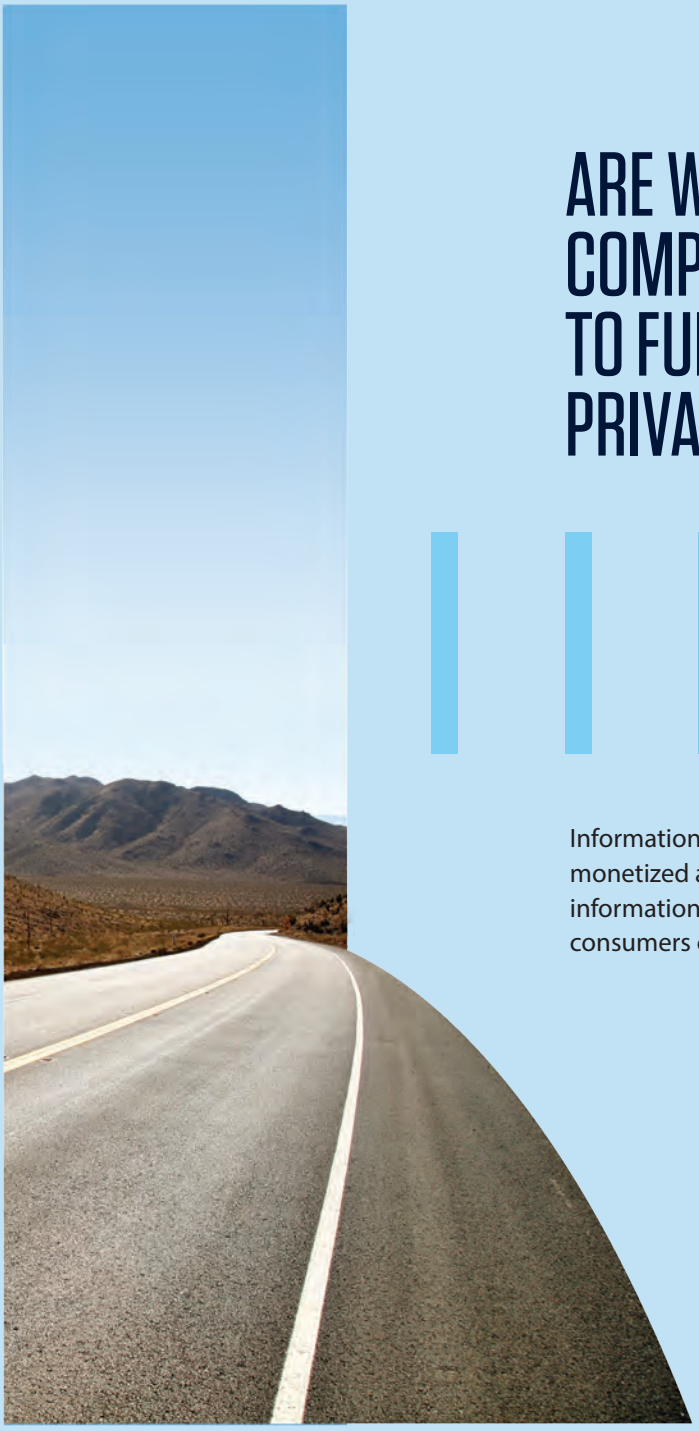
Infosys®
Navigate your next

VIEWPOINT



ARE WE THERE YET? COMPANIES FACE A LONG ROAD TO FULFILLING CONSUMER PRIVACY REQUIREMENTS

Information has never been as ubiquitous or easily monetized as it is now. This monetization of personal information happened faster than governments and consumers could perceive. Now, they are responding.

Infosys® | Knowledge Institute

Governments around the world have stepped in to protect the consumer. The European Union brought its General Data Protection Regulation into force in 2018. The California Consumer Privacy Act became law at the start of the year, with enforcement set to begin on July 1, 2020. The regulators and authors of these rules recognize the transformational value of data and its intrinsic complexity. California's attorney general estimates the total value of personal data in the state would be more than $20 billion U.S. annually.[1] Another study suggests that state of California has suffered more data breach incidents in past decade than any other US state.[2] With other states following California's lead,[3] companies must define their approach to privacy matters and establish detailed plans to comply with laws and preserve the trust of customers and other stakeholders.

At Infosys, our consulting practice has served many global clients in their GDPR and CCPA journeys to compliance. This has provided a unique perspective across companies, industries and even geographies.

This paper covers a brief about the CCPA regulation, the state of CCPA compliance, challenges faced by clients, best practices for executing a CCPA program and our view into the future of data privacy regulations.

California consumer privacy comes first

The California Consumer Privacy Act is one of the most comprehensive data privacy laws released by a U.S. state. The act went live on January 1 2020, providing residents of California a strong control on their personally identifiable information as well as a clear view into the ways firms use their data. Although the CCPA is still undergoing revisions,[4] it is shaping into one of the most impactful data privacy regulations in the digital era. Given the large scale and frequency of data breaches,[5] businesses should anticipate this and further interventions. Further, California officials in late March declared they will begin enforcing the law on July 1, regardless of disruptions tied to COVID-19.[6]

California officials estimate the cost of compliance with CCPA to be around $55 billion.[7] The CCPA outlines additional rights for California residents related to the collection, sharing, processing and storage of their personal information. Companies doing business in California must adopt an array of practices designed to protect consumer privacy and develop processes to enhance transparency around how consumer data is managed. Specifically, the act grants individuals:

- the **right to opt out** of services offered by an enterprise.
- the **right to know** what information is collected by a company.
- the **right to access** that information.
- the **right to delete** their information from a firm's databases.
- the **right to equal** service from a company.

Infosys Consulting has found that the right to opt out has the broadest potential impact across companies. Preparing for opt-out requests projects to have high impact in companies' people, process, technology and security domains. Some of our clients have prudently prioritized this as the first focus area in their work to address CCPA requirements.

Figure 1. The right to opt out has the broadest impact across enterprises.

	People	Process	Data	Technology	Security
Right to opt out	High	High	Medium	High	High
Right to know	High	High	High	Medium	Medium
Right to access	Medium	High	Medium	High	High
Right to delete	Medium	High	High	High	Medium
Right to equal service	Low	Medium	Low	Low	Low

Source: Infosys Consulting

Compliance coming slowly

Despite the fast-approaching enforcement deadline, most U.S. businesses do not comply with CCPA rules, according to a recent survey.[8] Most senior business managers do not grasp the importance of CCPA compliance, the survey shows. And nearly half of organizations surveyed have not allocated budgets to comply with CCPA (or other soon-to-come privacy laws). Further, more than one-third of organizations have not conducted an audit to determine where their data resides – a key early step to understand how privacy laws impact a company. This low compliance level suggests more possibility of low compliance for many companies and echoes the experiences of many companies and Europe's GDPR privacy rules.

When California begins enforcing its privacy rules on July 1, monetary penalties will likely accumulate swiftly, because the law levies fines on a per-violation basis. Since its implementation in 2018, EU authorities have imposed more than 100 million euros in fines and penalties through Jan 2020. In the largest single instance, CNIL, the French data protection regulator, fined Google 50 million euros for "insufficient legal basis for data processing." Google was fined another 7 million euros by Swedish authorities for "insufficient fulfilment of data subjects' rights."

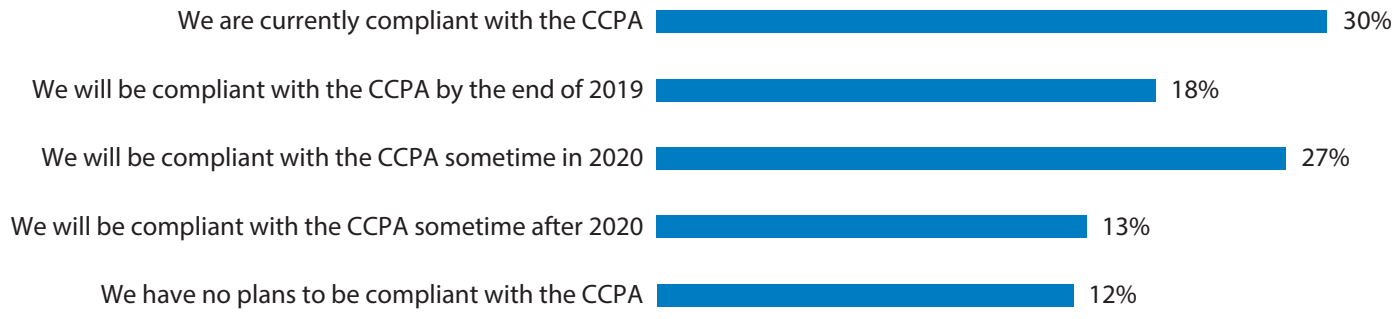
Three approaches to CCPA compliance

Organizations have taken up adoption of CCPA in different ways depending on their scale, commitment to privacy and how they perceive the privacy act will impact their business. There are three distinct approaches, with holistic most recommended:

The holistic approach

Some organizations have initiated strategic, enterprise-wide data privacy efforts with a long-term view toward establishing strong data stewardship and governance. This is the most prudent approach to data privacy, given the growing number of U.S.

Figure 2: Fewer than half of companies who were surveyed in late 2019 said they would achieve CCPA compliance before Jan. 1, 2020.



Source: Osterman Research

states that have introduced or passed privacy related regulation.[9] We have seen organizations in this category start their compliance journey early and establish robust programs to address the data privacy mandates.

The targeted approach

Other organizations have targeted focused first on complying with the low-hanging fruit of the CCPA, such as updating privacy notices. Some have targeted customer information databases and not scanned all repositories. In addition, their focus on training has been tactical at best. However, given the broad scope of CCPA requirements, this approach may help organizations meet regulations proposed by other states. However, if other states proposed stricter regulations, businesses will have to develop additional one-off solutions.

The wait-and-see approach

Some organizations have deferred CCPA specific initiatives – primarily by asserting they comply or by questioning whether data privacy rules apply to their business. For example, firms that already comply with data privacy provisions of the finance-oriented Gramm Leach Bliley Act of 1999 or the Health Insurance Portability and Accountability Act of 1996 highlight their similarities with the new California act. These firms have taken the position that they are broadly CCPA-compliant by virtue of following the existing regulations. While this may satisfy immediate needs, it will in no way prepare them for more stringent privacy regulations in the future.

Companies challenged to comply with CCPA

Companies face a myriad of challenges during their compliance journey. Some examples of these challenges include:

- **Personally identifiable information** – California classifies linked and linkable data as PII (Figure 3), but how much data that covers has yet to be clearly defined.

Figure 3. Personally identifiable information covered by California's data privacy act includes directly linked data and linkable data, which could identify a person when combined other data.

Linked data	Linkable data
• Name • Date of birth • Address, e-mail address, telephone number • Account information • Personal identification numbers such as social security number, passport number and driver's license number • Property information such as vehicle identification number, property title or products purchased	• Country, state, city, postcode • Place of birth • Gender • Race • Religion • Age range (e.g. 30-40 instead of 30) • Geolocation data • Browser history or search history

Source: Infosys Consulting

- **Data monetization** – CCPA covers the 'selling' of personal information, but many of our clients have expressed a lack of clarity about what constitutes a 'sale' of data.
- **Definition of customer** – The definition of the customer has also been in question. For example, if a 'potential' customer calls a brokerage house and provides their PII information, but does not end up becoming their customer, are they covered under the CCPA mandates?

Other states crafting their own data privacy regulations should provide more clarity on their upcoming mandates.

CCPA compliance goals and data privacy stewardship

Companies have taken a range of organizational strategies to compliance. Some have assigned a chief data officer. Others have pushed it down to individual lines of business. Still others have set up new data privacy groups to carry out this mandate. Regardless of organization approach, businesses should:

- Establish a responsive customer request process.
- Develop effective customer opt-out mechanisms.
- Update all privacy notices and communicate to clients.
- Identify all partners and ensure their compliance as part of the extended enterprise.
- Ensure information technology teams have the required visibility and access to identify all personally identifiable information.

Companies will develop the heightened data privacy stewardship needed by moving through four phases.

Phase 1: Readiness assessment

Organizations need to evaluate their current state of compliance by conducting a comprehensive assessment across people, processes, governance, technology and privacy and security. This phase includes taking stock of data and looking into data management across channels, data sources, data type, frequency of collection, extent of usage, sharing and transfer policies with any third parties.

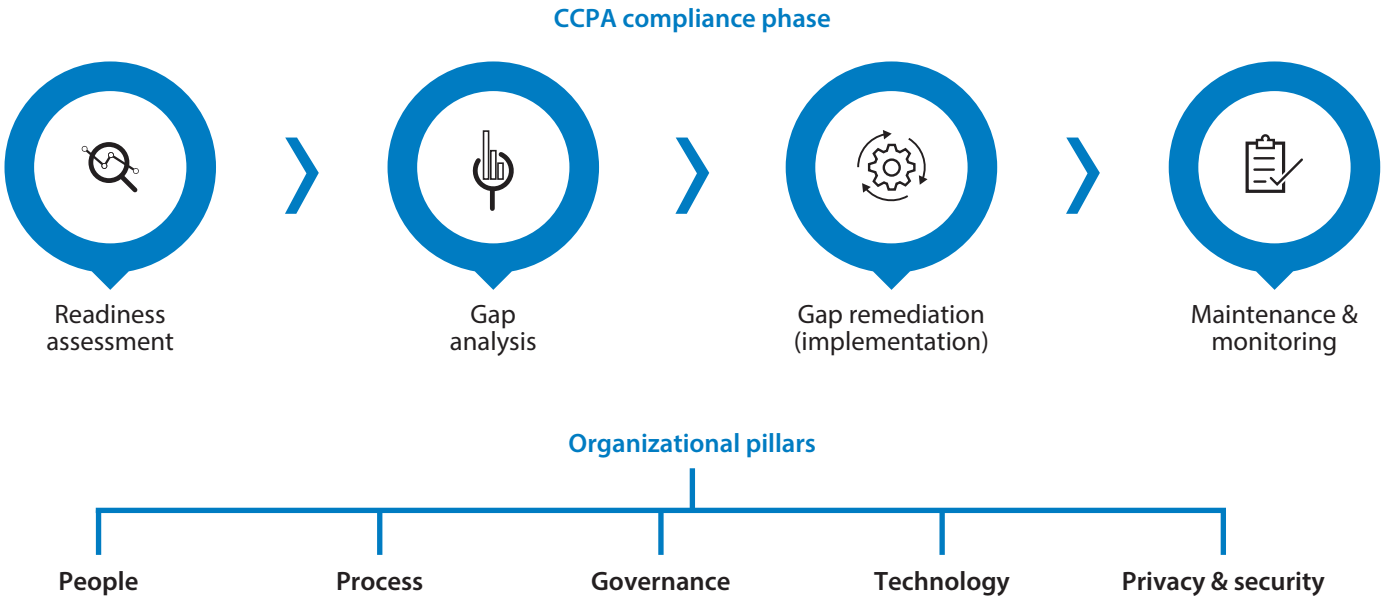
Phase 2: Gap analysis

Once data experts have assessed the current landscape within the organization, they next identify the gaps between existing compliance programs and new requirements including CCPA. Organizations can use this opportunity to review and rationalize their data management framework by performing simple activities like data minimization, data location, and data remediation.

Phase 3: Gap remediation

With gaps identified, companies and their partners modify the data management framework and align it to new privacy rules. The operations team must redefine the processes to handle all data requests and consent management. This will also address data repositories and retention policies.

Figure 4: The four phases on the way to superior data privacy stewardship.



Phase 4: Maintenance & monitoring

Privacy compliance (including CCPA) is not a one-time event but an operational state, and requires a sustained effort to monitor, periodic audit and maintain a unified view of personally identifiable data. To maintain good data privacy stewardship, companies must have a culture of respect for data privacy and leadership buy-in to support ongoing compliance.

The best data compliance roadmaps with new data privacy rules create repositories with comprehensive audit trails, retention and deletion policies.

Unlocking value by investing in data privacy

Regulators and consumer advocates will continue to demand that businesses become better stewards of the data entrusted to them.

Companies cannot address this long-term demand with a quick fix. As rules evolve and awareness grows, organizations will realize the most benefit by taking a long-term view of their data management policies and processes.

A company can even convert its compliance efforts into a pathway to build better trust with customers. The consent management mechanism required by CCPA provides a new avenue for consumer engagement and an opportunity to enhance customer experience. A superior service could be a differentiator as well as a brand-building exercise, especially in high touch industries, such as retail, marketing and advertising, which have been seeking innovative ways to enhance customer experiences.

Smart enterprises can use this opportunity to rationalize data across functions and operations that collect, store, use or transfer consumer data.

They have an opportunity to reimagine their data strategies, reduce cost and improve efficiency while meeting privacy regulations.

Business models as we know have changed forever in the post COVID-19 world. We expect data proliferation to happen on both traditional mediums and the cloud. This poses new challenges to protect and track data across the firm and with third parties. Given the July 1, 2020 deadline is fast approaching, we expect California regulators to soon be knocking on the doors of the non-compliant firms – now is the time to be ready.

References

[1] Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, David Roland-Holst, Samuel Evans, Drew Behnke et al., August 2019, Berkeley Economic Advising and Research for the California Attorney General's Office.

[2] Which states have the most data breaches? Data breaches by US state, Paul Bischoff, June 20, 2019, Comparitech.

[3] Examining Where eight US States Stand on Consumer Data Privacy Laws, Dom Nicastro, Aug. 30, 2019, CMS Wire.

[4] Three New Changes to the Revised CCPA Regulations and New CCPA Lawsuits, Philip Favro, March 24, 2020, Law.com.

[5] The 15 biggest data breaches of the 21st century, Dan Swinhoe, April 17, 2020, CSO Magazine.

[6] California attorney general's office: No delay on CCPA enforcement amid COVID-19, Joe Duball, March 23, 2020, International Association of Privacy Professionals.

[7] CCPA compliance costs projected to reach $55B, Aly McDevitt, Oct. 8, 2019, Compliance Week.

[8] Key Steps in Satisfying Your CCPA and Other Privacy Obligations, Osterman Research, December 2019.

[9] State Laws Related to Internet Privacy, National Conference of State Legislatures, Jan. 27, 2020.

Authors

Abhinav Jain

Senior Principal, Infosys Consulting

Chad Watt

Infosys Knowledge Institute

Sanjay Kumar

Senior Principal, Infosys Consulting

Senthil Kumar

Partner, Infosys Consulting

Rajesh Menon Pudukulangare

Managing Partner, Infosys Consulting

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next