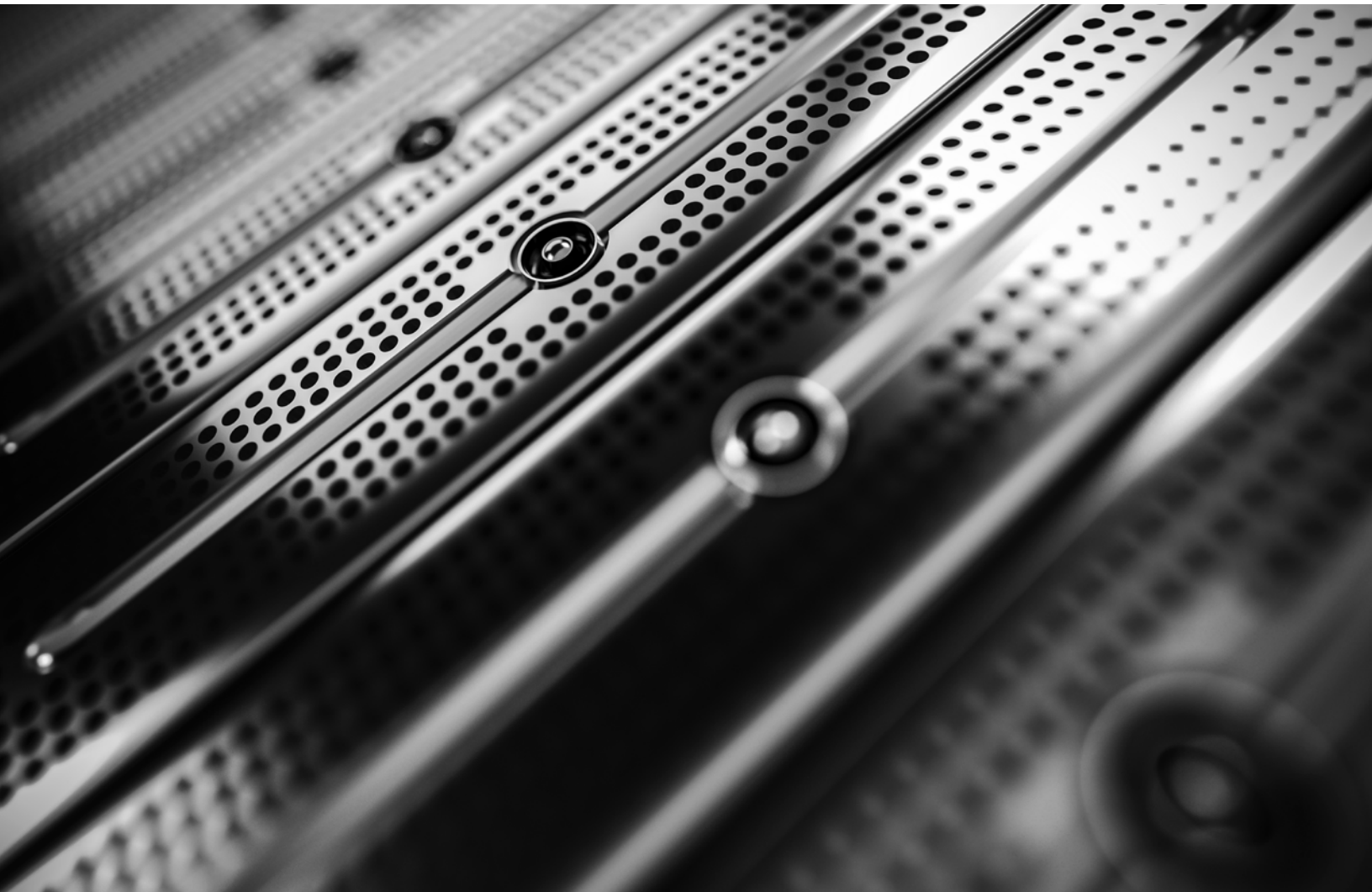
CAPCO

# GDPR LESSONS FOR CCPA COMPLIANCE

## CAPCO'S CYBERSECURITY INSIGHT SERIES



# ABSTRACT

The California Consumer Privacy Act (CCPA) fundamentally expands consumer rights and imposes requirements for covered business entities to enhance data management and protection practices, improve individual rights processes, and upgrade privacy policies. The failures of GDPR compliance offers organizations valuable insights into how they should craft their CCPA strategy.

# PRIVACY UNDER CCPA: LESSONS FROM GDPR COMPLIANCE FAILURES

A 2019 study[1] by the Pew Research Center shows that most Americans are not confident that companies would publicly admit to misusing consumers' data. Around 80 percent of Americans believe that companies will not openly admit mistakes and take responsibility if they misuse or compromise personal data. To understand this in context, it is essential to remember that the General Data Privacy Regulation (GDPR) was adopted in the European Union (EU) in 2016 to give users a say in how companies use personal consumer data. Although GDPR focused on data subjects not in the US, several American firms were also covered by the ruling due to the global nature of their businesses. Despite this, American consumers' confidence in organizations' management of their private information is low, and the market needs a seismic shift in data privacy practices.

Data privacy laws and regulations aimed at guaranteeing reliable protection for individuals as it pertains to their personal data have been evolving in recent years. The GDPR in the EU is seen as a precursor to the more recent CCPA that went into effect on January 1, 2020. A Varonis report on Global Data Risk in 2019, well past when GDPR went into effect, highlighted that 53 percent of companies surveyed found over 1,000 sensitive files exposed to all employees, and these files included data that was subject to GDPR. This lack of attention to data privacy by companies has manifested itself in significantly high monetary penalties to the tune of millions of euros.

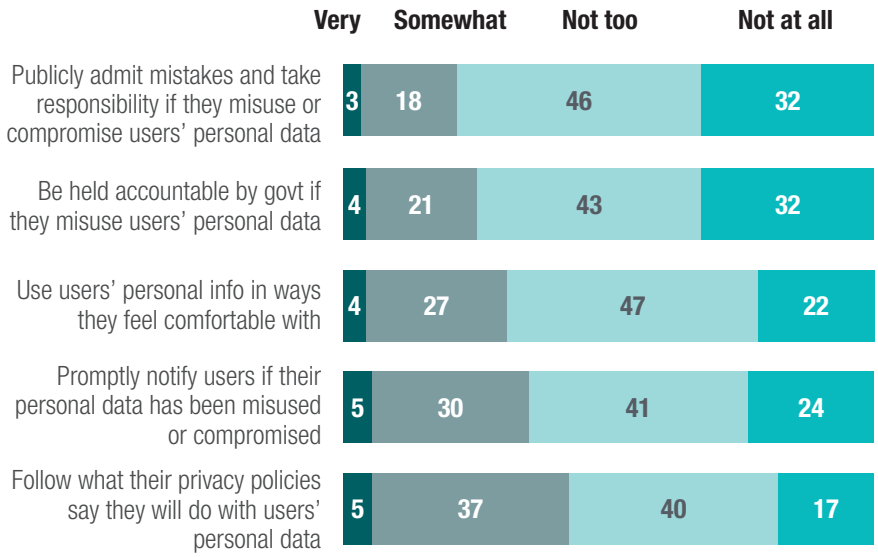
Though the CCPA differs from the GDPR in several areas, there are three critical lessons to be learned from the failures of GDPR compliance.

**53%**

*of companies found over 1,000 sensitive files exposed to all employees*

## Most Americans are not confident that companies would publicly admit to misusing consumers' data.

% of U.S. adults who say they are__confident that companies will do the following things




Note: Those who did not give an answer are not shown.

Source: Survey conducted June 3-17, 2019.

"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

**PEW RESEARCH CENTER**

Source: https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

## 1. Legal Interpretation Challenges:

As financial institutions interpret the various mandates of CCPA, it is also critical for the law to further clarify any ambiguities in the current law to avoid a sudden surge in lawsuits stemming from misinterpreted law. One such opportunity was available to the public as well as corporations via the California State Attorney General's request for comments/feedback on the law by December 2019. Our review of the CCPA reveals five key aspects that would benefit from additional clarifications from the California State:

**A. Technical limitations:**

Consider a historical customer who no longer uses the products/services of an organization. If this customer exercises their right to deletion, the organization might face challenges in the deletion of historical data stored on tape or WORM (write once, read many) storage. While laws such as the 23 NYCRR 500 allow for organizations to claim technical non-feasibility in deleting stale data, the CCPA provides no recourse for instances of technical non-feasibility or associated prohibitive costs.

**B. Statute of limitations for data rights:**

As organizations build their infrastructure to respond to consumer right to know or right to deletion, the state of California may need to consider a statute of limitations for such requests. If a consumer requests for access to data from beyond a reasonable timeframe, the cost, and challenges of discovering such old datasets might render this exercise impossible. California must define a statute of limitations for data rights, potentially contingent on costs to address the request.

**C. Reasonable need:**

The current law allows organizations several exceptional scenarios where compliance with a consumer's request for data deletion is not mandatory. Consider a consumer who realizes they have been the victim of identity theft. They request the organization that they suspect as the source of the breach to delete their data in adherence to the CCPA. However, the organization can justify a reasonable need to retain this data by indicating the consumer's data is required to debug code and identify and repair errors that impair intended functionality. In such cases, consumers would benefit from a definition of quantitative thresholds that organizations can use as a guide to justify a consumer request denial.

**D. Cost of personal information:**

CCPA does not allow organizations to discriminate against a consumer because the consumer exercised any of the consumer's rights under the law. The law also posits that a business may offer a different price of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data. However, the law is silent on how the business evaluates the cost of the consumer's personal information. This ambiguity will pose challenges in how organizations quantify the value of personal information and how California can govern this.

**E. Accountability for confidentiality risk:**

Organizations today work with several third parties to offer products and services to consumers. While CCPA is clear on the organization's responsibility for ensuring the privacy of its consumer data, it does not provide guidance on the responsibility of covered entities as it pertains to risks inherent to transmitting personal data over networks external to the organization.

## 2. Limiting Data Scope:

While planning their strategy and plan to comply with GDPR, several organizations first focused on segmenting customer data for EU data subjects. Implementing policies, processes, and solutions for GDPR compliance for only a limited scope has proven challenging for global organizations over time. With the advent of consumer data rights in the US as posited by the CCPA, organizations are making similar decisions. However, CCPA is the first of its kind, and draft legislation in several other states closely mirror it. The US is also considering the introduction of comprehensive federal legislation called COPRA (Consumer Online Privacy Rights Act) in 2020. Given that federal, state, and local levels, are contemplating privacy initiatives, organizations, especially those with presence in multiple US states and/or international presence, must consider an evaluation of solutions for all customers and make small adaptations for local mandates.

## 3. Insufficient Fund Allocation:

An independent study (Source: https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf) by the Ponemon Institute in 2017 revealed that organizations were not spending enough on core compliance activities. This was a surprising finding when seen in the context that the median cost of compliance with data privacy laws was $3.9 Million, and the median cost of non-compliance was a whopping $13.9 Million. The case for enforcing a comprehensive and strong privacy program has been proven to outweigh the costs associated with non-compliance. However, as in the case of the GDPR, organizations have been slow to invest in complying with the CCPA. While some organizations have focused on building small teams to field data rights requests from consumers, others are still contending with the challenge of identifying what consumers' personal information they possess and where this is stored. Given that the CCPA went live on January 1, 2020, it is imperative that organizations build their business case, and invest appropriately in data discovery exercises, drafting privacy policies and processes, and exploring ways to automate privacy management.

## Capco's Key To CCPA Compliance

Our advisory practice works with financial institutions to craft suitable CCPA and broader data privacy strategies. We recommend attention to five key tenets as financial institutions build comprehensive data privacy programs:

1. Obtain legal counsel's opinion as to what laws and regulations apply to your organization

2. Ensure that your incident response procedures include communication procedures to notify impacted parties in the event of a data breach within timeframes mandated by applicable laws

3. Accord highest priority to data discovery exercises to identify what consumer personal information your organization uses, stores, or transfers to third parties; constantly review and challenge controls around non-public information

4. Develop a comprehensive approach to data classification and data lifecycle management to drive transparency on data element lineage and usage

5. Combining the NIST CSF framework with DFS 500 requirements and privacy requirements of CCPA should position you to follow the current multitude of regulatory issuances requirements around the protection of NPI and establishment of a viable cybersecurity program

## GET IN TOUCH


**Jayadevan Vijayakrishnan**
Principal Consultant
jayadevan.vijayakrishnan@capco.com

**Sandeep Vishnu**
Partner
sandeep.vishnu@capco.com

**Julien Bonnay**
Partner
julien.bonnay@capco.com


## ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

## WORLDWIDE OFFICES

### APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

### EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

### NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

### SOUTH AMERICA
São Paulo

**WWW.CAPCO.COM**



CAPCO
THE FUTURE. NOW.