DATAGRAIL®

2021 CONSUMER PRIVACY REPORT

The State of CCPA

Benchmarking CCPA Trends Across Consumer (B2C) Brands

www.datagrail.io

The State of CCPA

2020 was the year that the California Consumer Privacy Act (CCPA) went into effect, giving Californian consumers—for the first time—the right to take more control over their data.

And though the Act is still in its first year, already millions of Californian consumers started to exercise their CCPA rights: to access their data, to delete their data or to stop the sale of their data to a third party. While it's true many consumers are still learning how to exercise their CCPA rights, we expect the trend of consumers taking control of their data to continue.

At DataGrail, we're in the unique position of fulfilling data subject requests (DSRs) for millions of consumers, which gives us unique insights into the number of requests a company can anticipate. We analyzed DSRs processed throughout 2020 across our business-to-consumer (B2C) customers, resulting in a powerful benchmark of what to expect as the CCPA and other privacy regulations start to have a larger impact on how business is done.

This research will help organizations confidently enter the era and help them understand where they stand relative to their peers in the space. It's early, but we hope these learnings help consumer businesses better prepare for the CCPA, and continuous changes to the regulatory landscape (such as the upcoming CPRA, which takes effect in 2023).

We reference three types of consumer rights requests that are part of the CCPA, often referred to as data subject requests (DSR):

The right to know the data collected. We refer to these as "access requests" or use the common acronym DSAR.

The right to deletion. We refer to these as "deletion requests."

The right to say no. We refer to these as "do not sell requests" (DNS).

2020 Highlights

Consumers are most likely to opt-out of their data being sold to a third party by submitting **do-not-sell (DNS) requests (46%)**.

In 2020, consumers were twice as likely to exercise their right to opt out of their data being sold, versus performing an "**access request.**"

1/3 of DSRs were deletion requests in 2020, proving consumers embraced their right to delete their data.

B2C companies received approximately **137 DSRs per million identities in 2020**, however the number of DSRs a company receives varies wildly depending on their privacy practices.

- Organizations who use a form and CAPTCHA tend to have **significantly less unverified requests** than organizations that ask customers to send an email.
- Organizations who update their privacy policy frequently tend to see a **surge of requests after an update**.

Lack of end-to-end privacy automation will cost you—B2C companies that manually process requests should expect to incur costs around **$190K per million identities** to fulfill requests.

"Hello, anyone there?" **Nearly half of all DSRs go unverified**, which means the requester did not follow through in proving their identity. Many unverified requests were actually veritable spam.

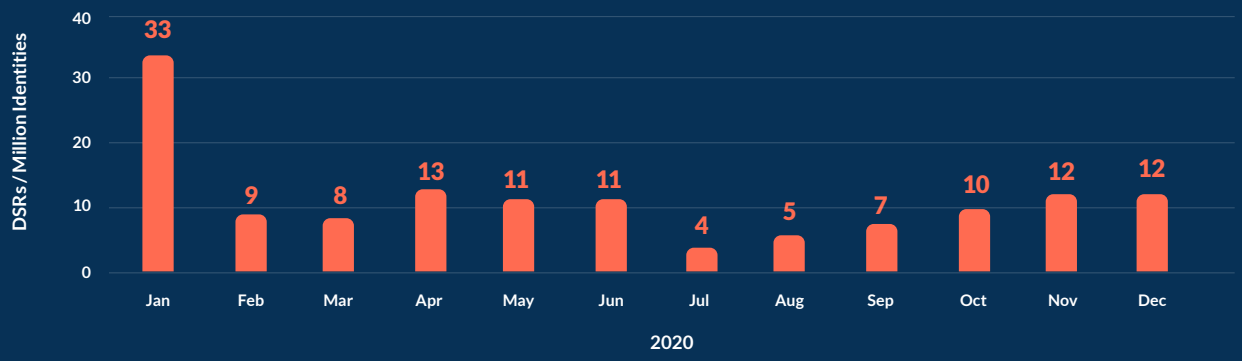
Note: Our dataset includes companies of all sizes, from startup direct-to-consumer sites to publicly traded household names. To normalize the data across different company sizes, we measure DSRs per one million identities. For example, the data shows that on average, businesses are getting about 11 DSRs **per one million identities** each month. So if an organization has 3 million identities, it can expect 33 DSRs per month.

What do we mean by "identities"? When we talk about a "identity" in the context of personal data that lives in an organization's apps and infrastructure, we mean the information associated with a unique customer. For example, a single identity accounts for a person's data across multiple systems at an organization.

Total Volume of Data Subject Requests (DSRs)

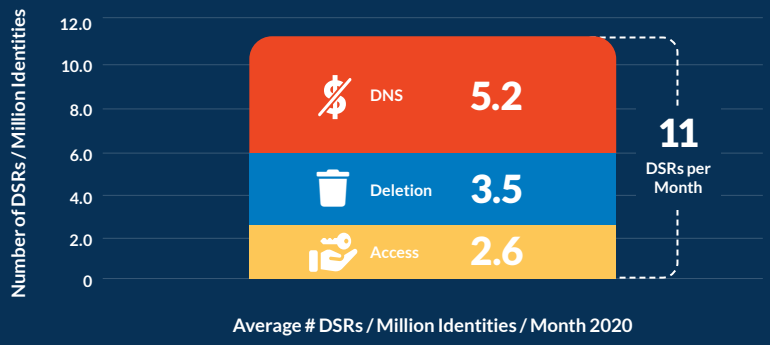
In January 2020, we saw a big bump in the number of DSRs submitted across our customer base, which correlated with customers updating privacy policies to comply with the CCPA. The CCPA Trends Report we published in June suggested that B2C brands should expect approximately 13 DSRs per month per million identities. However, when we look at the data across the entire calendar year, the number stabilizes around 11 DSRs per month per million identities (Figure 2). In total, the average B2C company received 137 DSRs per million identities in 2020.

Figure 1. Monthly DSRs Per Million Identities in 2020



Gartner data shows businesses that manually process data subject requests on average spend $1,406 per request. At this rate, B2C organizations who manually processed DSRs, spent approximately $192,000 per million identities in 2020 to process and fulfill data subject requests. In Figure 2 we see the average number of DNS requests stabilize around five requests per million identities. DSARs and deletion requests each sit around three requests per million identities.

Figure 2. DSRs by Type in 2020



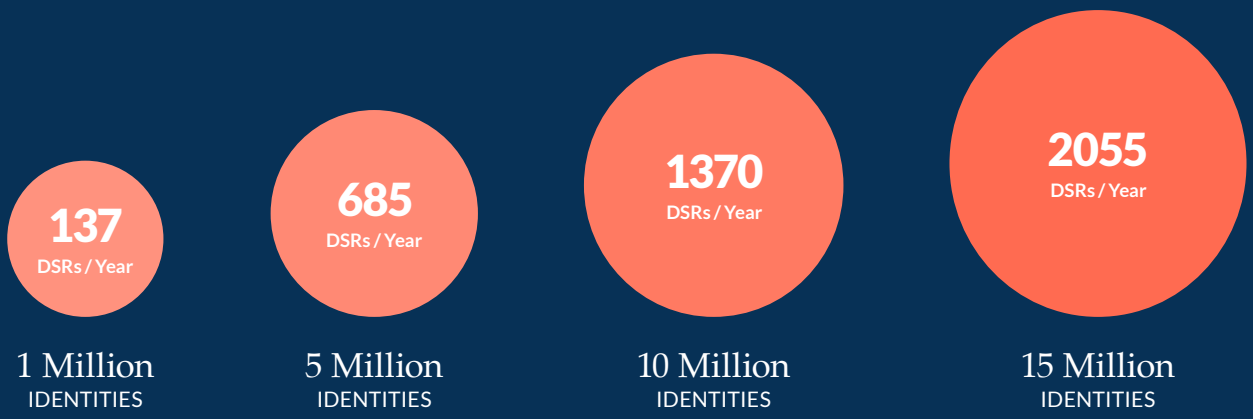
> "Organizations who manually processed DSRs, spent approximately $192,000 per million identities in 2020 to process and fulfill data subject requests"

This data is useful for extrapolating out to an industry average, as seen in Figure 3. As an example, a company with 8 million consumer identities should expect just over 1,000 DSRs per year. However, within the industry average, we saw some brands that trended much higher or lower than the average.

It's hard to pinpoint exactly what triggers more DSRs, but it's likely a combination of factors:

1. Requesting that consumers submit requests via email vs. using a form. Email requests typically result in more spam requests.
2. Sending out frequent privacy policy updates
3. Frequently sending email campaigns that aren't relevant to the customer's interests

Figure 3. Benchmarking the number of DSRs for Consumer Brands 2020

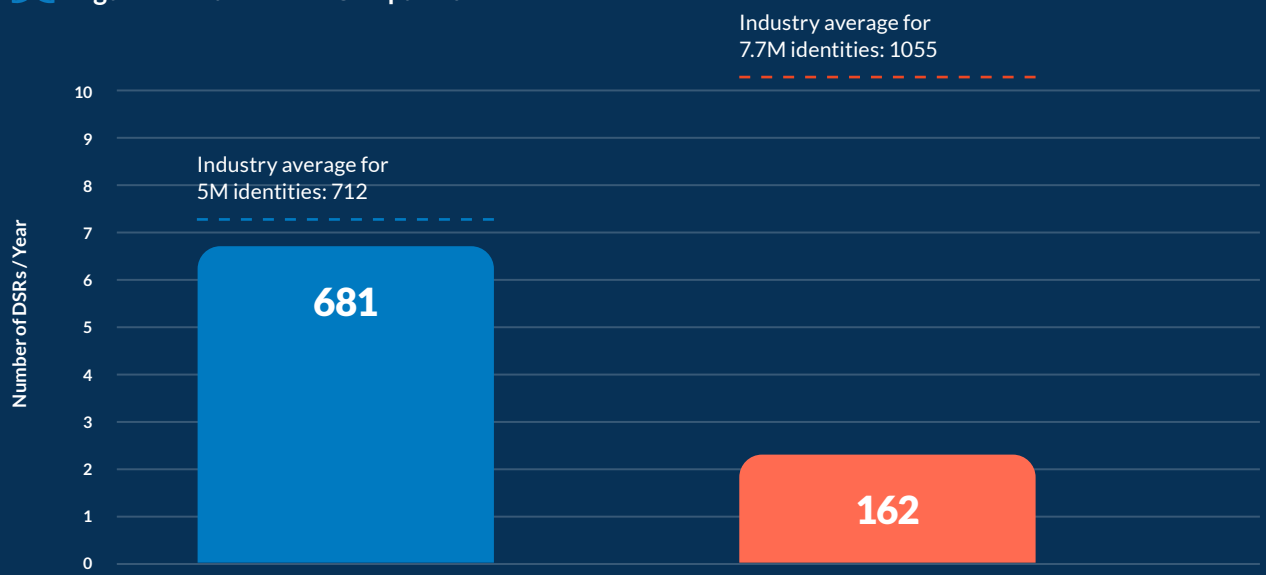


Note: A single "identity" would be a unique person's data within the apps and infrastructure at an organization.

A Tale of Two Companies

Within the industry average, we saw wild variations. As an example, two retail customers with a similar number of consumer identities saw drastically different volumes of requests. This difference is likely based on how the two companies accept data requests, how often they update their privacy policies, and the volume of marketing email campaigns they send. **Company A** received just under the industry average, whereas **Company B** received one tenth of the industry average. The difference can likely be attributed to the way company A requires consumers to submit DSRs. Rather than using a webform, it asks consumer to submit requests via email, which can trigger more spam requests.

Figure 4. A Tale of Two Companies



COMPANY A

Industry: E-commerce
Number of Identities: 5.2M
Number of DSRs / Year: 681
Industry average for 5M identities: 712

COMPANY B

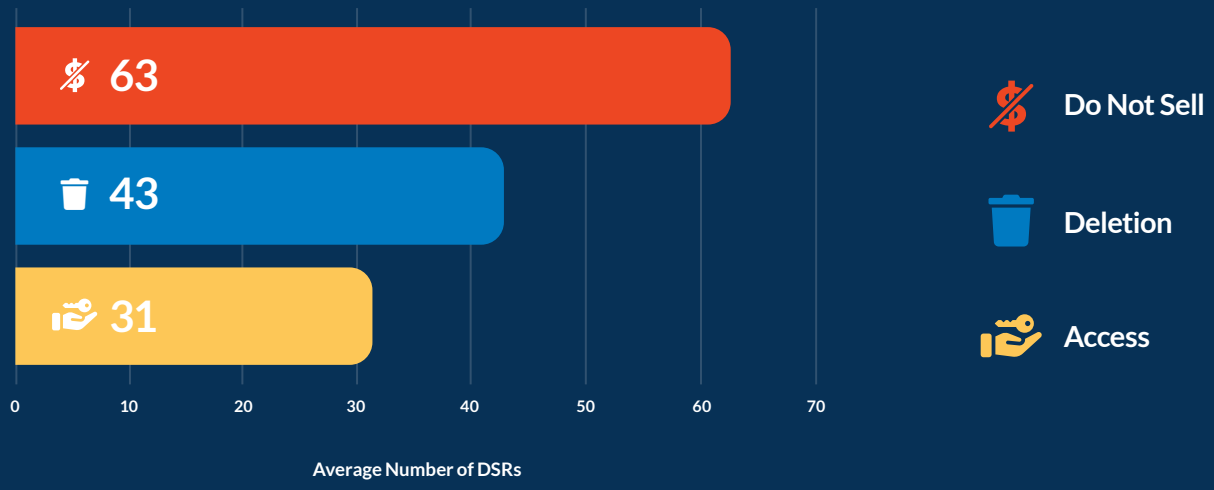
Industry: Retail
Number of Identities: 7.7M
Number of DSRs / Year: 162
Industry average for 7.7M identities: 1055

Requests by Type: Access (DSAR), Deletion, Do-Not-Sell

In Figure 5, we see do-not-sell (DNS) requests are still the most popular type of requests submitted by consumers in 2020, with the average B2C companies receiving 63 DNS requests per million identities. This is likely due to:

1. Many websites include a pop-up giving consumers the ability to opt out of their data being sold to a third party.
2. Consumers are increasingly aware of how their data is used online, and have more aggressively sought out ways to limit their data being sold.

Figure 5. Average Number of DSRs / Million Identities 2020, by Type



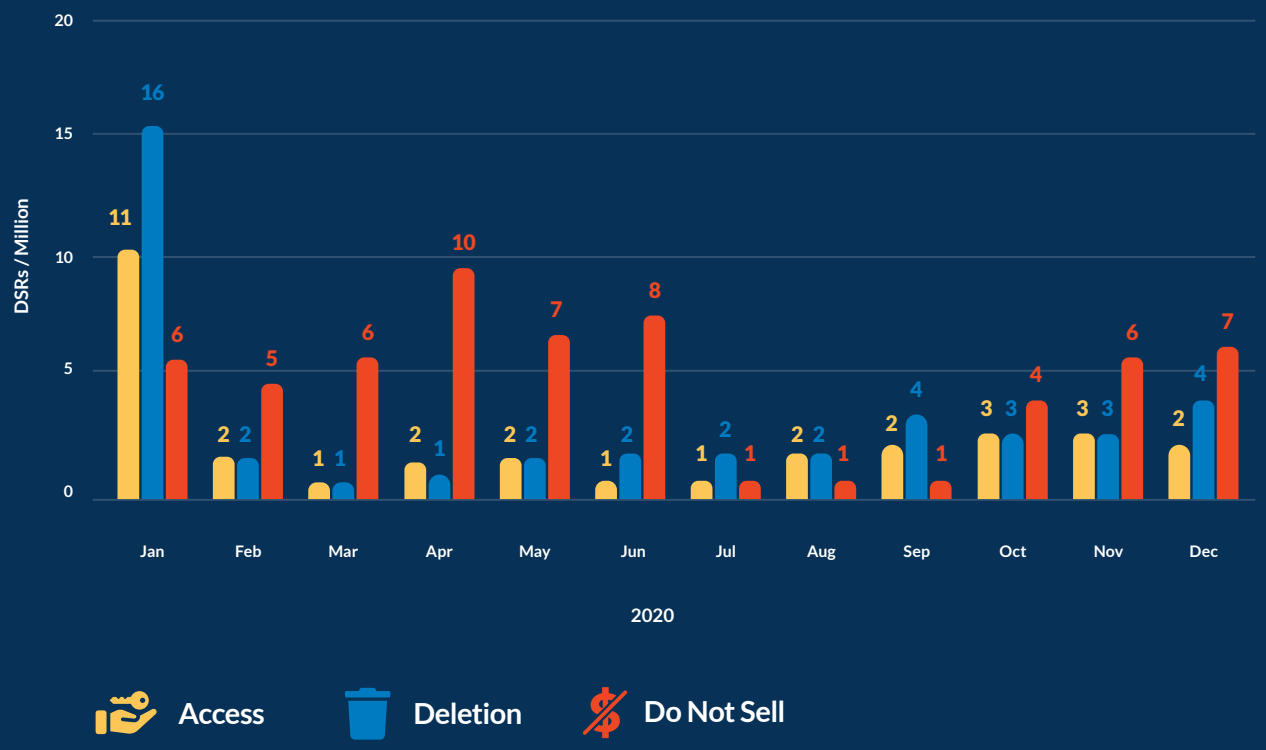
TIPS TO REDUCE DSRS

1. **Ask consumers to fill out a form to make a DSR.** DSRs sent via email typically result in more spam
2. **Update your privacy policy sparingly**
3. **Send targeted emails** and avoid sending emails that aren't relevant to the customer's interests

In fact, consumers are twice as likely to exercise their right to opt-out versus requesting access to the personal data a company has stored on them.

Tracking DSRs over time, we see that the number of requests fluctuates month to month, with the summer months coming in with the fewest requests when compared to other months of the year. In June, we saw a spike in deletion requests, but it's unclear as to why. One hypothesis is that many organizations refreshed their privacy policies in advance of the July 1st, 2020 CCPA enforcement date, triggering another round of deletion requests.

Figure 6. Access, Deletion and DNS Requests / Million Identities 2020



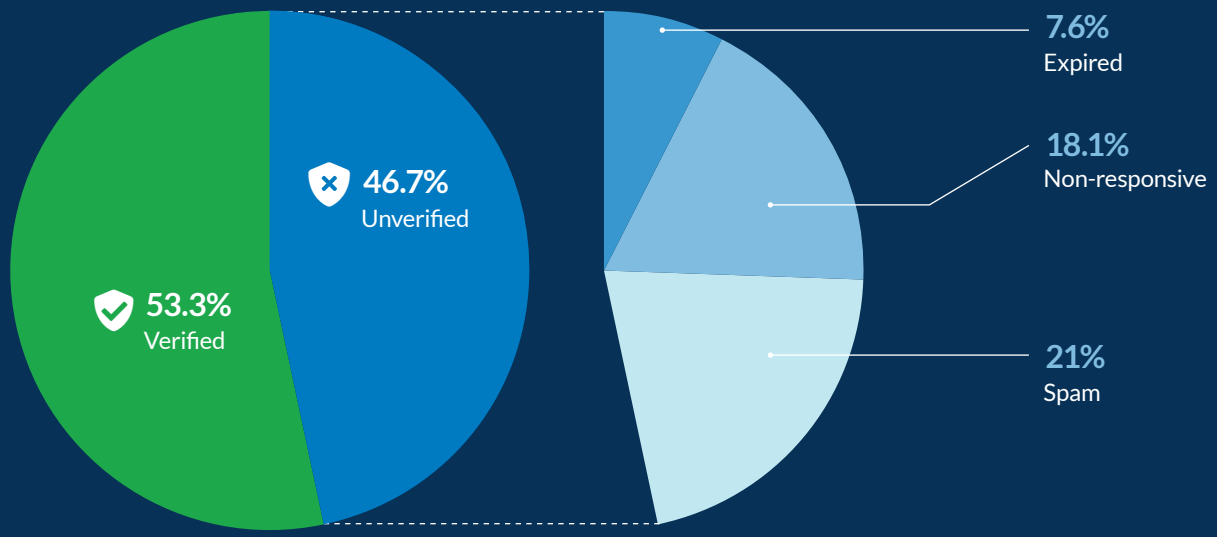
Data Subject Requests Verification

Fraud and spam are top concerns for organizations when they start to consider how to best process DSRs. To ensure no data ends up in the wrong hands, the CCPA requires that businesses use various methods to verify and authenticate the person is who they claim to be. DataGrail's Smart Verification technology uses existing data associated with the individual's identity, such as purchase history or user behaviors (e.g. games played, purchases, or products viewed) to securely validate the individual's identity. This is a preferred method, rather than asking a consumer to submit more personal data (like a government ID), which goes against the spirit of CCPA.

With Smart Verification, we were able to see that nearly 50% of DSRs went unverified in 2020, and of that most unverified requests are spam. Upon closer inspection, we found that the number of unverified requests changes dramatically depending on the customer's intake method for DSRs. **Organizations who use a form and have a CAPTCHA tend to have significantly less unverified requests than organizations that ask customers to make a request via email.**

> "The number of unverified requests changes dramatically depending on the customer's intake method for DSRs."

Figure 7. Verified vs. Unverified CCPA Requests Breakdown 2020



> "Nearly 50% of DSRs went unverified in 2020"

Note: In this graphic we're only looking at access (DSAR) and deletion requests, as Do Not Sell requests do not require the same level of verification.

Conclusion

Looking back on 2020 we see that DataGrail's mid-year predictions tracked closely to where we ended the year.

DSRs are stabilizing around 11 DSRS per million identities each month, with DNS being the most popular request. A lack of end-to-end privacy automation is starting to cost businesses, with expected costs north of $190K per million identities annually.

Consumers have embraced CCPA, and we expect we'll see an increase of DSR requests in 2021 as privacy issues continue to dominate the headlines. At the time of publishing this report in March 2021, the news of Apple and Facebook's feud over a new privacy feature in Apple's upcoming iOS update is driving more awareness. Apple's new App Tracking Transparency feature informs people head on with what's happening to their personal data. By adding a pop-up in apps, Apple is forcing a conversation about privacy that was previously tucked away in privacy policies and T&Cs. Consumers will finally be asked—at the right time—how they want their personal data handled.

But just because consumers are asking for more control, doesn't mean businesses need to be on the defense. It would be easy for businesses to approach this privacy-focused era with concerns about how it will impact profit margins, yet we are seeing that brands who lean into privacy can win. According to a study from Cisco, "Most organizations are seeing very positive returns on their privacy investments, and more than 40% are seeing benefits at least twice that of their privacy spend."

To achieve these returns, companies should take steps to integrate privacy into their overall business. A great first step is simplifying a privacy policy with language the average person can understand. Privacy requires cross-functional teams hashing through the details of what's collected, why, and how it's used and stored. Often these aren't fun conversations because there are competing priorities across the organization.

> "A great first step is simplifying a privacy policy with language the average person can understand."

That's where strong leadership and an organization-wide understanding of a company's approach to privacy are critical. More and more, we see leading brands, many of them DataGrail customers, centralizing privacy programs to ensure privacy mandates are woven throughout the fabric of the entire organization. Without that, employee *and* customer trust can be lost. But companies that proactively embrace privacy to add value to their brands and build trust with their customers will be the undisputed winners of this new era.

Methodology

DataGrail analyzed the data subject requests it helped process on behalf of select business-to-consumer customers with a substantial volume of privacy requests in the period January 1 to December 31st, 2020. This customer set had more than sixteen million consumer identities, where a "consumer identity" is defined as a single, individual identity associated with a unique email address within a customer's database. To determine the cost of manually processing requests, we used Gartner's estimate that manually processing a single request costs $1,406. Gartner published this statistic after releasing details from its 2019 Gartner Security and Risk Survey in February 2020.

DATAGRAIL®

DataGrail is the data privacy platform for modern brands to build customer trust and transparency. Datagrail untangles the complexity of data privacy and enables organizations to automate their privacy programs. We gives brands one easy-to-use platform to simplify, automate, and scale their privacy programs, and stay compliant with regulations like GDPR, CCPA, and CPRA. DataGrail services millions of consumers, through companies like Overstock, Restoration Hardware, NETGEAR, Twilio, Outreach, and has 4.8/5 stars on G2.

DataGrail automates data subject requests for CCPA/CPRA and GDPR, performs unified preference management, and ensures accurate data discovery, which is foundational to any privacy program. DataGrail saves privacy teams' time, reduces the risk of being fined, and ensures error-proof data discovery, all while promising an easy onboarding with little to no ongoing maintenance. With 900+ pre-built connections with popular enterprise applications, The DataGrail Integrations Network is the first of its kind to detect unknown applications and systems that may contain personal data, ensuring the most accurate data discovery possible.

To learn more about DataGrail, please visit www.datagrail.io or follow DataGrail on Twitter and LinkedIn

Learn more about DataGrail's Privacy Platform

Request a demo at www.datagrail.io