The Brave New World of Data Privacy: Benchmarking Corporate Compliance

Compliance and Ethics

Technology, Privacy, and eCommerce

Cheat Sheet

- **California Consumer Privacy Act (CCPA).** This is the first US statute to impose standard requirements on most businesses to report privacy practices in a corporate privacy notice.
- **Access requests.** The “right to access” or the “right to know” allows consumers to request certain information about their person.
- **Deletion requests.** The “right to be forgotten” or “right to deletion” allows consumers to request that businesses erase the personal data that it has collected from the individual.
- **Corporate response.** Most companies updated their privacy notices, including to include information about consumer rights to request or delete their data.

When many of us went to law school, there was no such thing as a class on data privacy. Indeed, the term “data privacy law” meant nothing to most law students or law professors. In the past 20 years, data breaches and privacy-related scandals have dominated the headlines. Given the widespread media attention on privacy, some might argue that passage of new laws and regulations was inevitable.

In 2018, the EU General Data Protection Regulation (GDPR) — a sweeping modernization of European privacy laws — went into effect. Two years later, in 2020, the California Consumer Privacy Act (CCPA) — the first general data privacy regime in the United States — was implemented.

When you combine weekly headlines about data privacy with sweeping new laws and regulations, it's not hard to understand why data privacy is routinely ranked as one of the top 10 risks by boards, chief legal officers, and the C-suite alike.

While the CCPA went into effect on Jan. 1, 2020, it did not become fully enforceable until July 1, 2020. When we passed the one-year anniversary of the CCPA becoming law, it provided an opportunity to assess the impact of the CCPA on privacy programs and to begin to benchmark against emerging industry standards. To that end, we reviewed the privacy policies of all Fortune 500 companies to identify emerging trends and patterns.

Background on the CCPA

The CCPA applies to for-profit organizations that fulfill one of the following criteria:

- Have an annual gross revenue in excess of US$25 million;
- Collect, buy, receive, sell, or share the personal information of 50,000 or more California-resident consumers, households, or devices; or
- Derive 50 percent or more of their annual revenue from selling consumers' personal information.

The CCPA revolutionized data privacy in the United States in several ways. It was the first US statute to impose standard requirements on most businesses to report privacy practices in a corporate privacy notice.

It was also the first US statute to require most businesses (i.e., those outside of the financial and health sector) to provide consumers with the right to access their personal information, request the deletion of their personal information, and request that their information not be sold to third parties.

Privacy notices

The CCPA and the regulations implementing the CCPA require that every business subject to it create a privacy notice that contains the following main provisions:

Required Privacy Notice Disclosure
1. Ability to opt-out of sale of information (to the extent a company sells personal information as defined under the act)
2. Access rights of individuals (an explanation of rights and instructions for how to exercise those rights)
3. Categories of personal information collected in the preceding 12 months
4. Categories of personal information shared with services providers or third parties for a business purpose in the preceding 12 months
5. Categories of personal information sold in the preceding 12 months
6. Contact information (including in some cases a toll-free telephone number or online form) for submitting requests
7. Date the privacy notice was last updated
8. Erasure rights of individuals (an explanation of rights and instructions for how to exercise those rights)
9. Metrics concerning the quantity of requests received from consumers (only applies to businesses that process over 10 million California consumers' personal data)

Required Privacy Notice Disclosure
10. Process for how an authorized agent can make a request on a consumer's behalf
11. Purpose for which information was collected
12. Sources from which personal information was collected
13. Statement regarding the right of consumers not to be discriminated against for exercising their rights
14. Statement regarding the sale of personal information of consumers under 16 years of age
15. Types of third-party recipients of information

Approximately 71.8 percent of the companies within the Fortune 500 updated their privacy notices to account for the CCPA. There was, however, significant divergence between the rates at which companies in different industry sectors updated their privacy notices.

While all the members of some industries (e.g., software, retail, and insurance) updated their privacy notices, few members of other industries (e.g., architecture and engineering, electricity generation, and certain manufacturing areas) did so.

Whether a company has updated its privacy notice for the CCPA is not necessarily indicative of whether the company is, or is not, complying with the CCPA. For example, a company that has not updated its privacy notice for the CCPA, but is not subject to the statute (i.e., does not do business in California, or is governed by federal privacy statutes that are exempted from the CCPA such as the Gramm Leach Bliley Act or the Fair Credit Reporting Act), would not be out of compliance.

Access requests and requests to know

The "right to access" or the "right to know" refers to the ability of a person to request to receive certain information about that person, including a copy of personal information that a company has collected about that individual.

The right to access is not unique to the CCPA and can be found in other sectoral laws within the United States, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA). However, prior to the enactment of the CCPA, there was no US statute that granted individuals the right to request most businesses to provide the personal information that the business held about them.

Most companies (80.6 percent) now provide individuals — or at least California residents — with the ability to request access to their personal information. Companies that also hold personal data of 10 million or more California residents in a calendar year — are required by CCPA regulations to disclose how many access requests they receive annually.

> Most companies (80.6 percent) now provide individuals — or at least California residents — with the ability to request access to their personal information.

While a relatively small number of businesses reported these metrics (only 52 companies within the Fortune 500), those companies collectively reported receiving around 4.7 million access requests.

Access requests were not evenly distributed among companies. Four companies in the technology sector collectively accounted for 4.59 million access requests — or 97 percent of all the access requests reported. Indeed, just one company received more access requests (2,951,350) than the

other 51 companies *combined.*

When non-technology companies are removed as outliers, the number of access requests received by companies becomes far more modest. The remaining companies received an average of 5,338 access requests, and the quantity of access requests received was highly industry dependent:

Industry	Average Quantity of Access Requests	Percentage of Access Requests Denied
Banking and financial services	689	40.3%
Broadcasting and media	1,323	21.1%
Healthcare and medical	3,767	Not reported
Insurance (life and health)	20	45.9%
Internet and web services	150	0%
Manufacturing	55	0%
Manufacturing (motor vehicle)	634	23%
Manufacturing (paper products)	27	0%
Motor vehicle and parts dealers	104	16.4%
Pharmaceuticals	3	66%
Professional services	47	18.1%
Restaurants	498	32.5%
Retail	14,998	21.3%
Telecommunications	350	13.1%

Deletion requests

The “right to be forgotten” or “right to deletion” refers to the ability of a consumer to request that a business erase the personal data that it has collected from the individual.

Although the CCPA indicates that consumers “have the right to request that a business delete any personal information about the consumer that the business has collected from the consumer,” that right is not absolute and subject to various exceptions. For example a business can refuse a deletion request on the following grounds:

1. **Complete a transaction.** If personal information is necessary for a business to complete a transaction with the consumer, to provide a product or services to the consumer, or to further the ongoing relationship with the consumer it does not need to be deleted.
2. **Security and integrity.** If personal information is necessary for a business to provide security and integrity it does not need to be deleted.
3. **Repair errors.** If personal information is necessary to “[d]ebug to identify and repair errors that impair existing intended functionality” it does not need to be deleted. (Neither the CCPA, nor the regulations implementing the CCPA, explain what use-cases may fall under this exception.)
4. **Free speech.** If personal information is necessary to exercise the free speech of the business, or the free speech of another consumer, it does not need to be deleted.
5. **Exercise legal right.** If personal information is necessary for the business to “exercise another right provided for by law” it does not need to be deleted.
6. **Research.** If personal information is reasonably necessary for the business to engage in research-whether that research is public, peer-reviewed scientific, historical, or statistical-it does not need to be deleted.
7. **Internal uses aligned with consumer expectations.** If personal information will have

"solely internal uses" for the business, and if those uses are "reasonably aligned with the expectations of the consumer it does not need to be deleted. (There is uncertainty as to whether a California court would evaluate the expectations of the consumer using a subjective standard or an objective standard.)

8. **Internal uses aligned with the context of collection.** If personal information will be used "internally" and in a manner that is "compatible" with the "context in which the consumer provided the information," it does not need to be deleted. (Note that this exception was removed by the CPRA and, as a result, will be unavailable to businesses beginning Jan. 1, 2023.)
9. **Comply with legal obligations.** If personal information is necessary for the business to comply with a legal obligation (e.g., a statute that requires that the business maintain documentation relating to the consumer), it does not need to be deleted.

As with access rights, most companies (78.8 percent) provide individuals — or at least California residents — with the ability to request the deletion of their personal information. Those companies that reported the quantity of deletion requests that they received collectively accounted for 4.3 million deletion requests (about 8.5 percent fewer than the collective access requests).

As with access requests, a handful of companies skew the overall average. Four companies accounted for more than four million requests — or 94 percent of the total volume. When those companies are removed as outliers, the remaining companies received, on average, 5,141 requests. Again the quantity of deletion requests was highly dependent on industry.

Industry	Average Quantity of Deletion Requests	Percentage of Deletion Requests Denied
Banking and financial services	322	67.3%
Broadcasting and media	2655	26.2%
Healthcare and medical	12,395	0.0%
Insurance (life and health)	13	57.9%
Internet and web services	62	0.0%
Manufacturing	250	0.0%
Manufacturing (motor vehicle)	4,494	27.2%
Manufacturing (paper products)	42	4.8%
Motor vehicle and parts dealers	116	19.0%
Pharmaceuticals	26	26.9%
Professional services	48	21.1%
Restaurants	2,659	52.4%
Retail	44,704	4.3%
Telecommunications	1,140	10.4%

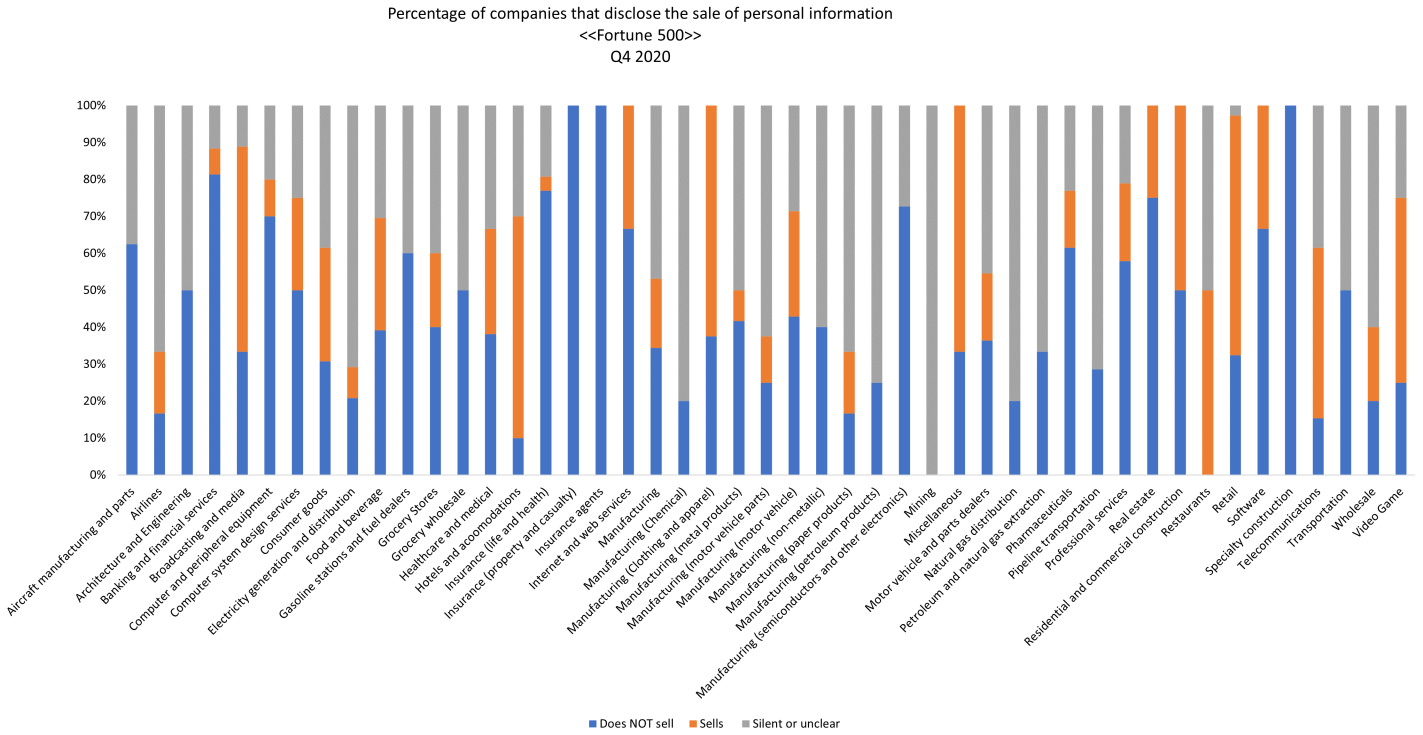
Do not sell requests

The CCPA requires businesses that sell personal information to notify consumers of the sale, include a list within their privacy notice of the categories of information that are sold, explain that consumers have a right to opt-out of such sales, and provide a clear and conspicuous link on their homepage titled "Do Not Sell My Personal Information" that takes the consumer to a mechanism that permits them to exercise their opt-out right.

If a company does not sell a consumer's personal information, most of the above requirements do not apply and the company can simply disclose in its privacy notice that it does not sell personal

information.

Only a relatively small minority of companies (21 percent) disclosed that they sold personal information. As with almost every aspect of privacy practices, and as the following graph shows, the decision to sell personal information tends to differ significantly among industries:



While relatively few companies offer a “do not sell” option, those that did received massive quantities of requests from consumers. The average quantity of Do Not Sell requests received by a company that sold data was 52,500. The following provides a breakdown of the average quantity of Do Not Sell requests received by industry (this includes data from only those companies that provide Do Not Sell links on their homepage):

Industry	Average Quantity of Opt-Out Requests	Percentage of Opt-Out Requests Denied
Broadcasting and media	12,742	0.4%
Healthcare and medical	306	0.0%
Internet and web services	7,143	0.0%
Manufacturing	463	0.0%
Manufacturing (motor vehicle)	31,946	0.0%
Manufacturing (paper products)	3,511	0.0%
Motor vehicle and parts dealers	3,447	0.0%
Professional services	4,526	0.0%
Retail	106,134	1.7%

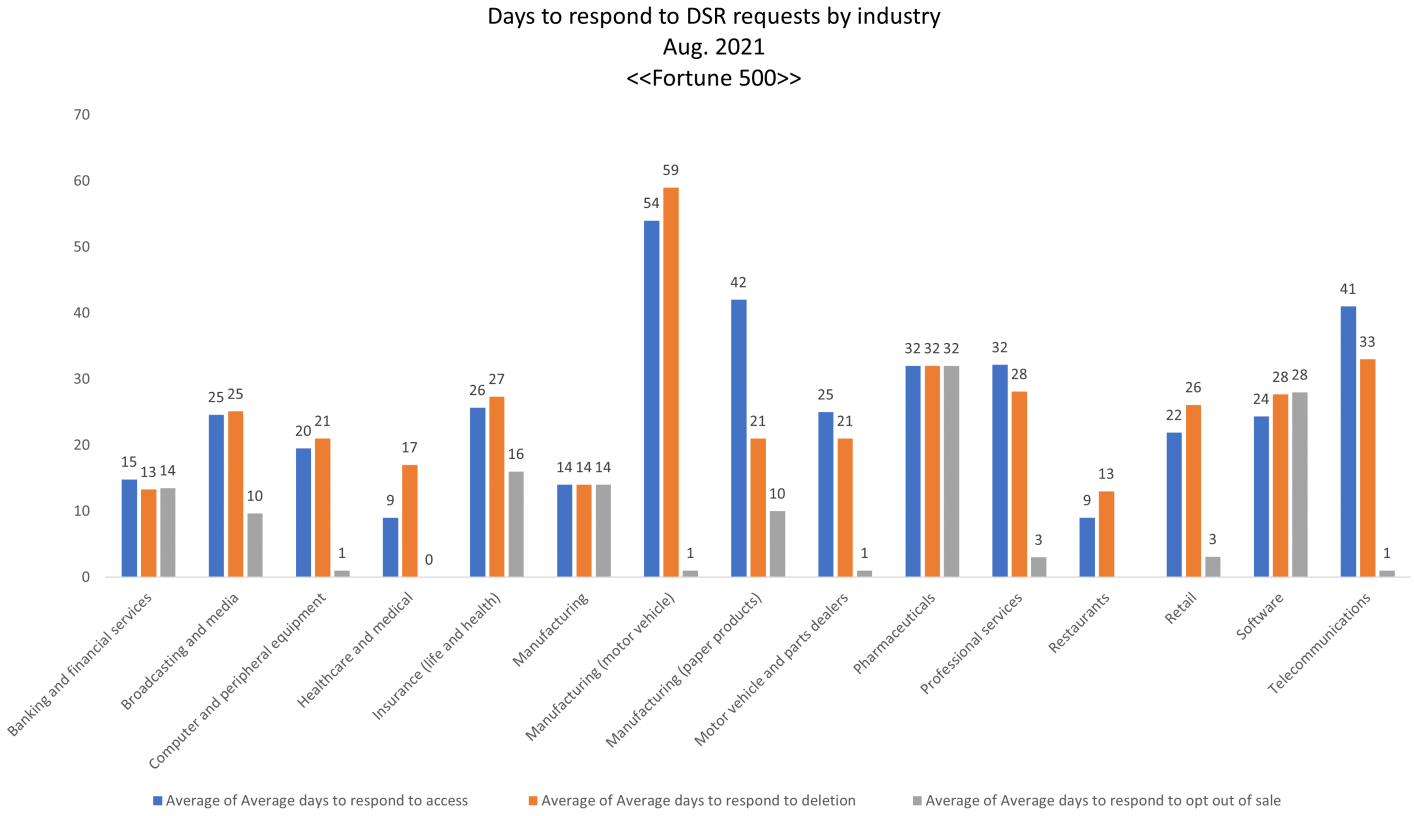
Note that the banking and financial service, insurance (life and health), professional services, and restaurant industry groups are not included in this chart as members of the industry group, which reported DSR metrics, also included a Do Not Sell My Personal Information Link on their homepage. While not reported here, it is worth mentioning that some companies within these industry groups did report receiving opt-out of sale requests. They have been excluded here as outliers.

Data request response timing

The CCPA requires that a business typically respond to an access or a deletion request within “45 days of receiving a verifiable consumer request,” but can extend the timing up to an additional 45 days. Businesses have 15 business days to respond to a request that a consumer’s personal information not be sold.

In practice, some companies were able to address requests in a handful of days, while many others took over a month (or exceeded the time permitted for normal requests under the CCPA). Overall companies reported an average/median of 22 days to respond to access and deletion requests, and six days to respond to DNS requests. That said, the number of days reported differed significantly between industries.

Note that the CCPA permits businesses to report either the median or average number of days to respond.



Note that the category of “industry and web services” was removed as certain industry members did not report an average or median number of days.

Lessons learned

Benchmarking can be a useful tool. There is a natural tendency for in-house counsel to want to verify that their company is not out of step with the industry. Our data analysis and benchmarking have identified the following lessons for in-house counsel:

- **Companies are responding to the CCPA and other data privacy laws.** While companies appear to be making different choices regarding some aspects of the CCPA, most companies updated their privacy notices to reflect the new regulatory environment brought on by the

CCPA, including by referencing consumer rights to request access to their personal information or deleting their personal information.

- **Current data metrics provide insights for future planning.** Companies want to know what their future request profile will look like to plan for potential increases in request volume. While the best predictor is the company's own request metrics, the data provides helpful snapshots for potential future request ranges, as well as consumers' experience and expectations regarding response time-periods.

- **Universal industry standards have not emerged in many areas.** There is arguably more divergence than convergence when it comes to specific privacy practices. There also appears to be divergence in terms of the types of rights that consumers are exercising vis-à-vis different companies in different industries, as well as different companies within the same industry.

- **Data subject requests are overwhelmingly focused on opting-out of the sale of personal information.** Although the CCPA conferred upon Californians the ability to request access to their personal information, request the deletion of their personal information, and request to opt-out of the sale of their personal information, companies that offered all three rights received opt-out of sale requests in far greater numbers than requests relating to the other rights.

- **Exemptions influence behavior.** Perhaps not surprisingly, the percentage of requests denied tend to be significantly greater in industries that are exempt from the CCPA (e.g., GLBA-regulated or HIPAA-regulated). Presumably, the denial rate reflects the practice of exempt entities denying (in part or in whole) requests for which they are not required to comply.

Ben Kimberley

Senior Director, Chief Counsel: Ethics, Compliance & Privacy

The Clorox Company

Ben Kimberley is Senior Director, Chief Counsel: Ethics, Compliance & Privacy for The Clorox Company. Before Clorox, he was an attorney at the international law firm of Winston & Strawn LLP. He holds a BA from Northwestern University and a JD from the University of California, Berkeley.

David Zetoony

Shareholder

Greenberg Traurig

David Zetoony, co-chair of the firm's US Data, Privacy, and Cybersecurity Practice, focuses on

helping businesses navigate data privacy and cybersecurity laws from a practical standpoint. He is based on Denver, Colorado.