. Start with CCPA. Some companies are primarily based in the US or have US-based divisions that hardly interact with Europe; or they haven’t yet achieved a satisfactory level of GDPR compliance. For these companies, it may make sense to start with a focus on California, then add on GDPR and other jurisdictions as needed.

Companies that choose the first option must pay special attention to how CCPA differs from GDPR, particularly the broadened definition of personal information and the new consumer right to opt out of the sale or disclosure of personal information.

Companies that choose the second option will have to plan for the future: build in the flexibility to make a “California-only” privacy program an integral part of a global privacy program. These organizations will also need to assess their desire or ability to bifurcate compliance capabilities between California customers and the rest of their US customer base.

Step 3. Strategize and plan

Mobilize across functions

Data crosses the entire enterprise; a single individual’s information likely touches multiple functions and business units. To achieve compliance, while meeting customer expectations and the business’s needs, bring all relevant business, technology, and compliance stakeholders on board, including existing digital, analytics, or data governance teams, to create a cross-functional team.

This team should be able to identify every part of the enterprise that is collecting, using, sharing, selling, or otherwise monetizing data. It can then

- determine needed new processes, technologies, and tools
- establish and define an ongoing governance structure to coordinate, operate, and implement remediation activities
- define the privacy program’s desired future state, including roles and responsibilities
- align the program with the needs of the business for new and better data gathering and analytics tools and technologies
- integrate customer expectations for transparency, protection, and value
- obtain senior level sponsorship
Step 4. Design and build

It’s now time to implement: focus on seven workstreams to enable sustainable compliance.

• **Policy management** - Update and document privacy policies, notices, procedures, and guidelines to fulfill CCPA requirements.

• **Data lifecycle management** - Identify new personal data processing and use activities; implement checkpoints and controls; establish a personal information “source-of-truth” for all CCPA compliance initiatives.

• **Individual rights processing** - Implement a request management process (including new technology as needed) to receive, verify, and comply with consumer privacy rights requests within CCPA’s 45 day timeframe.

• **Privacy by design** - Develop a privacy-by-design strategy and playbook to embed CCPA privacy controls and impact assessments throughout the data lifecycle.

• **Information security** - Identify existing information security and data protection controls; align practices with the CCPA’s needs; look to industry standards and align with the enterprise’s collection and usage of personal information.

• **Data processor accountability** - Establish or adjust privacy risk assessment and due diligence requirements for third parties and service providers to comply with CCPA; update as needed service-level agreements with third party data processors.

• **Training and awareness** - Create CCPA awareness across the organization, making use of existing data privacy related training efforts where possible.

Step 5. Operate and monitor

Even with a CCPA compliance program up and running, the job isn’t over. Establish an ongoing data governance and privacy compliance monitoring program to promote continued accountability. Consider a “playbook” to respond to possible inquiries from regulators and to demonstrate full and ongoing compliance. Leverage the third line of defense to define and implement an audit program that periodically assesses CCPA and privacy compliance controls and processes.
No one clamors for new regulations, but CCPA offers an opportunity: to rethink privacy programs to enable new technologies that give the business what it needs, while giving customers the transparency, rights, user experience, and value that they demand.

With a five-step approach that accounts for the enterprise’s existing and future data and privacy needs, it is possible to achieve a harmonious balance: achieve regulatory compliance while building brand loyalty and trust with customers and employees alike.

With 2020 nearing, and customer attention to privacy growing, now is the time to get started on a robust CCPA-compliant privacy program.

Contacts

**Sean Joyce**
Cybersecurity and Privacy Leader, PwC US
+1 (703) 918 3528
sean.joyce@pwc.com

**Jay Cline**
Principal, US Privacy Leader
+1 (612) 596 6403
jay.cline@pwc.com

**Mir Kashifuddin**
Partner, Cybersecurity
+1 (214) 754 4537
mir.kashifuddin@pwc.com

**Brett Croker**
Director, Consumer Markets Privacy
+1 (678) 419 2107
brett.j.croker@pwc.com

Strategic Team

Jocelyn Aqua
Amy Barry
Scott Bauer
Matt Egol
Joshua Goldman
Dan Horch
Christopher Perrigo