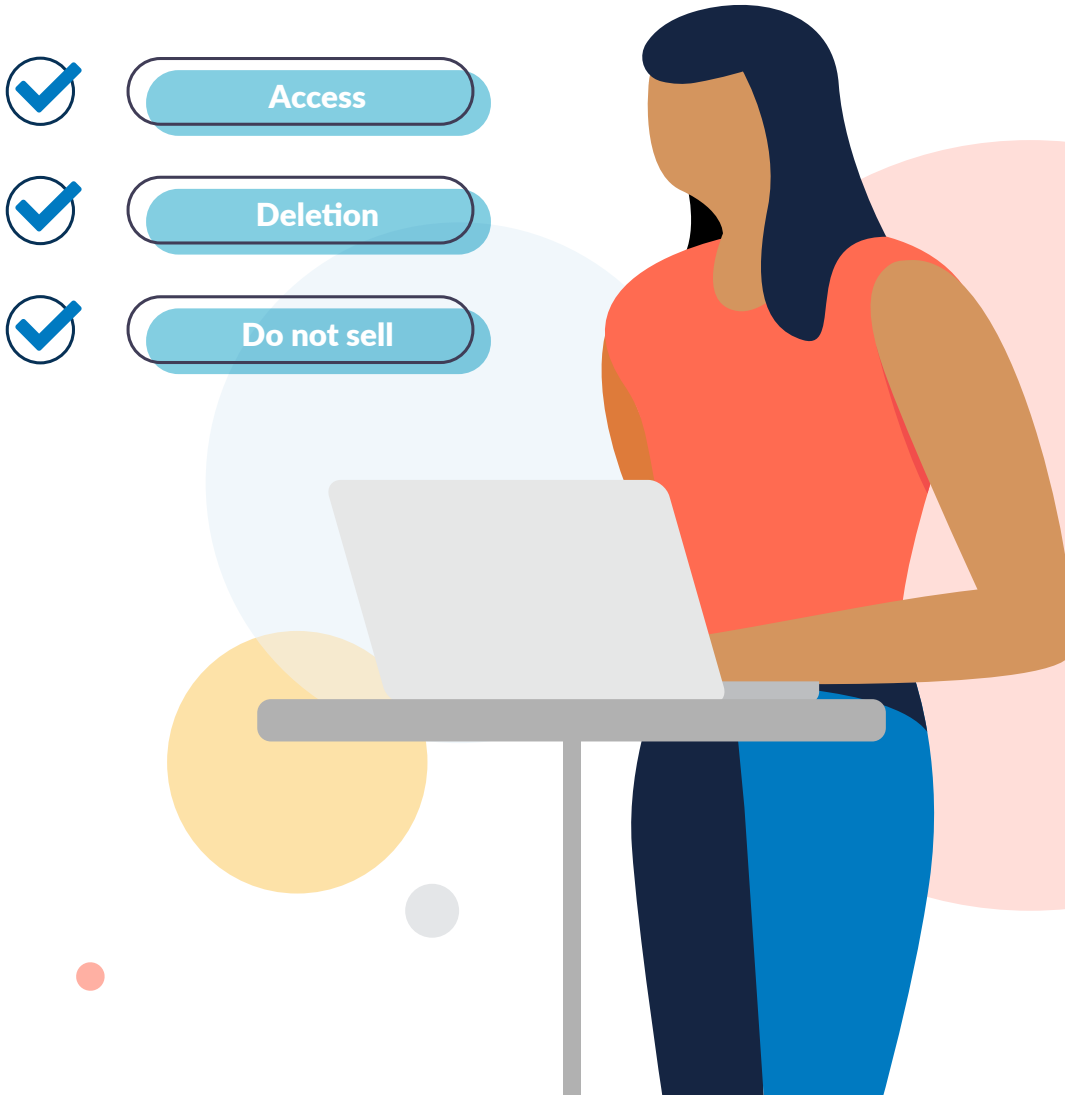
DATAGRAIL®

Insider's Look:

Mid-Year CCPA Trends Report 2020

See how many data subject requests (DSRs) your business may receive



www.datagrail.io

Insider's Look: Mid-Year CCPA Trends Report 2020

At DataGrail one of the biggest questions we get from our customers and prospects is: "How many data subject requests (DSR or sometimes referred to as DSAR) should I expect per year?"

While we can't predict the future, we can use the data from the first half of the year to plan for the future, especially as CCPA enforcement ramps up.

We service DSRs for millions of consumers, giving us unique insights into the number of requests a company can anticipate. We looked at the number of DSRs processed from January to June 2020 across our B2C customers to benchmark approximately how many DSRs a company can expect each month.

Our aim with this research is to help any consumer business (retail, e-commerce, direct-to-consumer, etc.) plan and benchmark where they stand relative to their peers in the space. It's early, but we hope these learnings help consumer businesses better prepare for CCPA and continuous amendments to the regulation (e.g CPRA).

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).

Highlights

Do-not-sell (DNS) requests are the most common type of DSR by nearly 2x.

In 2020, companies manually processing DSRs should expect to pay **$240,000 per million records** to fulfill **requests**.

B2C companies should prepare to process approximately **170 total DSRs per one million consumer records** each year.

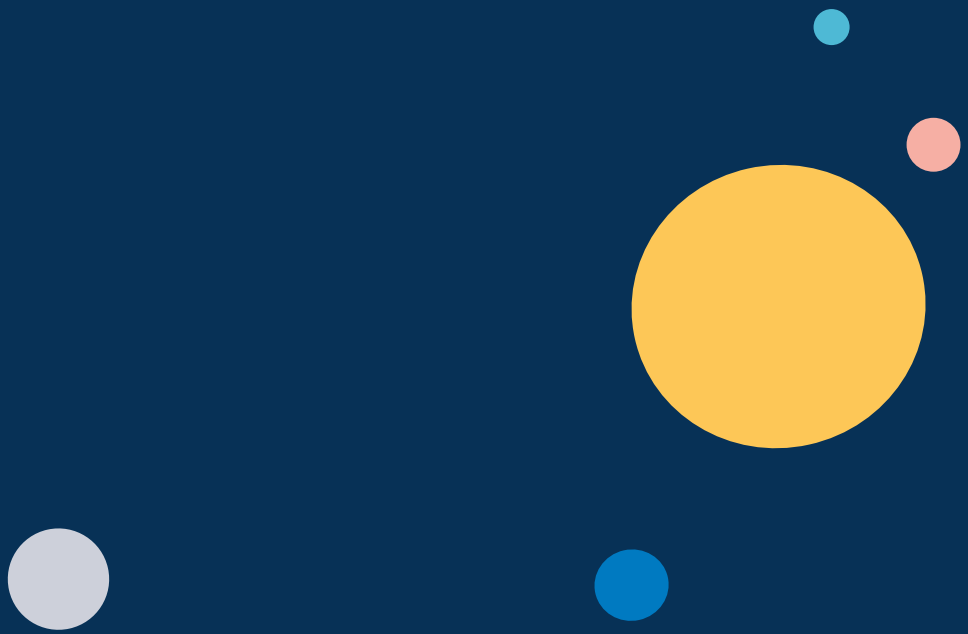
- In 2020, B2C companies should plan to process **84+ DNS requests per million records**.

Three of every ten DSRs will go unverified, confirming the need for a robust and scalable verification method to prevent fraud.

- Approximately **40% of access requests were not verified**, validating concerns that fraudulent requests are made to steal data.

Important note in interpreting the data: to normalize the data across different business types and company sizes, the data presented measures DSRs per one million records. For example, the data shows that on average, businesses are getting about 13 DSRs per one million records each month. This means if your business has 3 million records, you can expect 39 DSRs per month.

Contents



Total Volume of Data Subject Requests (DSRs)

In January 2020, we saw a large bump in the number of DSRs submitted across our customer base, which we believe is due to many of them updating privacy policies to comply with CCPA. Since then, we've seen the number stabilize around 13 DSRs per million records, per month.

In Figure 1 you can see that in the first half of 2020, we saw a total of approximately 84 total DSR requests per million records, leading us to the conclusion that businesses can expect around 170 DSRs per million records by the end of 2020.

Businesses should expect around 170 DSRs per million records every year.

Gartner data shows that manually processing a single data subject request costs (on average) $1,406. At this rate, **organizations can expect to spend almost $240,000 per million records** to fulfill data subject requests if they are done manually.

Figure 3 projects how many DSRs by type you should expect per year. DNS continues to be the most popular request by a factor of two.

Figure 1. Total Volume of DSRs in H1 2020 Per Million Records

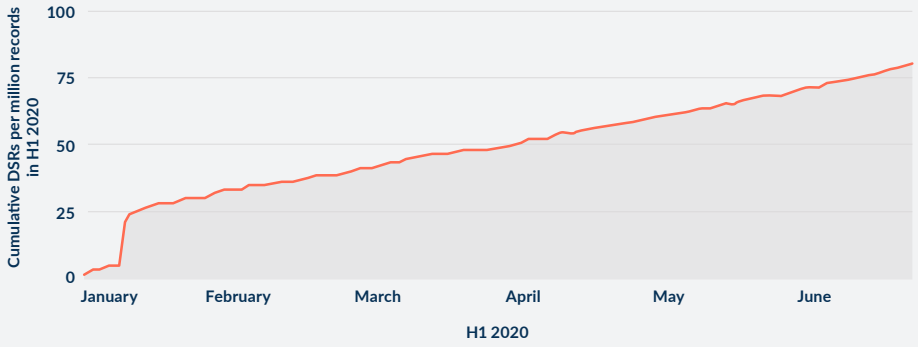


Figure 2. DSRs Per Million Records By Month H1 2020

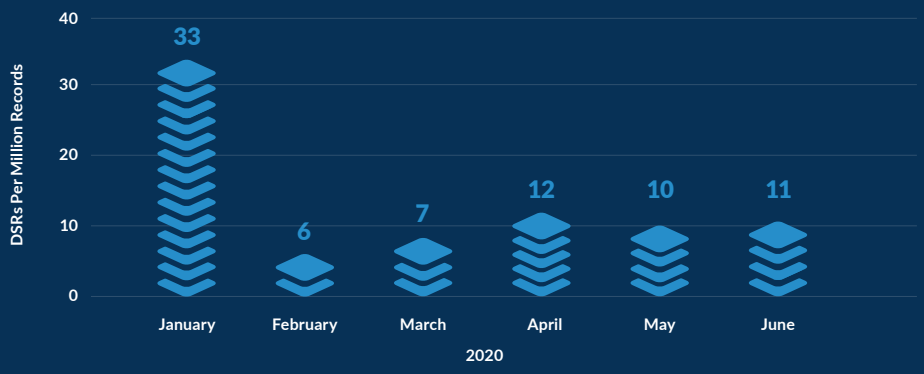
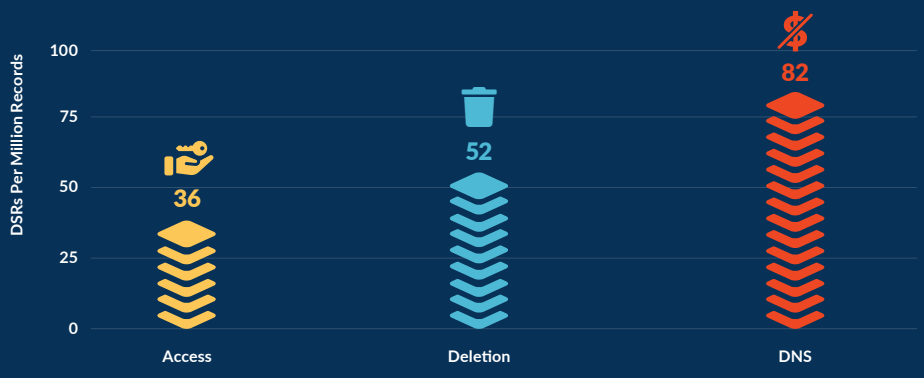


Figure 3. Projected DSRs Per Million Records In 2020



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

In Figure 4 we see Do-not-sell (DNS) requests are almost 50% of all DSRs, most likely because consumers are often prompted to accept cookie and DNS settings when they first visit an organization's website.

Do-not-sell (DNS) requests are almost 50% of all DSR requests.

When we look at the number and type of DSRs by month (see Figure 5), we see the number of requests start to stabilize. DNS requests stabilize around 7 requests/million records, DSARs sit around 3 requests/million records and deletions stabilize around 4 requests/million records. 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 enforcement date, triggering another round of deletion requests.

Figure 4. Requests by Type: Access, Deletion, Do Not Sell H1 2020

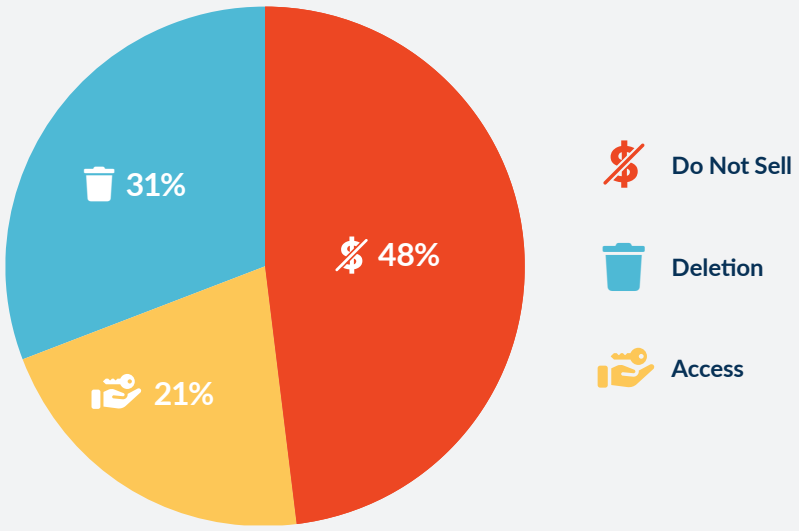
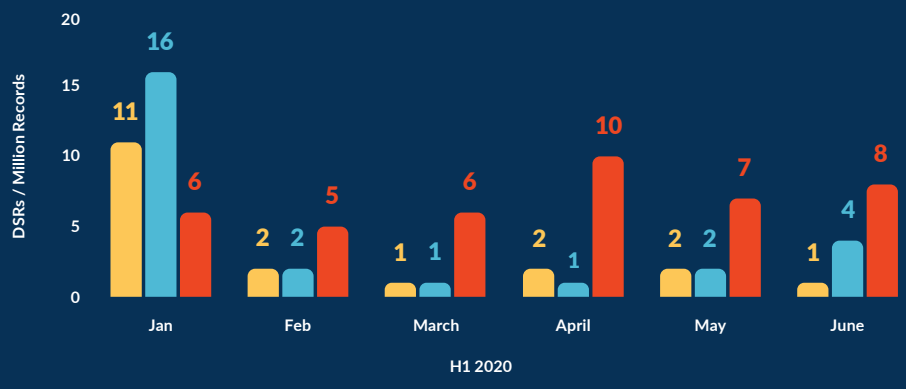


Figure 5. Access, Deletion and DNS Requests / Million Records H1 2020



Data Subject Request Verification And Potential Fraud

Fraud comes up as a top concern when organizations start to think about processing DSRs, especially when personal data is concerned - no organization wants to pass along personal information to the wrong person or someone who might be impersonating one of their customers. 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.

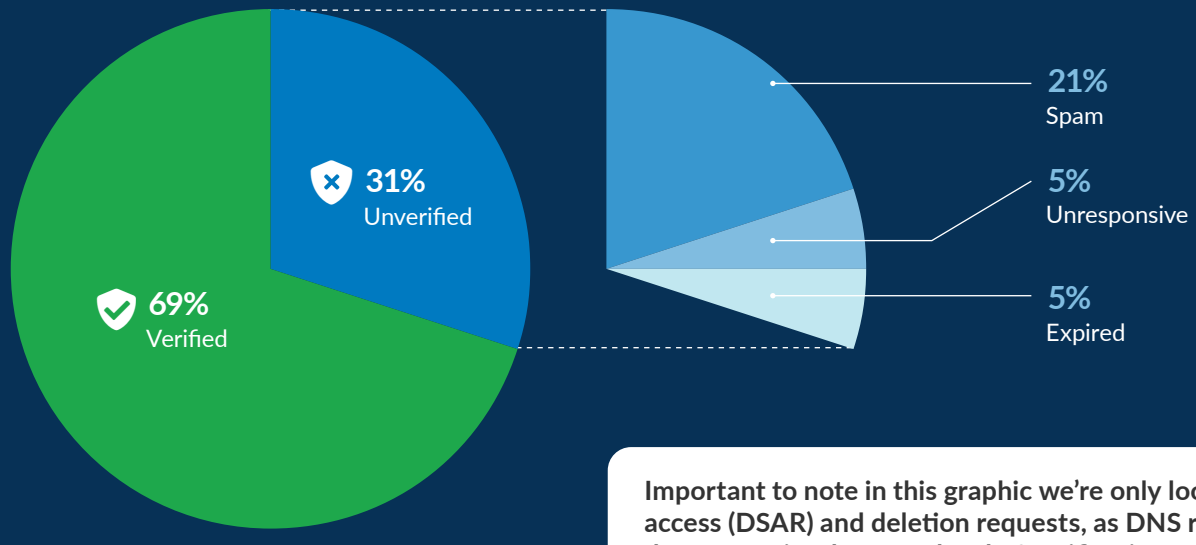
Though some platforms ask consumers to provide additional data to verify their identity (which goes against the spirit of CCPA), DataGrail's Smart Verification technology uses existing data associated with the individual's record, such as purchase history or user behaviors (e.g. games played, purchases or products viewed) to securely validate the individual's identity.

With that technology, we were able to see how many unverified (and potentially fraudulent) DSRs went across the platform, which was close to 30% as seen in Figure 6.* Three out of every 10 DSR requests will likely not be verified and could be fraudulent attempts at accessing or deleting data.

Within the bucket of unverified requests, the majority of those were spam. It appears for every five requests, you'll get one spam request (Figure 6). At DataGrail, a DSR is marked as spam by our customers who suspect it's not a valid request.

For every five requests, businesses can expect to receive one spam request.

Figure 6. Verified vs. Unverified CCPA Requests Breakdown H1 2020



Important to note in this graphic we're only looking at access (DSAR) and deletion requests, as DNS requests do not require the same level of verification.

DSAR Verification and Potential Fraud (Continued)

When we break down which types of requests were unverified (access vs. deletion), we see that access requests (DSARs) make up 70% of the unverified requests (Figure 7), validating the concern that nefarious characters could be making access requests to gain access to another person's personal information.

When we looked at just DSARs (both verified and unverified in Figure 8), to see what percentage of them were unverified, we saw that 40% of access requests were unverified, and of that, 30% were spam access requests.

Access requests (DSARs) make up 70% of the unverified requests.

Figure 7. Percent of Unverified CCPA Requests By Type H1 2020

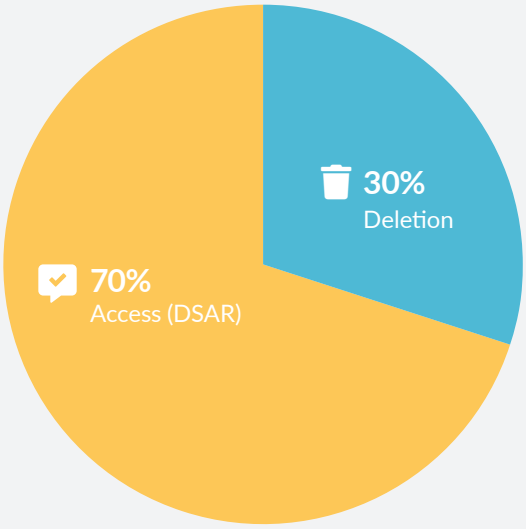
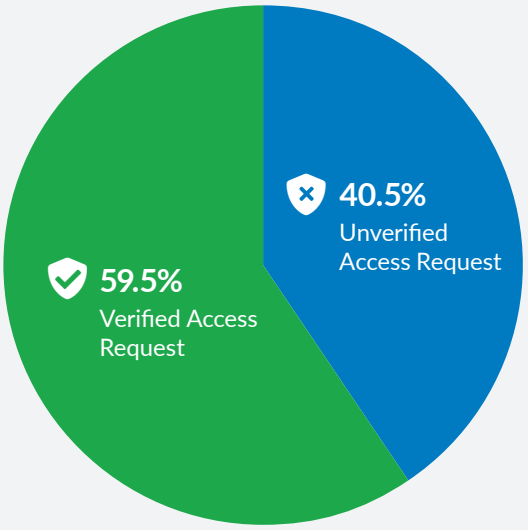


Figure 8. CCPA Data Subject Access Requests (DSAR) - Verified vs. Unverified H1 2020



Conclusion

As we look back on the first half of the year, we see that DSR requests are starting to stabilize around 13 DSRs per million records every month. This is an important benchmark to establish as companies continue to plan for resources and budget to get and stay compliant with CCPA for the remainder of 2020 and into 2021.

Without a technology solution in place, handling a single data subject request can potentially involve up to 26 people in an organization and cost $1,406 per request. Financially, that can cost businesses up to $240,000 per million records annually -- if they are processing requests manually.

As many in the privacy and security space feared, fraud is a valid concern. While we can't say for certain that all unverified requests are fraudulent, it's a fair assumption that a percentage of them are, requiring companies to have a very strong verification method.

We can expect the first CCPA fines to come in around October 2020.

At DataGrail, we recommend identifying a verification method that is frictionless for the consumer and does not ask them to submit additional personal information, as that increases an organization's risk and creates frustration for the consumer.

If we follow the trends of what happened with GDPR in 2018 and beyond, we can expect that businesses will start to be fined within the next couple months. GDPR went into effect in May of 2018, and the first fines were given in July of that same year. If we follow the same timeline for CCPA beginning from the enforcement date of July 1st, 2020, we can expect the first fines to come in around October 2020.

New regulations and amendments to existing ones will continue to emerge, and organizations that build privacy programs that can scale with those changes will be the ones who save on the bottom line in the long run. We hope this report helps you benchmark where your company needs might fall, forecast resources and budget for compliance, and work through your privacy program for the months to come.

Methodology

DataGrail took a look at 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 June 30th, 2020. This customer set had more than sixteen million consumer records, where a "consumer record" is defined as a single, individual record 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.

About DataGrail

DataGrail helps companies comply effortlessly with existing and emerging privacy laws, such as GDPR and CCPA. It was designed from the ground up to automate data discovery and streamline privacy programs to create less work for customers, while also ensuring a higher level of accuracy and reduced risk. DataGrail built its solution to directly integrate with an organization's internal databases and developed 250+ pre-built connectors with companies — such as Salesforce, Shopify, Adobe, AWS, Oracle, Okta, and many others. These connections provide organizations with an accurate, real-time view of the internal systems and third-party applications used and all the personal data that maps onto each of those systems. DataGrail also allows customers to manage their privacy request workflows and email preferences across applications.

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

Request a demo