



Peering Through the Lens:

**Video Surveillance and the
Unseen Gaps of the California
Consumer Privacy Act**

Table of Contents

Authors: Steve Trush
Brian Hofer

Published April 2023

We would like to thank
Shabnam Tai Hofer for her
contributions to this report.

Introduction

Methodology

Results

Accessing your data

Deleting your data

Summary of Results by Company

Conclusion



Secure Justice is an IRS registered 501(c)(3) non-profit organization advocating against state abuse of power, and for reduction in government and corporate over-reach. We target change in government contracting and corporate complicity with government policies and practices that are inconsistent with democratic values and principles of human rights.

We strive to create municipal civilian oversight frameworks that provide the community with a meaningful voice and a seat at the table when crafting rules for the use of surveillance technologies, and the data collected from such use. Although our primary focus is on entities with police power, the blurring lines between public-private partnerships and corporate complicity in the facilitation of human rights abuses by government actors causes us to also address the private sector's use of surveillance and smart city technologies, data sharing and mining practices.

Oakland, CA 94608 | secure-justice.org | brian@Secure-Justice.org



**This report was made possible
with generous support from
the Rose Foundation.**

Executive Summary

First signed into law by then-California Governor Jerry Brown in 2018, the California Consumer Privacy Act (CCPA) “gives consumers more control over the personal information that businesses collect about them”¹ by establishing privacy rights for California consumers. Similar to Europe’s General Data Protection Regulation (GDPR), Californians would now have the right to know and access what personal data a business collects on them, the right to delete their data, and the right to say no to the sale of their data. On January 1st, 2023, additional rights to correct inaccurate personal data and to limit the use and disclosure of sensitive personal data went into effect after Californians voted to modify the CCPA via approval of Proposition 24, the California Privacy Rights Act (CPRA), in November of 2020. Although this new oversight framework is in its early stages, in this report we tested the real world responses of companies subject to this ground-breaking law.

CCPA applies to many businesses,² including data brokers, who must provide written notice explaining their data collection practices as well as promptly respond to requests from Californians to exercise these privacy rights. The law also prohibits businesses from discriminating against any Californian for asserting their human right to privacy.

Our research below led us to conclude that the intent of the CPPA is not being fully honored, that there are multiple obstacles that will likely discourage consumers from exercising their rights, and that the real world responses from the targeted companies produced data that is meaningless to the average California consumer. Although the CPPA allows for sanctions to be imposed, we don’t believe that the average California consumer understands how to exercise their rights, cannot afford to hire legal counsel to advise them of their rights, and the relatively low dollar amount for sanctions (\$7,500 for intentional violations, \$2,500 for unintentional violations) does not provide a sufficient deterrent for future misconduct. We are encouraged by the California Attorney General’s announced expansion of a complaint system and increased enforcement, and the CPPA Board’s recent posted job announcements for additional enforcement officers. Unfortunately, the Attorney General’s complaint system at present is limited to drafting notices to businesses that do not post an easy-to-find “Do Not Sell My Personal Information” link on their website.³ Furthermore, greater enforcement alone may not necessarily lead to consumers having a greater understanding of the data returned to them by compliant businesses - the responses themselves must be modified based upon what we are seeing in practice today.

Although other organizations have surveyed companies' readiness and ability to comply with the new oversight framework, these reports have focused on business privacy policies and not the "real world" experience of an individual seeking to realize the benefits of the law that California consumers are entitled to.⁴ Several private sector entities are likewise attempting to help consumers have a more meaningful understanding of what data is being collected, outside of the CPPA framework.^{5,6}

In this report, Secure Justice researchers played the role of "secret shopper" so that we could measure a representative sample of entities that sell consumer home surveillance devices, and gauge their responsiveness to our requests for our own data, and also our requests to delete it. We chose to focus on the home surveillance industry because video surveillance vendors should be held to the highest privacy standards given the sensitivity and social impact of the data that they are collecting, yet we frequently see how these companies fail to protect consumers.^{7,8,9,10}

Portions of the CPRA privacy-protecting regulations will not be enforced until July 1, 2023, to both provide the business sector with sufficient time to prepare, and for additional rule making and public comment as the regulations that will implement the new law get developed. Prior to publication of this report, the recently formed CPPA Board, which is charged with overseeing the new framework, met on February 3, 2023 to consider a set of proposed rules. Some of the adopted rules, which are not yet in effect and require additional approval, will address concerns that we've identified in our report below. Unfortunately, we do not believe that the proposed rules will address all of the non-compliance issues we found, nor do they adequately help the consumer realize the full utility and intent of the law.

Furthermore, several of the new proposals raise additional concerns and might actually weaken the privacy protections that California voters desire, such as the proposed use of third party verification services which may lead to additional disclosure of sensitive data and increased risk of additional data breaches.¹¹

Finally, consider California companies to be on notice. This report can serve as a baseline as we will continue to investigate how these and other companies improve their practices once the new rules are enforced.

The research for this report was conducted in 2022. The Office of Administrative Law must still review the rule package approved by the CPPA Board on February 3, 2023. The rules could become effective at the earliest in April 2023.

Key Finding #1

Almost half of the businesses failed to provide the required privacy policy information due to their privacy policy either lacking CPRA required provisions, was out of date (e.g. 2017), had incorrect or no contact information, or was difficult to find amongst a corporate family of differing products and names (e.g. Nest and Google).

Recommendations

- A. A conspicuously posted privacy contact info/privacy tool management link should be mandated by the regulators, and businesses can and should voluntarily take this action now.
- B. Privacy policies must disclose all data types that may be collected.
- C. We recommend that the business sector and regulators consider accessibility concerns, including the blind, those less technically proficient like the elderly, and those that are non-native English speakers, which includes millions of California consumers. If a business offers services or products in different languages, privacy policy and privacy management solutions be in those languages.¹²

Key Finding #2

Five of 11 businesses failed to meet CCPA-mandated deadlines. Two businesses either failed to acknowledge our request for data within the required time period or failed to deliver the requested data within the required time period, with one company taking 129 days to complete the request. Three businesses failed to acknowledge our request to delete our data within the required time period, with two businesses failing to delete our data within the required time period.

Recommendations

- D. We do not believe that CPRA penalties are sufficient to deter future misconduct. Many of the businesses subject to this law collect billions in revenue each year. A \$7,500 penalty (per violation) will be absorbed as “the cost of doing business” by these larger entities. Fines must be effective, proportionate and dissuasive. We recommend that California raise the ceiling for penalties and mirror the GDPR model. For less severe violations, a penalty of up to \$10 million or 2% of worldwide annual revenue, whichever is higher; for more severe violations, a penalty of up to \$20 million or 4% of worldwide annual revenue, whichever is higher.

- E. So that consumers receive the most utility from this new oversight regime, we recommend that lax security practices by a business be penalized sufficiently to deter bad practices, such that a business at least attempts to protect the requested data with as much security that the consumer has previously requested via their account settings.
 - i. If a user enables two-factor authorization (2FA), the business should at least request some form of additional factor beyond the email of the account; requests for data and to delete should be made from within the account itself. For paid accounts, a business could use the last 4 of a credit card or payment source provided by the consumer.
 - ii. Businesses should require use of 2FA for both data requests and delete requests. Our research revealed dangerous security practices such as requesting passwords from the user via email or sharing sensitive information in unsafe ways.
- F. Consumers should be able to view which companies are frequent violators. The Attorney General's limited complaint system should be improved to provide data on which companies have prior substantiated complaints, with a dashboard like the one created for the GDPR by CMS.¹³
- G. Businesses should publish, and regulators should mandate, transparency reports similar to what Google has created.^{14,15}

Key Finding #3

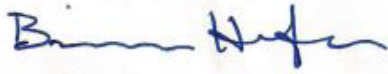
Data was not produced to us in an “easy to understand” or “machine readable” format, defeating the utility of the law.

Recommendations

- H. A “reasonable person” standard exists in US law. Our report contains multiple screenshots of the data we received. A reasonable person would likely agree that the data shared by the companies we surveyed is not understandable by the “average consumer” for various reasons including file formats, file structures, and lack of plain language data descriptions. One company had a proprietary file structure that was unintelligible.
- I. Businesses should incorporate greater use of automation and repeatable processes to improve responsiveness and legal compliance with regulations

J. CPRA Article 3 Section 7020(a) only requires that a business provide an email address for submitting requests to delete, correct, and know. We recommend use of an online form to allow for automation and scalability, to increase the participation rate of consumers and decrease the administrative burden and cost on the business community. This would support the greater use of automation.

The conclusion of our report contains additional recommendations for consumers, policy makers, and the business sector.

A handwritten signature in blue ink, appearing to read "Brian Hofer", is positioned above the printed name.

Brian Hofer

Executive Director



Introduction

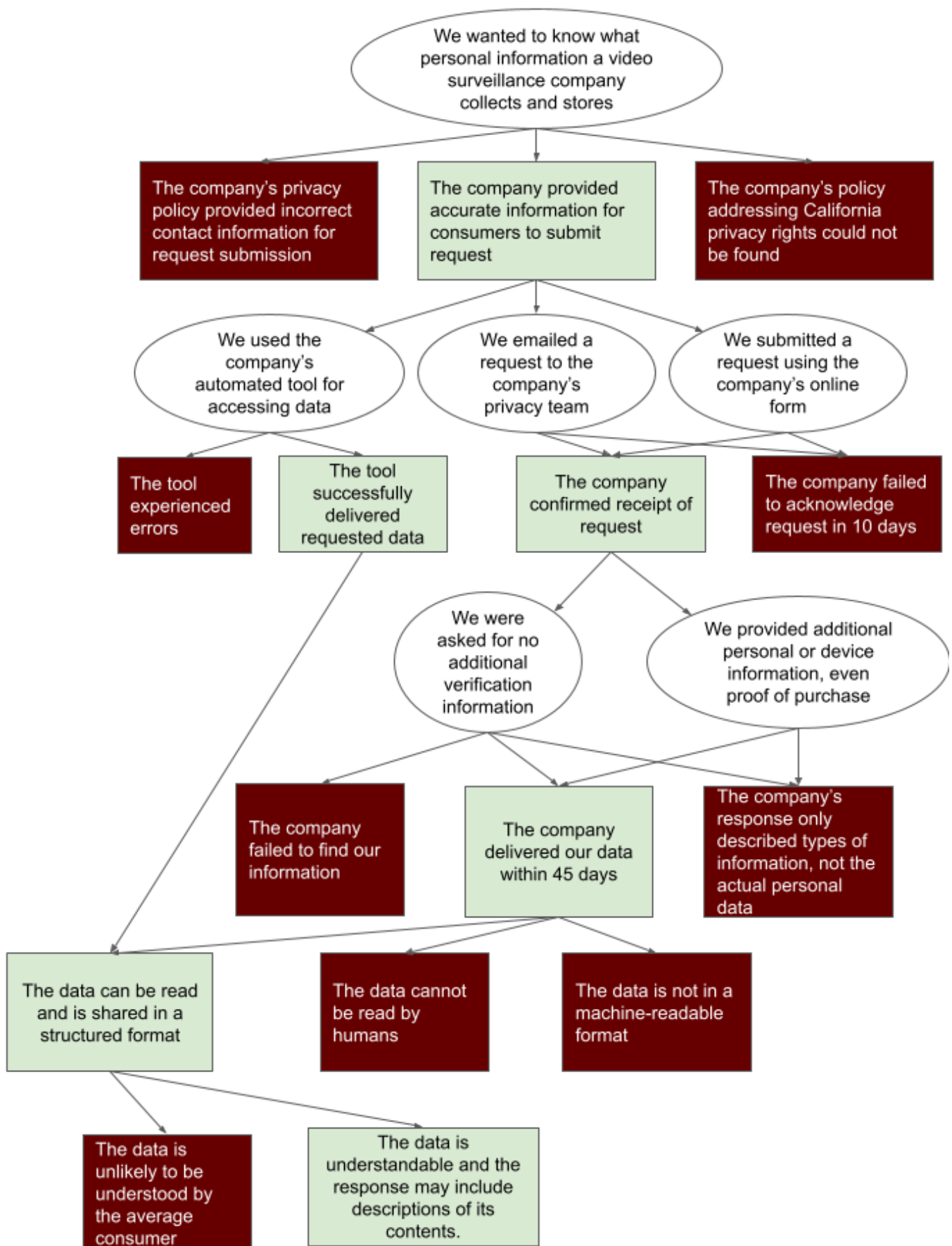
Secure Justice conducted a study of popular video surveillance vendors to evaluate the ability of those companies to respect the privacy rights of California consumers as required by the California Consumer Privacy Act and the California Privacy Rights Act. This study was made possible with generous funding from the Rose Foundation.

The multiple paths and obstacles underscore how the process can be challenging for a consumer to answer the simple question “what information does this company collect and store about me?”

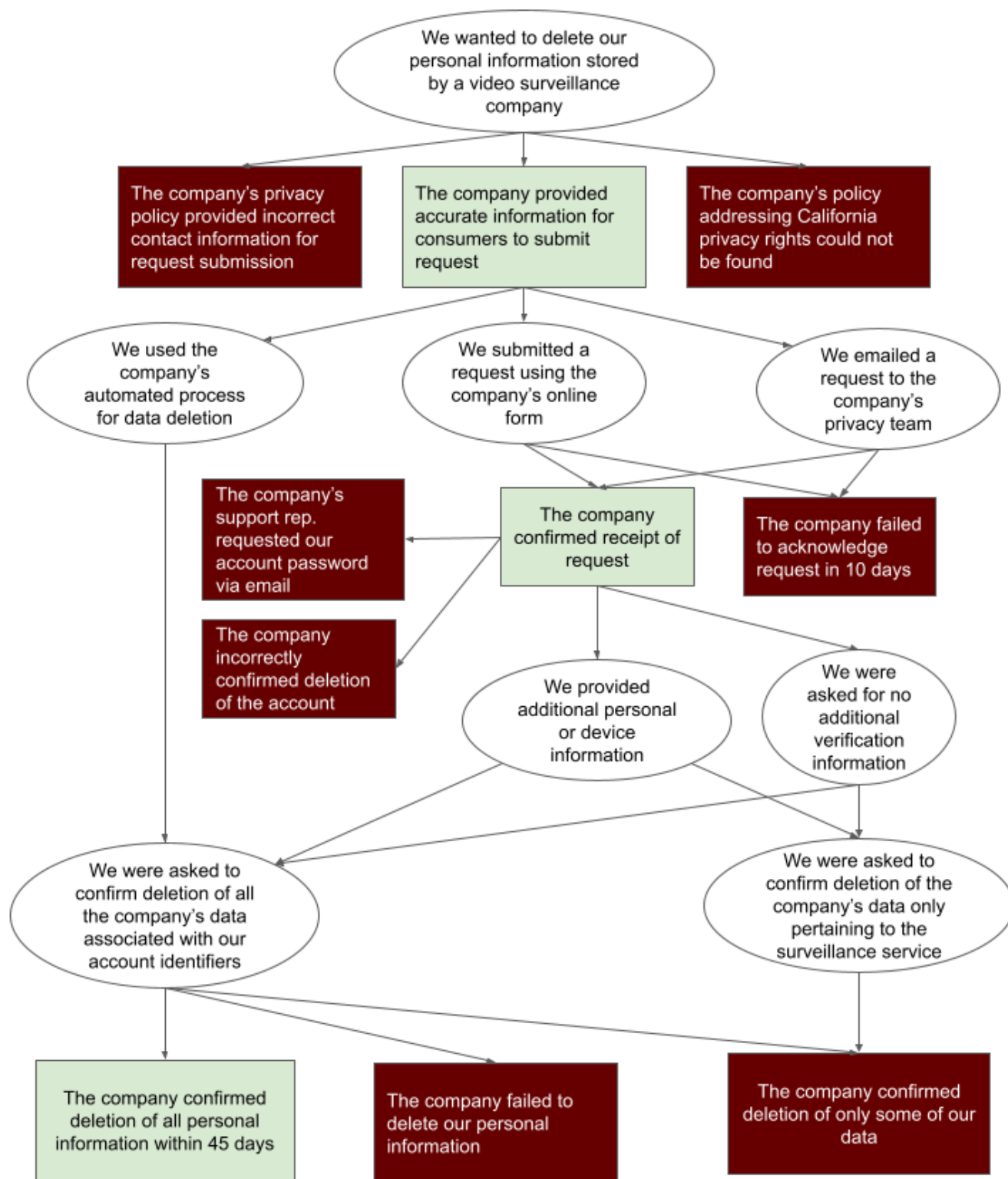
California legislators champion nation-leading privacy rights guaranteed by legislation such as the California Consumer Privacy Act and California Privacy Rights Act, but little work has shown how these laws affect consumers’ ability to manage data collection. Further, consumers installing these devices concerned about safety may not even realize what privacy risks exist or, even if they did, how to manage their privacy interests. The affordability of these systems combined with the failure of law enforcement to protect underserved communities can make installing personal home surveillance systems appealing to Californians. This dynamic creates the need to both educate and protect the consumer and the community at-large from the disparate impact of surveillance.

Our investigation revealed how the process for California consumers to request or delete their own personal data can offer multiple obstacles to understanding which personal information video surveillance companies are collecting and storing about Californians. While some companies in our sample failed to meet the standards of the California Consumer Privacy Act, the companies’ different processes and responses showed how the data rights request processes can vary drastically even when companies are compliant with CCPA.

We have charted our experiences in requesting personal data from popular home surveillance vendors. The multiple paths and obstacles (highlighted in dark red boxes with white text) underscore how the process can be challenging for a consumer to answer the simple question “what information does this company collect and store about me?” We believe the multiple branches of this privacy “Choose Your Own Adventure” journey create friction that can discourage most Californians from exercising their Right to Know.



We also looked at the process for deleting personal data from those same companies. The California consumer may face additional issues when deciding that a video surveillance company should not possess their personal information.



If an average Californian cannot successfully request their information, cannot understand the data included in a company's response, and cannot delete their personal information, how useful are the data access rights mandated by the CCPA? We suggest that companies should improve their processes, that policymakers should realize how the law's mandates are implemented and hold companies accountable for noncompliance, and that advocates such as ourselves should use our technological expertise to improve the public understanding of what video surveillance companies are collecting in California.



Methodology

Our study uses qualitative research methods to understand a range of experiences that a California consumer may have with video surveillance companies operating in the state. Through the conduct and analysis of email dialogue, written policies, and system interactions, we learned how companies may respond or react to some California consumers. As such, this report does not make statistical claims about the rate of success for any single company or all companies in the business of video surveillance. We realize that another consumer may have a different experience with any of the companies that we assessed. In fact, we encourage other Californians to recreate these requests for themselves.

First, we reviewed the current legal requirements for companies operating in California as required by the CCPA. From the law, we formed a list of questions that we wanted to investigate, which included some things that were not mandated by CCPA:

- Did the company provide sufficient means to make a consumer request pursuant to the California Privacy Rights Act and *130(a)(5)*, including in Spanish *[not legally required]*?
- Did the company share applicable and appropriate data with the consumer pursuant to *130(a)(2)(B)*?
- Did the company acknowledge all of our data requests in 10 business days *[per Cal. Code Regs. Tit. 11, §7021(a)]*?
- Did the company deliver our data upon request within 45 calendar days *[per Cal. Civ. Code §1798.130(a)(2) and Cal. Code Regs. Tit. 11, §7021(b)]*?
- Did the company delete our data upon request within 45 calendar days *[per Cal. Code Regs. Tit. 11, §7021(b)]*?
- Was the company's request for additional information for verification appear to be reasonable *[per Cal. Civ. Code §1798.130(a)(2)]*?
- Was the company's request process free of errors that delayed fulfillment of rights?
- Did the company deliver all data in a format "easily understandable to the average consumer" *[per Cal. Civ. Code §1798.130(a)(3)(B)(iii)]*?

- Did the company deliver all data in a “structured, commonly used, machine-readable format” [per Cal. Civ. Code §1798.130(a)(3)(B)(iii)]?
- Did the company provide descriptions of data, files, or folders?

Our process then involved building a sample of companies that potentially provided a range of consumer experiences during the request process. We looked for the most popular internet-connected devices for exterior (doorbell or mounted camera systems) and interior home camera systems on Amazon and selected a sample to have a range of company size, company location (California-based, US-based outside of California, and based outside of the United States), technological features (i.e., each device had an associated iPhone application and connected to wireless internet), and device affordability.

Company Name	Headquarters Location	Size (# of Employees)	Website
Apple	Cupertino, CA, USA	10001+ ¹⁶	www.apple.com
Arlo	San Jose, CA, USA	501-1000 ¹⁷	www.arlo.com
Blurams	Shenzhen, China	251-500 ¹⁸	www.blurams.com
D-Link	Taipei, Taiwan	1001-5000 ¹⁹	www.dlink.com
Eufy (Anker brand)	Changsha, China	3,532 ²⁰	www.eufylife.com
Kasa Smart (TP-Link brand)	Hong Kong / Shenzhen, China	10001+ ^{21,22}	www.tp-link.com & www.kasasmart.com
Nest (Google brand)	Mountain View, CA, USA	10001+ ²³	www.google.com & www.nest.com
Logitech	Newark, CA, USA	5001 - 10000 ²⁴	www.logitech.com
Ring (Amazon subsidiary)	Santa Monica, CA, USA	1001 - 5000 ²⁵	www.ring.com
Simplisafe	Boston, MA, USA	501 - 1000 ²⁶	www.simplisafe.com
Wyze	Kirkland, WA, USA	238 ²⁷	www.wyze.com

After identifying these companies, we procured a popular surveillance device offered by each vendor. After device installation on our test network, mobile application installation, and user account creation, we generated data sets by interacting with each device (pushing door bells, activating motion sensors, recording video and sound, adjusting device settings). We then reviewed vendor privacy policies to locate instructions for fulfilling our California consumer data rights. As “secret shoppers,” we requested access and deletion of our information while reacting to a company’s responses as we believed an average Californian might.

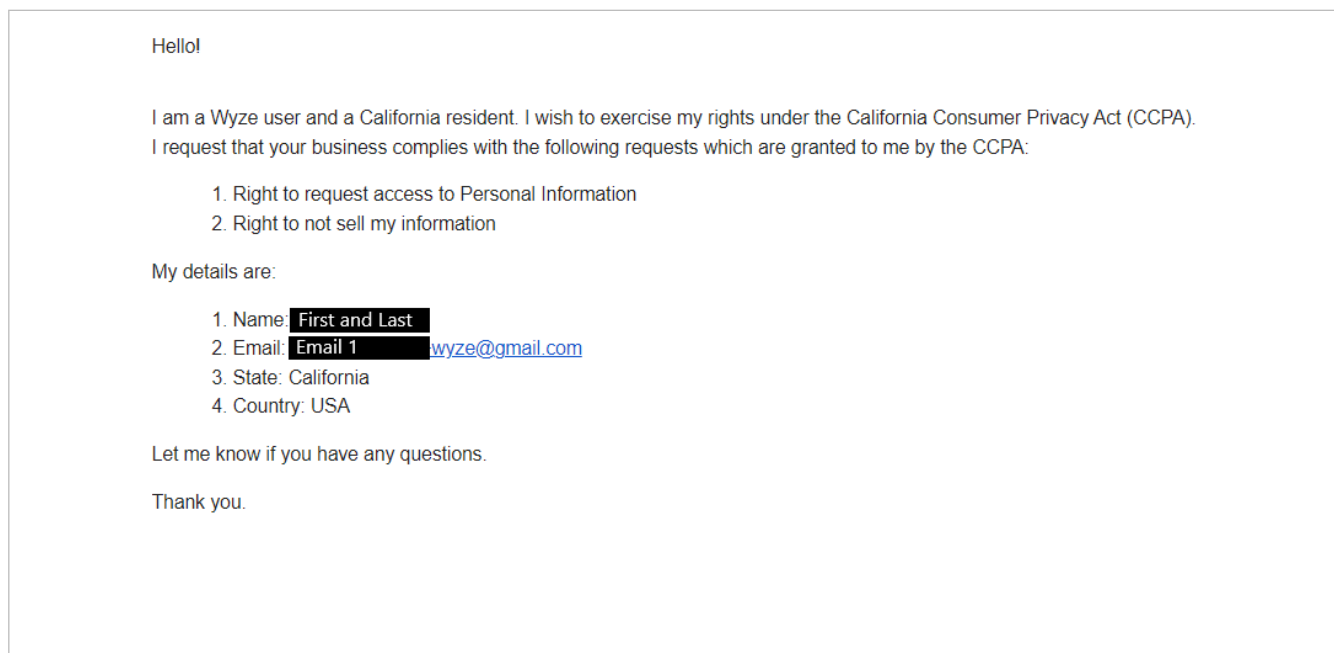
We kept this report’s sample to a manageable list of 11 companies. It is important to recognize that purchasing a surveillance system does contribute some revenue to the vendors, so we were judicious in our procurement. While the potential benefit of our findings definitely outweighs the modest cost of these individual systems, the procured devices will be repeatedly used to investigate their respective vendors as we seek to make and understand changes in California consumer privacy.

Results

Accessing your data

A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

- Cal. Civ. Code §1798.100(a)



A sample of our emailed data access request

Where to begin a data request

- How did we find the privacy policy?
- How did we find instructions to submit a request?
- What was the process for submitting a request?

The CPRA requires that each company with California-based customers needs to provide instructions on fulfilling their data rights. A company should place instructions in a privacy policy that is accessible and conspicuously posted on their website.

[A] business shall, in a form that is reasonably accessible to consumers:

(1)(A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

- Cal. Civ. Code §1798.130(a)

Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

- Cal. Civ. Code §1798.130(a)(5)

We found that all companies posted a link to their privacy policy on their main website. During the course of our research, one company (Blurams) did not have a link to their privacy policy until July 2022²⁸, having recently updated their website to comply with this requirement (although the privacy policy itself was last updated in 2017²⁹).

...With several companies, the more difficult process was determining which privacy policy would provide relevant instructions.

If anything, with several companies, the more difficult process was determining which privacy policy would provide relevant instructions. Depending on whether you know Google owns Nest, you may find yourself on Nest's privacy page³⁰ which directs consumers to Google's privacy page listing a generic privacy policy applicable to all of Google's products, leaving users searching for additional answers on Nest-specific data.

For D-Link, Kasa Smart (a brand of TP-Link), and Blurams users, they may stumble across different versions of privacy policies depending on whether you performed a web search, used the link to the privacy policy from the AppStore³¹, or accessed the privacy policy from their customer portal. This may not be a problem except each of the policies had different contact information for their Privacy teams, or had not included information related to California rights altogether.

D-Link's non-US privacy policy may confuse California users

D-Link does not include California-related information in their broader privacy policy listed on the AppStore, their customer portal (MyDlink.com), nor web search results:

If you have a question about this Privacy Policy, or wish to inquire about our personal information handling practices, please contact us as follows:

D-Link Corporation

No. 289. Xinhua 3rd Road, Neihu District

Taipei City, Taiwan

<https://www.dlink.com/support>

Contact information from D-Link's global privacy policy

Visiting their website from a US-based network does list a US-centric policy with California-related information and a more useful contact method:

Disclosure - You have the right to request that we disclose to you the personal information we have collected, used, disclosed or sold about you in the previous 12 months. You may submit a request to [My Information](#). **Note:** link is "[mailto: privacy@dlink.com?subject=Privacy](mailto:privacy@dlink.com?subject=Privacy)"

Contact information from D-Link's United States privacy policy

TP-Link / Kasa Smart lists different privacy contacts

The two versions of Kasa's privacy policies slightly vary by email address. Fortunately, the phone contact information was the same.

To exercise any of the rights listed above, please submit a verifiable consumer request to us by either emailing us at privacy.us@tp-link.com or calling us at 1-866-225-8139. You are not required to have an account with us in order to submit a request and we will only use personal information provided in a consumer request to verify the requestor's identity or authority to make such a request. Please note you may only make a verifiable consumer request for access or data portability twice within a 12-month period.

Contact information from the privacy policy listed in Kasa Smart's AppStore entry

To exercise any of the rights listed above, please submit a verifiable consumer request to us by either emailing us at privacy.tpra@tp-link.com or calling us at 1-866-225-8139. You are not required to have an account with us in order to submit a request and we will only use personal information provided in a consumer request to verify the requestor's identity or authority to make such a request. Please note you may only make a verifiable consumer request for access or data portability twice within a 12-month period.

Contact information from the privacy policy listed in Kasa Smart's AppStore entry

Blurams privacy policies lists either incorrect or no contact information

Blurams' privacy policy listed on the Appstore and web search results does not list contact information for data rights requests:

You can submit your request to us through "help and feedback".

Their privacy policy listed on their website provides an email address, however our initial access request to info@blurams.com went unanswered until we sent a follow-up including a different email (support@blurams.com) listed under "Support" on their website.

For other personal information, we make good faith efforts to provide you with access and support so you can request that we correct the data if it is inaccurate, or delete the data if Blurams is not required to retain it by law or for legitimate business purposes. Please contact Blurams customer support for such request. If you do not want to receive any marketing or promotional email from Blurams or Blurams, you can either choose the opt-out option where it is available or contact Blurams or Blurams customer support (info@blurams.com).

Ultimately, while some versions of privacy policies did not feature information related to California privacy rights, each company had at least one privacy policy that did mention privacy rights specific to California residents. Blurams, whose policy had not been updated since 2017, only referenced the older California “shine the light” law:

Your California Privacy Rights

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our customers who are California residents to request and obtain from us once a year, free of charge, information about the personal information (if any) we disclosed to third parties for direct marketing purposes in the preceding calendar year. If applicable, this information would include a list of the categories of personal information that was shared and the names and addresses of all third parties with which we shared information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request to info@blurams.com.

Requesting data

The below table shows the contact information or portal that we used to request our data. For email inquiries, we used a standard message stating that we were users of the company's product, a California resident, that we wanted the company to fulfill our data access rights as guaranteed by CCPA, and the relevant account information (our researcher's name and the email address used for account setup).

Hello!

I am a Wyze user and a California resident. I wish to exercise my rights under the California Consumer Privacy Act (CCPA). I request that your business complies with the following requests which are granted to me by the CCPA:

1. Right to request access to Personal Information
2. Right to not sell my information

My details are:

1. Name: **First and Last**
2. Email: **Email 1** wyze@gmail.com
3. State: California
4. Country: USA

Let me know if you have any questions.

Thank you.

A sample of our emailed data access requests

Some companies offered multiple methods to request information or contact their privacy team, including phone numbers. The below table shows the methods that we used to request our data.

Data request methods

	Company Information
Email	Arlo: privacy.policy@arlo.com Blurams: info@blurams.com ³² , support@blurams.com D-Link: privacy@dlink.com Eufy: support@eufylife.com Logitech: privacy@logitech.com TPLink/Kasa Smart: privacy.tpra@tp-link.com Wyze: privacy@wyze.com
Online Form	SimpliSafe (via OneTrust): https://simplisafe.com/access-delete-info ³³
Product Web Application	Ring (Control Center): https://account.ring.com/account/control-center/data-requests DLink (MyDlink): https://sso.dlink.com/profile
Company-wide Export Tool	Google/Nest (Takeout): https://takeout.google.com/ Apple: https://privacy.apple.com/

When was data delivered

- How long did the company take to acknowledge the data access request?
- How long did the company take to deliver the information?

Companies operating in California shall confirm the receipt of data access requests within 10 business days and deliver the California-based consumers' data within 45 calendar days (or 90 days with an explanation of the delay) of the request.

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

(b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

- Cal. Code Regs. Tit. 11, §7021

10 of 11 companies acknowledged our data request within the required ten days. 1 company failed to deliver data within 45 days.

Blurams did not answer our initial access request to the contact address listed in their privacy policy (info@blurams.com) but answered our follow-up message to a different email (support@blurams.com) found under the customer support section on their website.

Company response times

Company	Initial Request Date	Business days till acknowledgement of data access request	Calendar days until personal data response received from company
Ring	6/19/22	Same day (6/19/22)	1 day (6/20/22)
TP-Link/Kasa Smart	8/29/22	Same day (8/29/22)	3 days (9/1/22)
Wyze	7/5/22	1 day (7/6/22)	3 days (7/8/22)
Eufy	7/5/22	2 days (7/7/22)	3 days (7/8/22)
Apple	8/29/22	Same day (8/29/22)	5 days (9/3/22)
Google/Nest	7/14/22	Same day (7/14/22)	7 days (7/21/22)
Arlo	8/29/22	1 day (8/30/22)	14 days (9/12/22)
DLINK	8/29/22	8 days (9/9/22)	22 days (9/20/22)
Blurams	7/5/22	11 days (7/20/22)	22 days (7/27/22)
Logitech	8/29/22	2 days (8/31/22)	32 days (9/30/22)
SimpliSafe	8/29/22	Same day (8/29/22)	129 days (1/5/23)

How the consumer's data access request is verified

- What did the company ask for to verify the request?

CCPA specifies that businesses shall promptly determine whether a data access request is a verifiable consumer request, but there is no definition of a “verified consumer request” and no standards on what companies can ask from a requestor, just that the verification process does not extend the 45-day deadline to return personal information and that any information provided for verification is only used for that purpose.

... The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request. ... The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

- Cal. Civ. Code §1798.130(a)(2)

... [A] business shall, in a form that is reasonably accessible to consumers:

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification.

- Cal. Civ. Code §1798.130(a)(7)

Verification requires a balance between security and burden on the consumer. While some measures should exist to ensure a user's personal information is not sent to anyone who requests it (given how simple it can be to *spoof an email*³⁴), requiring proof of purchase or invoices may place those who can only afford second-hand equipment at a disadvantage. Notably, no company required proof of California residency from the requestor.

Required to send an email from the consumer account

Required an additional reply from the consumer account

Required additional personal information

Required additional product or device information

Required a login using credentials for the account

Required a login using a two-factor authentication method

D-Link³⁵, Eufy, and TP-Link (Kasa Smart) only required the request to come from the email listed on the consumer account.

Logitech requests an email reply from the consumer account confirming the data request.

Wyze requests an email reply including the name on the account and a confirmation code sent to the consumer account's inbox.

SimpliSafe requests the last four digits of the credit card used for the account's subscription. Access to OneTrust portal requires using a temporary code emailed to the requestor's inbox.

Arlo requests the first and last name on the consumer account and serial number of an Arlo device connected to the account.

Blurams requests an email from the consumer account with a screenshot or PDF of the invoice for the purchased camera and the MAC address of the camera.

Google (Nest) required email and password to access Takeout (users can enable second-factor authentication if desired).

Apple required Apple ID, password, and a temporary code pushed to the iPhone associated with the Apple ID.

Ring required email, password, and the user's preferred two-factor authentication method³⁶ to access the Control Center.

How the data are returned

- Was data returned to the consumer?
- What quantity of data was returned?
- How was the data shared with the consumer?

Each company should return data within 45 days or inform the consumer of the need for an extension up to 90 days. We had no issue getting a response from this set of companies within the 45 day window, but we learned that users cannot take for granted that a company's response will actually provide the requested personal information.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

- Cal. Civ. Code §1798.130(a)(2)

The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.

- Cal. Civ. Code §1798.100(d)

No personal data.

**No personal data... oh wait,
here's your data.**

Here's some data.

**Oh, you want data? We have
plenty of data for you.**

Apple - all data related to HomeKit is "inaccessible during transmission and iCloud storage."³⁷

DLink - did not find our data until we sent repeated follow-ups, export tool gave us 1 file (3,144 bytes)

Eufy - initially just sent us a link to their privacy policy. After reiterating our request, Eufy sent us descriptions of data, but not the data itself. After escalating our request, they sent us 1 file (19,846 bytes)

SimpliSafe - initially only sent us descriptions of our data. After follow-up, they sent us 1 file (144,469 bytes)

Blurams - 1 email (241 bytes)³⁸

Arlo - 1 email (1,083 bytes)

TPLink/Kasa - 1 file (7,537 bytes)

Logitech - 2 files (61,452 bytes)

Wyze - 1 file (637,298 bytes)

Ring - archive with 31 files in 17 folders (628,907 bytes)

Google/Nest - archive with 468 files in 41 folders (3,618,509,946 bytes)

The privacy team did respond that they made an error and, due to our followup, fixed their internal processes to prevent future mistakes.

D-Link’s privacy team could not locate our data, but fixed their process after our interaction

D-Link was the only company to send us a negative response to our request, stating that the company did not have any personal information related to our account. Of course, our active account and camera told us that this was incorrect so we asked them to check again. As our investigation of their platform continued, we used the data export tool available on the D-Link customer portal, but wanted to understand why the company gave us a negative response. The privacy team did respond that they made an error and, due to our followup, fixed their internal processes to prevent future mistakes.

How should the average California consumer respond when a company tells them there is no data? For D-Link, we had a working user account so we knew the company was incorrect, but, for various other situations when a consumer is not able to confirm whether a company possesses their personal information or not, it may be practically impossible to confirm whether the company made a mistake.

From privacy@us.dlink.com to our researcher

From our researcher to privacy@us.dlink.com

Sept. 9th

Thank you for your inquiry.
D-Link does not have any Personal Information related to the following:
1. Name: REDACTED³⁹
2. Email: REDACTED

D-Link does not sale, trade, or rent Personal Information to third parties.

Sept. 9th

I have an account with D-Link associated with that email address (Personal Information see attached screenshot of the D-Link app) so I don't understand why there is no Personal Information related to this registration. Can you have your team re-check for data? There should at least be registration information for the account.

Sept. 20th

I was able to download my personal data (name, location, email, ip address, mac address) via the DLink portal that I did not even know existed until I tried to delete my account. I am curious why your team was not able to locate any personal information in response to my request. Thank you for any helpful information!

Sept. 20th

Sorry for the delayed response.

After your initial reply to our response, our team did a further analysis and discovered an internal error resulted in your information not being found. We have since modified the procedure to ensure any such data is located going forward.

Eufy and SimpliSafe sent us data definitions instead of our personal information

Some companies appear to interpret requests for personal information as requests for more information about the company's data collection and storage practices.

Eufy initially sent us an email with a link to their California Privacy notice page on the Eufy website.

Thank you for contacting eufy customer service.

I am deeply sorry about all inconvenience caused to you. Customer's safety and privacy are our top concern. In your case, please know that you can refer to the following link to see how we collect your information. Please know that we will not sell your personal information to any third-party.

<https://support.eufylife.com/s/article/California-Privacy-Notice-1617357656354>

Deeply sorry for all the trouble it has caused. Please feel free to let us know if there is anything that we can do for you. We are always here.

Eufy's initial response only provided a link

After we responded and asked again for personal data, Eufy then sent us a spreadsheet that described the data attributes that the company collects, but not the actual personal data.

		Data Classification	Data Details	Purpose of collection and use	Legal basis
What information we collect	User Personal Information and Product Equipment Information	Account Related Information	Account email address	User login to use device	Obtain user consent
		Location	Country, City	Connect to servers and products, provide services to the products	Necessary for product service
		Device Information	Device list, model, time of activation, sharing information	Connect to servers and products, provide services to the products	Necessary for product service
		User mobile phone information	Mobile phone No. , phone system version	Connect to servers and products, provide services to the products	Necessary for product service
		App information	App version	Connect to servers and products, provide services to the products	Necessary for product service
		Settings and Preferences	camera night vision mode	In order to send instructions to the device, provide product services. At the same time, after switching the device, synchronize the setting information	Necessary for product service
			Path to file of local storage		
Product Log	Log	Automatically or manually collect for App or device operation logs	Record product operation	Necessary for product service	

Eufy's response to our second request for information included this spreadsheet

Using Eufy's escalation process, we requested our personal information for a third time and did eventually receive our personal information in a structured, machine-readable format.

SimpliSafe sent us a PDF describing the type of information about us that the company has collected and stored, but did not send us our personal data. After our follow-up communications, the company included our personal information in a PDF sent 129 days after our original request.

<p><i>Customer Support Calls</i></p> <p><i>(provided by you or automatically collected by the phone carrier when you contact our call center)</i></p>	<p>Commercial Information, Identifiers</p>	<p>Phone number, call recording (to the extent it contains personal information)</p>	<p>To communicate with you</p>		<p>if you call customer support, the phone number you called from and a recording of the call is stored by our call center communications technology provider.</p>
<p><i>Camera</i></p> <p><i>(automatically collected when you use our products and services)</i></p>	<p>Audio, Visual Information</p>	<p>Video data, MAC address</p> <p>(Video recordings are automatically deleted after 30 days)</p>	<p>To deliver our services to you</p>	<p>✓</p>	
<p><i>Order, Shipment and Payment/Billing Information</i></p> <p><i>(provided by you when you purchase, setup and use our products and services)</i></p>	<p>Identifiers</p>	<p>Name, email, , addresses, city, state, zip code, country, last 4 digits of payment card used,</p>	<p>To process transactions, fulfill orders and deliver our services to you</p>	<p>✓</p> <p>Accessible via your email account used to install and view your camera.</p>	
<p><i>Account Identifier/Forum</i></p> <p><i>(provided by you when you setup and use our products and services)</i></p>	<p>Identifiers</p>	<p>User name, email (Forum user name is automatically created based on the email address you provide. You can change this in your account)</p>	<p>To communicate with you, to deliver our services to you</p>	<p>✓</p>	

From the initial response from SimpliSafe - no personal data was disclosed

Google’s Takeout export tool failed multiple times; even when successful, it wasn’t “able to fetch all the data” requested

Larger companies such as Google and Ring provide automated tools to download personal information. These tools allow the companies to respond to the large number of requests from their customers that happen every day. Google states that approximately 3.9 million people requested information via their Takeout portal in 2021.⁴⁰

While these tools benefit consumers by automatically providing personal data within 24-72 hours, the tools do not always work. Takeout failed 2 of the 5 attempts we tried for our test Google account, both when only exporting Nest data and when exporting a combination of Nest and other Google services.

← Manage your exports

Export	Created on	Available until	Details
Nest 3.37 GB	July 26, 2022	August 7, 2022	Show exports ▼
Nest	July 24, 2022		! Export failed Try again ▼
4 products 2.9 MB	July 18, 2022	Expired	▼
38 products	July 14, 2022		! Export failed Try again ▼


[Create new export](#)

Fortunately, we could simply request the data again and cross our fingers that the next attempt would be successful. Surprisingly, each of our successful Nest exports were accompanied by a message stating that the tool did not fetch all the data we requested.

← Manage your exports

Export	Created on	Available until	Details
Nest 3.37 GB	July 26, 2022	August 7, 2022	Show exports ▲


We weren't able to fetch all the data you requested. The list below highlights the services that had problems. You can still download your files, but please be aware that there will be data missing. Inside your export you will find an html file that will have more details about the errors.

 Nest !

Exploring the archive created by Takeout, we were informed that there were 130 errors with multiple files that the Takeout service “failed to retrieve.”

Jul 31, 2022, 4:44:05 AM PDT • 3.37 GB • [Learn more](#) about Google archives and your [deleted data](#)

PRODUCTS IN ARCHIVE (1)

 Nest
468 files, 3.37 GB
130 errors!

Data that are still in the process of being deleted are not included in your archive. [Learn more](#) about your deleted data.

Failed Files
Some of the files requested for your archive failed to download. In many cases, clicking on the failed file below will take you directly to the file within its original service. Other times this was caused by a file that was somehow corrupted (e.g. a photo that was only partially uploaded) and is not recoverable. You can retry your download [here](#) or use the link in the menu at the top of that page to send us feedback.

- camera
- geofence
 - geofence_events.jsonl
- homeaway_history
 - home_away_assist.jsonl **Service failed to retrieve this item**
- nestgraph
 - notifications.jsonl **Service failed to retrieve this item**
- subscriptions
- timeofusemetadata
 - time_of_use_metadata.jsonl **Service failed to retrieve this item**
- user
- wnn
 - resource_usage.jsonl **Service failed to retrieve this item**

Using Google’s privacy inquiry form (support.google.com/policies/contact/general_privacy_form), we requested these files. 51 business days later, Google responded that they could not find the requested information related to our Nest device.

We understand that you requested information relating to Nest videos and various data points (specifically homeaway_history, nestgraph, timeofusemetadata, and wwn) for the Google Account associated with the email address **email 1**

After a diligent search, Google has been unable to locate any data responsive to your request. For information about how Google retains data we collect, please visit: <https://policies.google.com/technologies/retention>. There, you can review our data deletion policy regarding when we delete data, to make sure that your data is safely and completely removed from our servers.

We do not know why the Takeout tool would call its lack of data retrieval an “error” if the data, according to Google’s representatives, cannot be located. This interaction leaves us with a modern day philosophical query: *Does your data even exist if the Google Takeout tool cannot retrieve it?*

What the data look like

- In what format was the data returned?
- Is the data readable by a human?
- Is the data readable by a machine?

Companies are required to send information to a consumer in a way that can be easily understood and, “to the extent technically feasible”, in a structured, commonly used machine-readable format.

Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance.

- Cal. Civ. Code §1798.130(a)(3)(B)(iii)

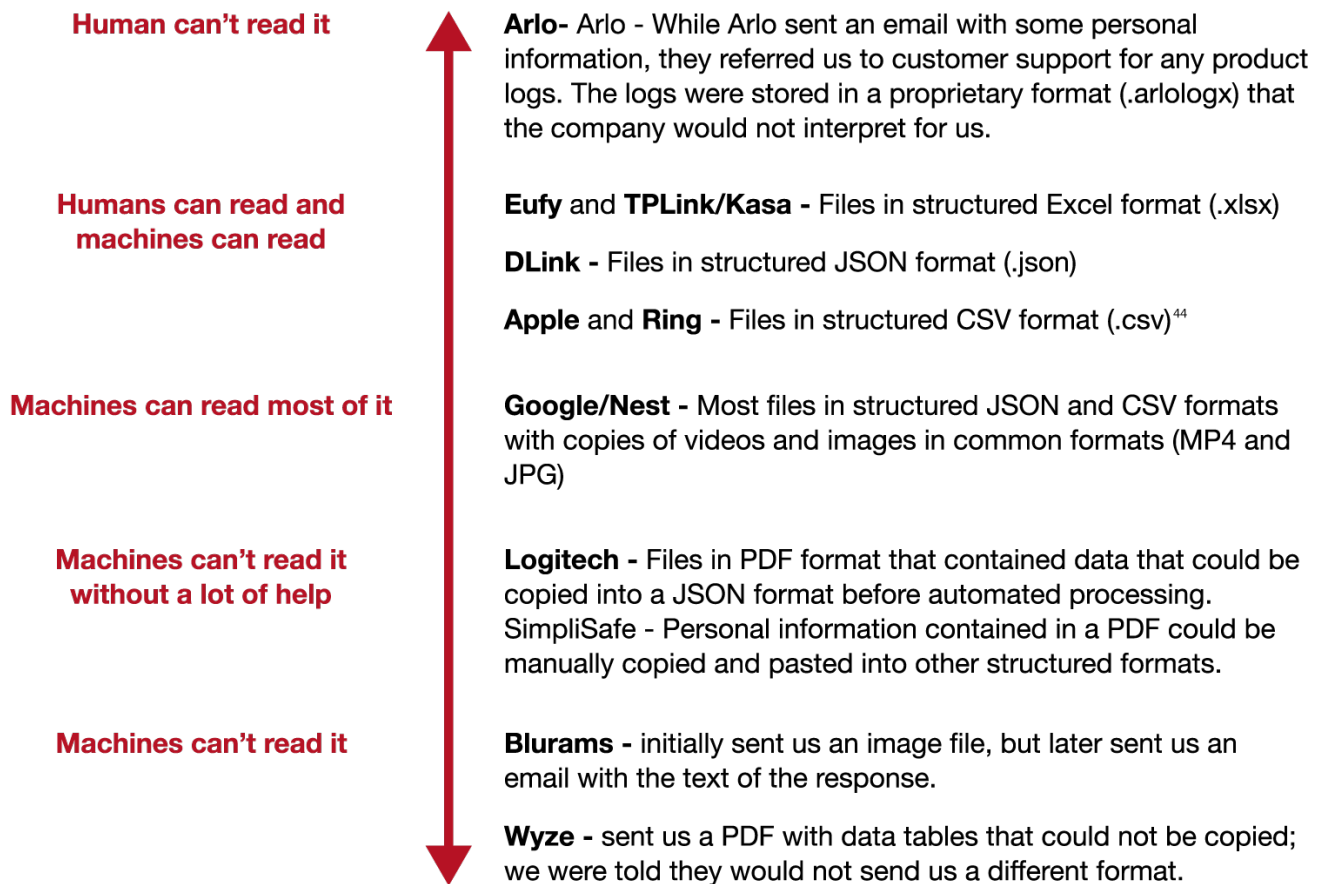
To break these qualifications down, one must realize that “easily understandable to the average consumer” is fairly vague and leaves a company with plenty of room to interpret that. We believe that information should not require special tools or software in order to translate it from raw binary digits into something a human can read.⁴¹ “To the extent technically feasible” also gives companies a bit of independence and flexibility for deciding which formats to send to consumers.

A “**structured format**” refers to formats that typically follow a standard model⁴²; one common example is a spreadsheet where data is placed into rows and columns according to its type. Most data found in a table is “structured” and can be commonly found in filetypes ending in .xls/.xlsx (Excel), .json (JavaScript Object Notation), .csv (Comma-Separated Values), or .xml (eXtensible Markup Language). Less commonly, structured data may sometimes be shared with consumers as lists or tables included within other files such as PDFs (Portable Document Format).

“**Machine readable**” refers to data that can be “automatically read and processed by a computer”⁴³ and again is commonly found in .xls/.xlsx, .json, .csv, .xml, and even basic text files (.txt). While a computer could open and process most files as a series of 1’s and 0’s, machine-readability usually depends upon the data being in a structured model.

Computers will not be able to automatically process a PDF file, but several companies still chose to send them to us in response to our request. Unfortunately for consumers, not all PDFs are created equal. If a PDF includes information tables, sometimes we can simply copy-and-paste that table into a spreadsheet. Other times, the tables were embedded as images that required us to manually transcribe the information for further analysis.

The results from our requests illustrate these differences.



Arlo shares incomprehensible product logs with its users

Arlo responded to our data access request via email that included some personal information such as our name and email address. With regards to cookies / tracking technology and product usage, we were told that the information was included in the app logs.

Cookies and Tracking Technologies: The Arlo app itself collects data but no cookies and Tracking Technologies are collected unless requested by our Support Team for troubleshooting purposes. To know how to access app logs, please reach out to our support through Arlo App>Settings>Support.

Product Usage: These information are also included in the app logs.

From Arlo's emailed response to our data access request

After contacting customer support to learn how to export the app logs from the Arlo mobile app, we were able to access a file of unintelligible hexadecimal numbers. Files such as these do not qualify as “easily understandable to the average consumer” so it is confusing why the user would be directed to this information in response to their data access request.

```
2022-09-13 092002.arilogx x
1 80b1 59f0 593a 790d 088c 06ca 17d3 dd77
2 7d4e 876b 5cce 6132 7bc1 c972 2990 13ba
3 412f a92a 5a15 56af 6fe0 f0e9 52ab 3b82
4 b0d0 9bc8 7435 fcba bb07 467d f566 b5a2
5 4ca0 af23 a72f 44dd ba47 a115 d90b c2a9
6 1fba 765c f645 c27a 5dac b816 9905 dcb6
7 34ec c441 0902 339b fd5b 2c6f 8b69 d6b8
8 c140 7c66 4417 a7ca 37ad 0eac a69d 7999
9 846c df7c 990f 51b8 4c13 1c62 232b 19bc
10 307d 8b8a 3c08 da17 8c54 cc89 78b4 1aad
11 6c36 ae52 8d15 262c 924c 68fc 1a87 e3db
12 650f 917b 425a 03ea 19d6 d3c2 edf8 7c5e
13 0dc3 c267 65ea 5800 ab9e 6a4e 4290 fa53
14 a090 40a3 6f7a 65ae a2bb 4d43 38ff 94f9
15 a604 edbd af89 303c 064c 6629 f97c 8910
16 3d27 a677 c7d9 e645 63bd 33ee 7363 9a3e
17 ea5f ad03 3d3a 7611 e489 27bc bf74 3470
```

A portion of the exported log from Arlo’s mobile app.

When we asked for support from Arlo to interpret the data within this .arilogx file, a customer care advocate informed us that the company does not have any means of translating the logs into a human-readable format.

The logs are usually used by the engineering team for investigation purposes only. Specially when there are bugs that are reported. Unfortunately, we have no means of translating the logs.

The usage of the product depends on the settings that a user sets on the cameras itself.

The response from Arlo when we requested help in understanding the product usage log.

Wyze refuses to provide a machine-readable format despite its feasibility

A frustrating aspect of receiving data in unreadable formats is when the data is shared in a manner that shows how the data existed in a more readable form. For example, Wyze sent us a response using a PDF file that appears to be an export from a spreadsheet application. The limitations of the PDF included not being able to read the entire description for some data attributes and not being able to copy-and-paste the data into another application. ***This response was not machine readable***, but merely an image of something that is machine readable.

Data Request				
Request date:				
Requester:		7/8/2022		
Reply email:				
Support ticket #:				
Your Wyze Account	Description	Data Found (Yes/No)	Value	Value
Name on Wyze Account	First and last name.	Yes		
Wyze User ID	System generated ID.	Yes		
Email	Email address attached to your account.	Yes		
Wyze Nickname	Your nickname or username.	Yes		
Mailing list subscription	Signed up for Wyze newsletters.	Yes	1 Newsletter	
Your Product Data	Description	Data Found (Yes/No)	Value	Value
Wyze Cam v1	Event videos, device settings.	No	No data provided	
Wyze Cam v2	Event videos, device settings.	No	No data provided	
Wyze Cam Pan	Event videos, device settings.	No	No data provided	
Wyze Cam Outdoor	Event videos, device settings.	No	No data provided	
Wyze Doorbell	Event videos, device settings.	Yes		
Wyze Sense	Device settings.	No	No data provided	
Wyze Bulb	Device settings.	No	No data provided	
Wyze Plug	Device settings.	No	No data provided	
Wyze Lock	Device settings.	No	No data provided	
Wyze Scale	App and device settings, health data.	No	No data provided	
Wyze Band	App and device settings, health data.	No	No data provided	
Wyze Sprinkler	Device settings.	No	No data provided	
Wyze Switch	Device settings.	No	No data provided	
Wyze Thermostat	Device settings.	No	No data provided	
Your App Data	Description	Data Found (Yes/No)	Value	Value
App Platform	Details for each device you have the Wyze app is installed on.	Yes		
App Shop Data	Shop tab interactions and comments.	No	No data provided	
App Discover Data	Discover tab interactions and comments.	No	No data provided	
App Membership	Wyze Services subscribed to.	Yes		
App Usage	Account registration date, device activation, etc	Yes		
Your Orders Data	Description	Data Found (Yes/No)	Value	Value
Order History	Your Wyze orders.	Yes	Please log into wyze.com to view	
Order Info	Your Wyze orders details.	Yes	Please log into wyze.com to view	
Order Info: Name	The name on your Wyze orders.	Yes	Please log into wyze.com to view	
Order Info: Billing address	The billing address on your Wyze orders.	Yes	Please log into wyze.com to view	
Order Info: Shipping address	The shipping address on your Wyze orders.	Yes	Please log into wyze.com to view	
Order Info: Contact info	The contact information on your Wyze orders	Yes	Please log into wyze.com to view	

The Wyze data response appears to be an export of a spreadsheet, but without the machine readability.

When we asked for a version of the response in a spreadsheet or other machine-readable format, our request was denied after the customer support representative consulted with their leadership.

From privacy@wyze.com to our researcher

From our researcher to privacy@wyze.com

July 8th

The data request you made on July 5, 2022, is now complete. You can view the data we collect to provide Wyze's services to you by opening the PDF [2193118_data_request.pdf] attached below. For your privacy and security, we will automatically delete this file from our records within 45 days.

July 8th

Thank you for the prompt response! Is it possible to get this data in a spreadsheet or other machine-readable format? A couple of the columns are cut-off in the pdf. Thanks!

July 8th

As I have further checked, the sheet only shows these data: [attached screenshot of pdf]. There are no other characters shown on the right side of the page/columns. If you feel that you are not seeing the same image I have shared here, please try viewing the file with another browser.

July 8th

Thanks for the response, [name redacted]. I wanted to know what the "Description" for "App Usage" and "Order Info: Contact Info" were as it appears they are both cut-off. I tried a different browser... :(Can you please let me know?

July 14th

I may need to coordinate this with our team. I'll send you an update on this once I have gathered the data that you are requesting.

July 23rd

This is the only file that we can provide to you as per our lead. I hope this is the one that you need. Please do let us know if you need further assistance.

Blurams tried to send us a picture

A strange response from Blurams indicated possible bugs to work out in their internal processes. The company tried to send us a response via an attached picture. When we attempted to download the PNG file from their Zendesk service, we received an error message. After our follow-up, Blurams copied our personal information into the body of their email response.

	From privacy@blurams.zendesk.com to our researcher	From our researcher to privacy@blurams.zendesk.com
July 27th	Thanks for the information. We are glad to provide the information for you, please see the attached picture. Attachment(s) [email redacted]information.png	
	July 27th	The link does not work. It says "Not Found You've reached this page because what you were looking for does not exist or there's been an error."
July 27th	Thanks for letting us know. We are glad to provide the information here, please refer to the below: Account: [redacted] Device name: [redacted] Status: Normal MAC address: [redacted] S/N: [redacted] Model: [redacted] Firmware: [redacted] Register time: [redacted] Timezone: America/Los_Angeles PDT	

What the data represent

- Were definitions provided to explain the data?
- How do the definitions assist in understanding the data?
- How else can a consumer interpret the data?

Other than stating that data responses should be “easily understandable to the average consumer,” CCPA does not specifically mandate how the companies might help consumers make sense of the request. From our experience, most companies across every industry do not offer much explanation on what the data mean or how to find certain identifiers within a response.

While personal data that is labeled like “*First Name*” or “*Phone_Number*” may be easily deciphered in a short file, there can be two issues. In a response with hundreds of data values (such as the case with Ring and Google/Nest), finding all the files with a certain category of information (for example, finding all of one’s personal identifiers - names, phone numbers, email addresses - or all online activity - IP addresses, network IDs) becomes cumbersome and time-consuming. Secondly, even consumers with computer science backgrounds may not understand data labeled with names such as “*private_state.is_cz_update_state_ok*”, “*aux_primary_fabric_id*”, or “*bindAt*”.

We wanted to highlight how home video surveillance companies approached this issue of understandability. Human comprehension of a list of data is subjective and highly favors those consumers with technical literacy, but companies can help those that may want to understand what the information means to them by providing definitions or descriptions of data attributes.⁴⁵ Also, if providing the consumer with a large archive with many files and folders, providing a map to find relevant information is also helpful.

Only 2 companies (Eufy and Wyze) provided any definitions or descriptions of the included data with the data response. Google/Nest provided a list of rough descriptions for each folder in the response, which is more useful than nothing.

Wyze and Eufy provided short descriptions for each data attribute

While their descriptions are not detailed, we believe the practices of Wyze and Eufy to offer some explanation of the data helps consumers to understand the meaning of the data held by those companies.

Your Wyze Account	Description	Data Found (Yes/No)	Value
Name on Wyze Account	First and last name.	Yes	
Wyze User ID	System generated ID.	Yes	
Email	Email address attached to your account.	Yes	
Wyze Nickname	Your nickname or username.	Yes	
Mailing list subscription	Signed up for Wyze newsletters.	Yes	

A sample of Wyze’s response (data values are redacted by us). Note the description column.

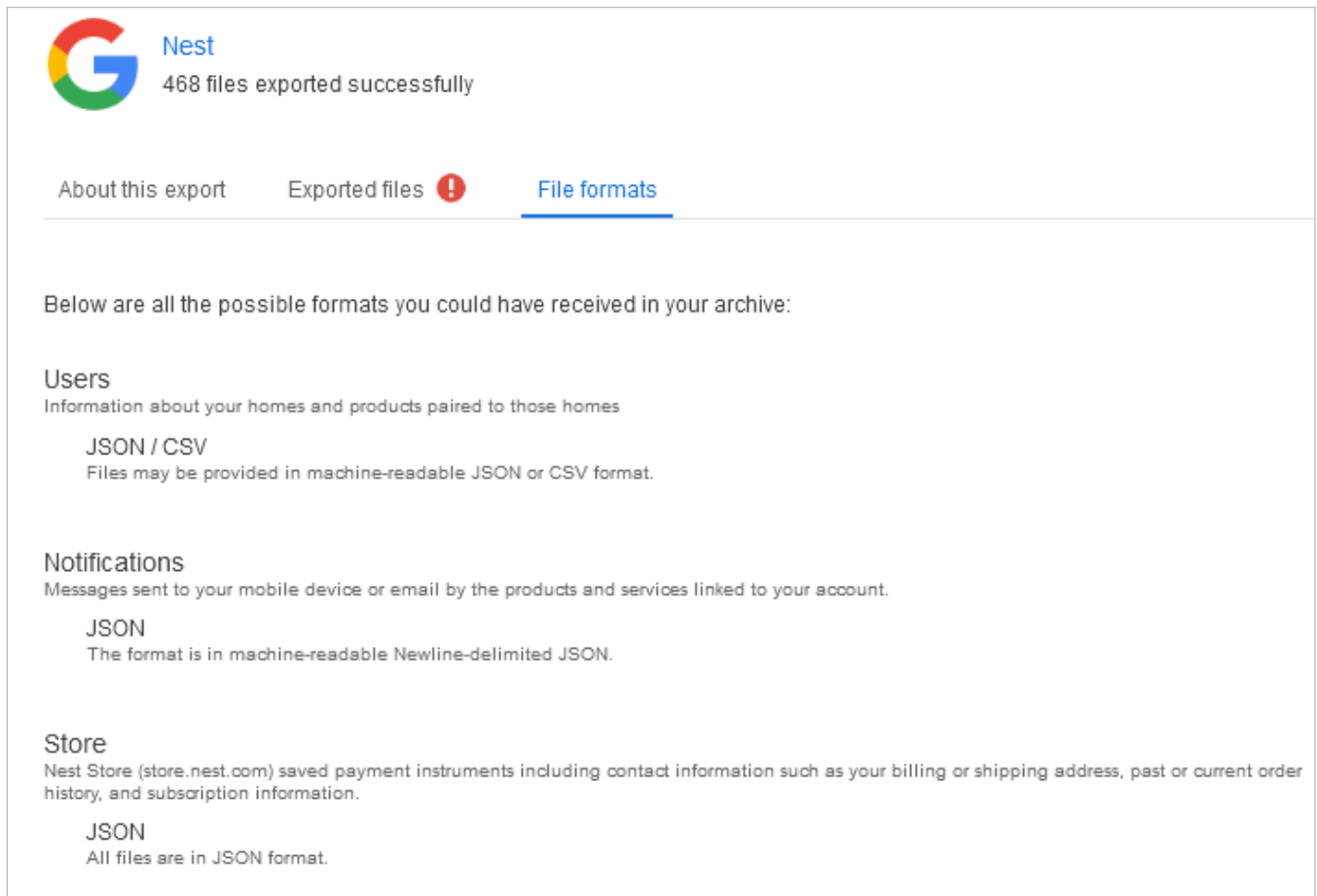
Can the descriptions be improved upon? Certainly - Eufy's response repeats a vague purpose and legal basis for both location and device information - but some description - as long as the company does not mislead the consumer - is better than no description.

Data Classification	Data Details	Purpose of collection and use	Legal basis
Account Related Information	[REDACTED]	User login to use device	Obtain user consent
Location	[REDACTED]	Connect to servers and products, provide services to the products	Necessary for product service
Device Information	[REDACTED]	Connect to servers and products, provide services to the products	Necessary for product service

Eufy's vague descriptions of purpose and legal basis in their response (data details redacted by us)

Google describes the contents of folders included in their Nest archive

The exported archive from Google's Takeout tool includes a file named `archive_browser.html`. If the user opens this file in a web browser, they can view information about the archive that includes plain language descriptions about each folder in the archive. These descriptions also tell the user which file formats to expect in each folder. Although each data attribute is not described and users are not directed to specific categories of personal information (which files contain personal identifiers, geolocation data, or network activity, for example), these descriptions are helpful for navigating such a sizable data export - the archive's 468 files contained at least 438 separate data attributes according to our analysis.

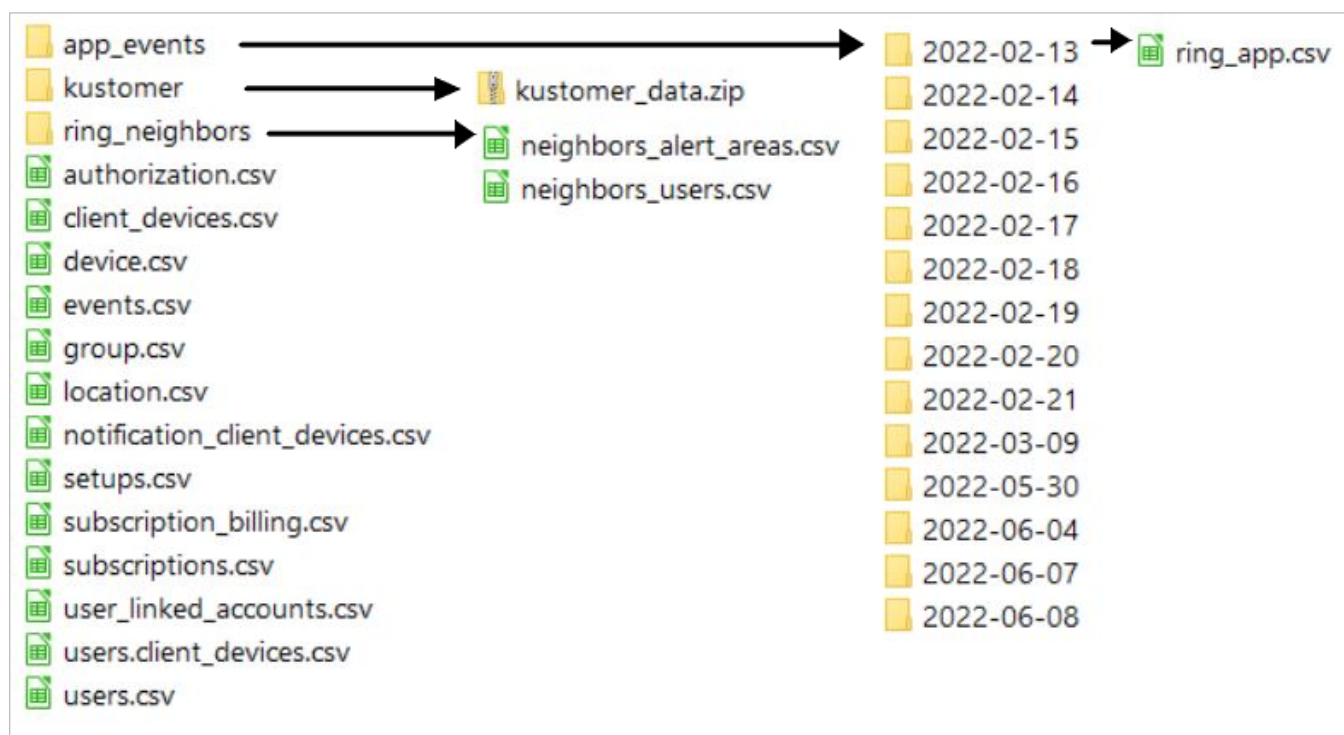


The screenshot shows a web interface for a Google Nest archive. At the top left is the Google logo and the text "Nest 468 files exported successfully". Below this are three navigation tabs: "About this export", "Exported files" (with a red exclamation mark icon), and "File formats" (which is underlined in blue). The main content area is titled "Below are all the possible formats you could have received in your archive:". It lists three categories: "Users" (Information about your homes and products paired to those homes), "Notifications" (Messages sent to your mobile device or email by the products and services linked to your account.), and "Store" (Nest Store (store.nest.com) saved payment instruments including contact information such as your billing or shipping address, past or current order history, and subscription information.). Each category lists the file format: "JSON / CSV" for Users, "JSON" for Notifications, and "JSON" for Store.

A snapshot of the folder descriptions in Google's `archive_browser` file

Ring does not provide any descriptions of data attributes or a guide to find specific categories of information in its archive

We assess that, of all companies within our sample, Ring has the most room for improvement in terms of helping users understand the provided information within their response. Ring provides its users with an archive with unintuitive naming as files may be closely named “client devices”, “devices”, “notification client devices”, “events”, or “app_events” without any pointers towards which files contain which categories of personal information.



Our diagram showing the Ring archive folder structure. Each folder titled with a date (YYYY-MM-DD) contains a separate csv with the activity log for the Ring application on that date.

While all files could be opened and understood by a human reader, we were only able to create a clear picture of what Ring has collected on us after writing a computer program to parse through this archive.⁴⁶ As other media outlets have reported, the amount and type of collected information can be surprising once efforts are made to understand the contents of the archive.⁴⁷

Fortunately, the files from Ring are machine-readable; unfortunately, the average consumer does not have the technical ability to perform this level of data analysis. Instead, the consumer needs to make sense of lengthy logs that look like this:

```
Event,Timestamp,Properties
App Opened,2022-02-14 00:02:19,{"Ip Address": "111.111.111.11", "App Version": "v5.49.0 (5.49.0.12)", "OS": "ios",
"Hardware ID": "0ABC98DE-FA7B-6543-2109-87CD65432EF1", "App Brand": "Ring"}
Toggled speaker,2022-02-14 00:02:23,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Toggled speaker,2022-02-14 00:02:35,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
LV Session Orientation,2022-02-14 00:02:38,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Adjusted Volume Slider,2022-02-14 00:02:38,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
LiveCallStatsMain,2022-02-14 00:02:39,{"Ip Address": "111.111.111.11", "App Version": "v5.49.0 (5.49.0.12)", "OS": "ios",
"Hardware ID": "0ABC98DE-FA7B-6543-2109-87CD65432EF1", "App Brand": "Ring"}
App Opened,2022-02-14 00:07:59,{"Ip Address": "111.111.111.11", "App Version": "v5.49.0 (5.49.0.12)", "OS": "ios",
"Hardware ID": "0ABC98DE-FA7B-6543-2109-87CD65432EF1", "App Brand": "Ring"}
Toggled speaker,2022-02-14 00:08:05,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Tapped renderer,2022-02-14 00:09:56,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
LV Session Orientation,2022-02-14 00:19:19,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Adjusted Volume Slider,2022-02-14 00:19:19,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Adjusted Volume Slider,2022-02-14 00:19:19,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
```

A portion of Ring's device activity log (ring_app.csv) for a single day

Summary of Data Attributes Shared by Each Company

We analyzed the disclosed data and inventoried what data companies chose to send to us. Every company (except Apple which allegedly does not store our Home data on their servers) sent us basic account information, but only the two largest surveillance vendors, Google and Ring, sent us a comprehensive history of our device usage. Only Google includes videos recorded by the device in their export; other companies direct users to use the company's mobile or web applications to review videos.

We have shared our redacted lists of the responses' data attributes online at <https://ccdd-prototype.secure-justice.org>. When the company provided explanations or definitions of the attributes, we have included that information as well.

It is important to note that different users will have slightly different numbers of attributes shared in their own disclosures. These variations may be due to different devices and settings, different subscription statuses, different histories of interactions with the company, and different histories of product usage. Also, what data is included in a response can change over time.

Do we believe that the companies which only shared a couple dozen or fewer attributes actually hold more of our personal information than their privacy teams are willing or technically able to share?

Yes. Every time we logged into those companies’ online web portals, we build a history on their servers that would, at a minimum, associate our personal identifiers (email address for the account) with our computer or phone device information (personal device identifiers) with the identity of our internet connection (IP address, potentially internet service provider) and, in turn, inferences about our location. Unless those companies are proactively deleting such server logs, we should expect that information to be included in a data access response. **Most companies actually tell users that they collect these categories of personal information via their privacy policies posted publicly on their websites.**

We also imagine other consumers would expect video data that a company stores to also be shared during a disclosure. While a company may not decide to transfer a large archive of video, alternative approaches could include providing information about stored videos, including time the video was recorded, the length of the video, whether the video was watched or deleted, and the reason the video was recorded.

Still, each system implementation is different. Companies could choose not to store personal information, device activity logs, or videos on their servers in the interest of privacy and security. It is impossible for consumers to verify a personal data disclosure for completeness and conclude “company X does not store this category of information” on me, especially as each user may have different interactions and configurations with the company’s products.

Company Name	Number of data attributes disclosed	Did the response include device activity logs?	Did the response include videos?
Apple ⁴⁸	N/A	N/A	N/A
Arlo	4	No	No
Blurams	9	No	No
D-Link	60+	No	No
Eufy (Anker brand)	6	No	No
Nest (Google brand)	437+	Yes	Yes
Logitech	33	No	No
Ring (Amazon subsidiary)	165+	Yes	No
Simplisafe	31	Yes	No
TP-Link / Kasa Smart	12	No	No
Wyze	34	No	No



Deleting your data

A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

- Cal. Civ. Code §1798.105(a)

Greetings,

I am a Eufy user and a California resident. I wish to exercise my rights under the California Consumer Privacy Act (CCPA). I request that your business complies with the following requests which are granted to me by the CCPA:

1. Right to delete my information

My details are:

1. Name: [Redacted] First and Last
2. Email: [Redacted] eufy@gmail.com
3. State: California
4. Country: USA

Please delete my personal information. Thank you.

A sample of our emails sent to companies to request data deletion

How to delete data

- Where can consumers find instructions for deleting data?

A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

- Cal. Civ. Code §1798.105(b)




While users can have problems locating the relevant privacy policies, each company did mention the process to request deletion of data in their privacy policies (Blurams does not mention deletion under its section on California rights, but does state that users can request data deletion under the separate section of privacy policy titled “Access to Personal Information”).


We followed similar steps to request data deletion as we performed for requesting access to our data, with a few exceptions discussed below.

Google/Nest deletion is not straightforward

While accessing one’s Nest data simply involves using the Takeout tool and selecting the Nest service, Google’s privacy policy directs its users to four options for deleting information. Unlike requesting access, there’s no specific option for deleting Nest information within these options.

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#) 
- [Delete specific Google products](#) , including your information associated with those products
- [Delete your entire Google Account](#) 



[Delete your information](#)

Google’s Privacy Policy and its links to other webpages did not specifically address deleting Nest data.

Google provides a form to ask privacy-related questions.⁴⁹

Hi, I can’t understand how to simply delete all data Google has collected associated with the Nest. According to California privacy law, I should be able to delete the data associated with my Nest. The Google Privacy webpages give a bunch of irrelevant links. Can you please simply fulfill the request? Thank you!

While we hoped Google might simply delete our Nest-related data, we received a response with instructions on deleting our entire Google account.

Delete your Google Account

You can [delete your Google Account](#) at any time. If you change your mind or accidentally delete your account, you might be able to get it back. [Learn how to recover your account.](#)

Once your account is deleted, all your data and account content is removed from our systems after a certain amount of time. In some cases, Google is required to retain data for longer, and [our retention policy](#) describes why we hold on to different types of data for different periods of time.

From Google's email response to our deletion inquiry

We were also warned that by deleting our account, we'd not be able to use Gmail, Drive, and Calendar, any movies, games, or music purchased on Google Play, information we've saved in Chrome, among other things.

Once you delete your Google Account, you'll no longer be able to use the following:

- Services that require you to sign in, like Gmail, Drive, and Calendar;
- Data associated with your account, including emails, photos, and records of transactions;
- Subscriptions on YouTube;
- Content you purchased on Google Play, like movies, games, or music;
- Information you've saved in Chrome;
- Your Gmail username. Once it's deleted, you can't use it again later, and you can't create a new Google Account with the same username.

From Google's email response to our deletion inquiry.

This warning highlights how users do not have the ability to only delete their information related to the Nest camera. While CCPA was not drafted to provide users with the right to delete their personal data related to a single service from a company's holdings, we'd argue that the CPRA should be enforced this way to effectuate consumers' right to request deletion in instances where large companies offer many services to California consumers. Moreover, this issue would cause consumers to rethink linking their home surveillance activity to the rest of their Google account, which would both narrow viable options for consumers in the market and may result in revenue loss for companies offering multiple services without offering consumers the ability to delete on a per-service basis.

Users are able to delete *some* of their Nest data.

Google does have a FAQ on Nest privacy in its Help Center⁵⁰ that proves slightly more helpful as it at least provides instructions for users on how to delete any videos using the Nest app.⁵¹

How can I delete data associated with my use of Nest and Home devices? ^

- **Google Home search history and voice recordings:** See the "Data deletion" section of [Data security and privacy on devices that work with Assistant](#).
- **Google Assistant activity:** [Delete your Google Assistant activity](#)
- **Nest Cam:** [How to delete your camera's video history and snapshots](#)
- **Nest Aware Sound Detection:** [Learn about sound detection on speakers and displays](#) to delete Nest Aware sound detection clips.

The options available to Nest users for data deletion beyond deleting their entire Google account.

We followed the instructions titled "How to delete your camera's video history and snapshots" and compared the data exports performed via Google's Takeout service.

Export	Created on	Available until	Details
Nest 3.37 GB	July 26, 2022	August 7, 2022	Show exports ▼

"3.37 GB" of data before deleting camera video history (takeout.google.com)

Export	Created on	Available until	Details
Nest less than 1 MB	November 7, 2022	November 15, 2022	Show exports ▼

"Less than 1 MB" of data after deleting camera video history (takeout.google.com)

While the data export size was reduced dramatically, mainly due to the removal of large video files and the camera-specific logs, the new export still returned at least 197 data attributes about our Nest activity!

Google account deletion is simple, but does not specify Nest data removal.

We did perform a Google account deletion. The process immediately disables the user's account and all associated services.

Please read this carefully. It's not the usual yada yada.

You're trying to delete your Google Account, which provides access to various Google services. You'll no longer be able to use any of those services, and your account and data will be lost.

You also could lose access to services outside of Google where you use [REDACTED]. For example, if you use this email address as a recovery email for your bank account, you may have difficulty resetting your bank password. If you proceed, you'll need to update your email address everywhere you use it outside of Google.

From myaccount.google.com/deleteaccount

While Google's plain language about the ramifications of account deletion are clear and simple, Google does not actually specify Nest activity in the list of content to be deleted leaving the user to assume that Nest is one of the many unidentified Google services addressed in the below note.

All this content will be deleted

Note: the list below may not contain every Google service affected by your deletion, such as services Google no longer supports. Your data will be deleted from these services as well.



Gmail

48 conversations will be deleted

Most recent: Stream more and spend less with \$10 off *November 9, 3:50 PM*



Contacts

4 contacts will be deleted

Google only lists a couple of their services in the final screen before account deletion.

Logitech offers deletion of all company data, but also just specific services

As Google warns consumers on how deleting their data will remove the user's ability to use any of the company's services, several other companies will make statements that they will include any and all services owned by the company. Like Nest's relationship to Google, Eufy is a brand of the company Anker. Our request to Eufy's support was responded with a similar warning that other Anker offerings would also be affected:

Thank you for contacting Anker and eufy Customer Support and for addressing your concern with us.

Regretfully, if the data is deleted, all data associated with the email address including the order information and any APP account at Anker, Soundcore, eufy and Nebula will also be deleted.

Most companies offering video surveillance in addition to other potentially-less-privacy-impacting services create a situation where users must throw out the companies' other babies with all of the surveillance bath water. We recognized that Logitech offers its users the choice to delete information associated with one of their specific services (in this case, Circle) without deleting all Logitech data.

We are happy to process a deletion request. Can I just confirm whether you would like to delete all Logitech data or just that associated with your Circle account?

Please note; if you delete all Logitech data, it may affect other products/services you have with Logitech such as Astro, Blue, Streamlabs, Options, Logitech G.

Most companies offering video surveillance in addition to other potentially-less-privacy-impacting services create a situation where users must throw out the companies' other babies with all of the surveillance bath water. We recognized that Logitech offers its users the choice to delete information associated with one of their specific services (in this case, Circle) without deleting all Logitech data.

How the consumer's data deletion request is verified

- What did the company ask to verify your request?

A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

- Cal. Civ. Code §1798.105(c)

The verification process of the data deletion requests followed similar steps as the verification of the data access requests. Companies may ask for additional email confirmation that the consumer understands the impact of data deletion on their ability to use the company's products, but the burden placed upon the consumer to prove their identity was not any greater than what was required for receiving personal information. Two companies, Eufy and Blurams, still created concerning interactions during this verification process.

Eufy possibly deleted the wrong account

As Anker (the company that owns the Eufy brand) was one of the companies that did not ask for additional information to verify our data access request, we decided to see whether the company would delete our personal information if we requested the deletion from an email address that was not associated with our Eufy account. To our surprise, the company informed us that they had deleted our account!

Our login to the Eufy application and website still worked, so we followed up to ensure the company deleted our account. The Eufy representatives then realized the discrepancy and asked for our deletion request to originate from the email address associated with our Eufy account.

We do not know what Eufy's representatives may have deleted when they first informed us that our deletion request was successful. Our hypothesis is that Eufy's employees checked whether an account existed for our second email address and, after seeing that no account existed, informed us that the account was deleted.

From support@eufylife.com to our researcher

From our researcher to support@eufylife.com

Aug. 2nd

Sent from EMAIL2eufy@gmail.com
requesting the deletion
of any information associated
with EMAIL1eufy@gmail.com

I am a Eufy user and a California resident. I wish to exercise my rights under the California Consumer Privacy Act (CCPA). I request that your business complies with the following requests which are granted to me by the CCPA:
Right to delete my information
My details are:
Name: REDACTED
Email: **EMAIL1eufy@gmail.com**
State: California
Country: USA
Please delete my personal information. Thank you.

Aug. 2nd

Thank you for contacting Eufy customer service. We have received your email, and the ticket number for this case is REDACTED.

We do our best to respond within 24 hours (excluding holidays). Thank you in advance for your patience as we look into your request.

Aug. 4th

Thank you for contacting eufy customer service. Sorry for my late response.

Please know that we have deleted your account from our official website.


Aug. 4th

My account and any data for **EMAIL1eufy@gmail.com** should be deleted from the mobile application too. When will this be effective?


Aug. 5th

Thank you for your quick reply.

I am deeply sorry that we are not able to delete the information and data for **EMAIL1eufy@gmail.com**. Please contact us via that email authorization for us to operate.



Any company requesting a user's unencrypted password over email should raise concerns about their ability to protect the security or privacy of their customers' data.



Blurams asked for our account password via email

After requesting deletion of our information with Blurams, their customer support representative showed a serious lack of good security practice by asking us to provide them with our password. Emailing passwords and sharing passwords directly with company employees unnecessarily raise the risk of personal data breaches and account takeovers.⁵² As many internet users reuse the same password on multiple platforms, this practice also increases the chances of an unauthorized individual accessing the user's accounts on other websites.

Any company requesting a user's unencrypted password over email should raise concerns about their ability to protect the security or privacy of their customers' data. The CCPA itself states that “[a] business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5”.

From support@blurams.com to our researcher

From our researcher to support@blurams.com

Aug. 4th

I am a Blurams user and a California resident. I wish to exercise my rights under the California Consumer Privacy Act (CCPA). I request that your business complies with the following requests which are granted to me by the CCPA:
Right to delete my information
My details are:
Name: REDACTED
Email: **EMAIL1@gmail.com**
State: California
Country: USA
Please delete my personal information. Thank you.

Aug. 4th

If you don't mind, may we know the reason why you want your account deleted? Also if you could provide us the password so we can help fix it better. Looking forward to your reply.

Aug. 4th

I want to delete it because I no longer need it. I will not send you my password over email. That is inappropriate.

Aug. 4th

I understand your concern. Let me forward your request then to the responsible team. Please be patient, they will get in touch with you within 24/48 hours for an update via email. Thank you for your patience and kind understanding in advance.

Aug. 9th

If you want to delete/cancel the account from our cloud server. Please go to blurams app>- [Me], Tap the top right icon, then Tap [Account]>- [Account cancellation]. Please read the confirmation carefully, then enter the verification code to finish it.

When was data deleted

- How long did the company take to acknowledge the deletion request?
- How long did the company take to delete the information?

Companies operating in California shall confirm the receipt of deletion requests within 10 business days and delete California-based consumers' data within 45 calendar days (or 90 days with an explanation of the delay) of the request.

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

(b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

- Cal. Code Regs. Tit. 11, §7021

3 of 10 companies failed to acknowledge our data deletion requests within 10 business days. 2 companies failed to delete our information within 45 days.

Overall, the fulfillment of our data deletion requests took longer than our data access requests. We expected the additional timeline due to the technological complexity of removing data from all company storage, however three companies (TP-Link/Kasa Smart, D-Link, and Wyze) did not even acknowledge our deletion request until we sent follow-up emails to each company.

Company Response Time⁵³

Company Name	Initial Request Date	Business days until acknowledgement of data deletion	Calendar days until confirmation of deletion
Google/Nest	8/29/22	8 days (9/9/22)	Same day (11/11/22) ⁵⁴
Ring	8/29/22	Same day (6/22/22)	9 days (7/1/22)
Blurams	8/4/22	Same day (8/4/22)	11 days (8/15/22)
Arlo	9/28/22	1 day (9/29/22)	9 days (10/7/22)
Eufy	8/5/22	1 day (8/8/22)	11 days (8/16/22)
Logitech	10/4/22	1 day (10/5/22)	38 days (11/11/22) ⁵⁵
TP-Link/Kasa Smart	9/28/22	24 days (11/2/22)	37 days (11/4/22)
D-Link	9/20/22	32 days (11/4/22)	45 days (11/4/22)
Wyze	8/4/22	13 days (8/23/22)	Not Completed Yet
Simplisafe	1/6/23	Same day (1/6/23)	49 days (2/24/23)

Wyze has not deleted our data yet

Our request for data deletion from Wyze is an ongoing saga of follow-up emails with no resolution.

From privacy@wyze.com to our researcher

From our researcher to privacy@wyze.com

Aug. 4th

I am a Wyze user and a California resident. I wish to exercise my rights under the California Consumer Privacy Act (CCPA). I request that your business complies with the following requests which are granted to me by the CCPA:
Right to delete my information.

My details are:
Name: REDACTED
Email: **EMAIL1wyze@gmail.com**
State: California
Country: USA
Let me know if you have any questions. Thank you.

Aug. 22nd

Greetings Wyze team,

I am hoping you can help with this data deletion request. By California law, your company is supposed to confirm receipt of this request within 10 business days. Can you please confirm this request and help perform this action? Thank you.

Aug. 23rd

Thank you for reaching out to Wyze. We have received a request to delete your data and in order to do so, your account.

Please confirm that **EMAIL1wyze@gmail.com** is the account that you have on file and wish to have removed. Once we receive your confirmation your account will be submitted for deletion. No follow-up message will occur as your email address will also be removed from our system.

Aug. 23rd

Thank you. I confirm the deletion for this account.

Aug. 25th

We recently wrote to you about your request (#REDACTED) but we haven't heard back from you. Please let us know if your issue has been resolved, or provide any additional information so that we can continue helping you.

Below is a copy of the messages for your request. You can reply to this email to continue working with us on this request. Thanks!

Aug. 27th

We haven't heard back from you about your request #REDACTED. Please reply back to let us know if you are still having an issue or if you're busy simply reply back when you have a chance.

Below is a copy of the messages for your request. You can reply to this email anytime to continue working with us on this request.

Aug. 29th

Yes, I confirm. Please proceed with the deletion.

	<p style="text-align: center;">Sept. 19th (also sent to support@wyze.com)</p>	<p>I am still trying to delete my account. So far when I log in, the account is still available. Do you know why it is taking so long? I have confirmed this deletion request multiple times.</p>
<p>Sept. 19th</p>	<p>Thanks for reaching out to Wyze. This is an auto-reply to let you know that we've received your message and we'll get you a human response as soon as possible. Hang tight!</p>	
	<p style="text-align: center;">Oct. 27th</p>	<p>It's been over 30 days since my followup request and over 60 days since my initial deletion request. I have not seen any confirmation of my data being deleted. In fact, I still get daily emails from Wyze and also can still access the website and app using my account credentials. Please let me know how to proceed - thank you!</p>
<p>Oct. 27th</p>	<p>Thanks for reaching out to Wyze. This is an auto-reply to let you know that we've received your message and we'll get you a human response as soon as possible.</p> <p>While we've got you, Two-Factor Authentication is coming!</p>	

How did you know when or if it was deleted?

- Does the company confirm that personal data was deleted?
- How does the company confirm that personal data was deleted?

California consumers should realize that while a user account can be deleted, the user's personal information might still remain in the company's storage. We think it likely that an average consumer, especially those whose primary language is not English, will mistakenly only ask that their account be deleted even though their intent was to have all their data deleted, not understanding that their request may not include much of the retained personal information that a company has on its servers. As companies can also collect and store data on subjects that do not have accounts, consumers should be given positive confirmation that all of their personal information - not just an account - have been deleted.

We documented whether each company confirmed whether they deleted all associated data. Verbiage that only mentioned account deletion or cancellation does not tell the user that their personal information has been deleted.

Company Name	Does the company confirm data was deleted?	Deletion Confirmation Verbiage
Arlo	Yes	“This email confirms that we have completed your request to delete your personal information from our records.”
Blurams	No, refers to account cancellation.	“Dear users: Your account has been successfully canceled. If you want to continue using it, please register the account again. If this is not your own operation, please consult blurams after-sales service.”
D-Link	Yes, states the data removal is automatic after the user deletes their account by themselves.	<p>“D-Link Systems, Inc. previously deleted your personal information from its database. You should not be receiving any communication from D-Link. Please confirm.</p> <p>However, your camera linked to your mydlink account still shows as active. That account will include some basic personal information required for the account to be active. If you do not wish for that to remain active and want the associated information to be deleted, you need to go into your account and delete it yourself. This is a necessary step to ensure the authenticity of your request. Your deletion of the account will automatically remove all associated information on our end.”</p> <p>-----</p> <p>“Your D-Link account was successfully deleted on 04/11/2022 19:00 as per your request from IP address [REDACTED]. We are very sorry to see you go, but we hope to see you back soon!”</p>
Eufy	No, only affirms that they have “submitted a process”	<p>“Please know, we have submitted a process to delete your information/data/account under this email address. It takes 1-2 business days to have it been finished.</p> <p>Please understand, eufy takes our users’ security and privacy concerns seriously. We strive to ensure that user data is kept secure and that we collect only as much personal data as is required to make our users’ experience with eufy as efficient and satisfying as possible.”</p>

Logitech	No, only gives their timeline to process deletion.	“Thank you for confirming your wish to erase your data. We will process your data deletion request within 30 days.”
Ring	Yes	“Per your request, we’ve deleted your personal data and Ring account. As a reminder, we might keep certain data as required or permitted by applicable law. If you subscribed to Ring Protect, the subscription(s) associated with your Ring account have automatically been canceled and your Ring videos have been deleted. Starting today, you will no longer be able to log into or access your account and your Ring devices are now inactive.”
TP-Link/Kasa Smart	Yes	“The TP-Link ID has been removed from the TP-Link cloud server and all data related to this ID has been deleted. This TP-Link ID can no longer be used to manage the devices.”
Wyze		<i>Pending</i>
Google/Nest	Yes, company requests user confirmation.	“Yes, I want to permanently delete this Google Account and all its data.”
SimpliSafe	Yes, but acknowledges that not all personal information was deleted.	<p>“After verifying your identity with the information you provided, we proceeded with your deletion request and have deleted some of your Personal Information from our systems. We also canceled your SimpliSafe subscription, opted you out of any sales or sharing of your personal information, and unsubscribed you from any future marketing emails from us.</p> <p>Please note, as a customer who purchased our products and/or services, our ability to delete all of your Personal Information data is limited because this information is needed for internal business purposes, such as maintaining business records and for product safety.</p> <p>SimpliSafe will maintain a record of this request for compliance and record-keeping purposes”</p>

Summary of Results by Company

	Apple	Arlo	Blurams	D-Link	Eufy (Anker)	Kasa Smart (TP-Link)	Nest (Google)	Logitech	Ring (Amazon subsidiary)	SimpliSafe	Wyze
Did company effectively share California privacy rights information?	B	A	F	C	A	C	C	A	A	A	A
Did company acknowledge all of our data requests in 10 business days?	A	A	F	F	B	F	A	B	A	A	F
Did company deliver our data within 45 calendar days?	A	B	B	B	B	A	A	B	A	F	A
Did the company delete our data within 45 calendar days?		B	B	B	B	B	A	B	B	F	F
Was the company's request for additional information reasonable?	A	A	F	B	B	B	A	A	A	A	A
Was the company's process free of errors that delayed fulfillment?	A	A	A	F	F	A	D	A	A	F	A
Did the company deliver all data in a human readable format?		F	A	A	A	A	B	A	B	A	A
Did the company deliver all data in a structured, machine readable format?		C	D	A	B	B	A	D	A	C	F
Did the company provide descriptions of data, files, or folders?		C	F	F	B	F	B	F	F	A	B

Apple: Information about Apple's HomeKit data collection was difficult to find since privacy information is not provided within the iOS app nor listed in Apple's generic privacy policy. As Apple states that the company does not have access to HomeKit information, those categories are unscored since no data were delivered or deleted.

Arlo: Personal information, with some limited descriptions of the data, was returned in the body of the email and directed customers to contact support to access device usage logs. Unfortunately, those logs are stored in a proprietary format which Arlo states cannot be translated for customer review.

Blurams: Required CCPA information was not located on their website or iOS app. Access request was not answered until our follow-up was sent to their customer support. Additional information requested by Blurams was burdensome and unsafe; they requested the password to the user account and a copy of the invoice from the device purchase. Blurams attempted to deliver data via an image file, but ultimately sent minimal information in the body of an email.

D-Link: Privacy policy versions lacking CCPA instructions are found when using the iOS app and user portal. D-Link's privacy team responded that no data could be found, later admitting that they made an error upon our followup. No descriptions of data attributes were provided. D-Link also did not confirm receipt of our deletion request within the required 10 business days.

Eufy (Anker): In response to our data request, Eufy originally sent us a link to their privacy policy. After reiterating our request, Eufy sent us descriptions of data. After escalating our request, we received one file with some personal information. For our deletion request, Eufy initially confirmed deletion of the incorrect account before requesting additional information from us.

KasaSmart (TP-Link): Conflicting contact information was found in their privacy policies. TP-Link did not acknowledge our deletion request within the required 10 business day window. Data response did not include descriptions.

Nest (Google): Consumers may sift through the old Nest website, Google's generic policies, and Google's Nest-related web pages to find relevant privacy information. Google's Takeout tool would not retrieve Nest data at times citing system errors.

Logitech: Data response was in PDF format, but data could be copied into a text file. Data response did not include descriptions.

Ring (Amazon): Data response did not include descriptions or map despite its size and complex file structure.

SimpliSafe: SimpliSafe's original response only contained descriptions of data without our personal information. The company eventually took 129 days to deliver our personal information albeit in PDF format. They deleted our information after 49 days.

Wyze: Wyze did not acknowledge our deletion request within 10 business days and has still not performed deletion. Data response was delivered in a PDF format that could not be copied into a text file. Wyze refused to provide another format.

Conclusion

Accessibility may be the biggest obstacle to the average consumer benefiting from this new oversight framework. Policymakers, companies, and advocates must understand that the incorporating multiple languages into consumer-facing documents provides consumers greater accessibility to exercise their privacy rights.

Our research was conducted by a team of native English speakers with technical and legal expertise. Most Californians do not have these privileges but are still entitled to their rights guaranteed by law. Similar to the need for federal and state laws governing voter guides, the lack of multiple language privacy policies and privacy management tools will disenfranchise certain demographics from realizing the benefits of the CPRA.⁵⁶

We found that only four companies (Ring, Google, Arlo, and Apple) offered Spanish language policies that included instructions on exercising California privacy rights. Millions of Californians speak Spanish as their first language. Other companies (Eufy, D-Link, TP-Link, and Logitech) may have a Spanish-language policy but those policies are tailored to European users or are out-of-date. We could not find Spanish-language policies from Wyze, Blurams, or SimpliSafe.

Non-English speaking consumers may be directed to using their browsers' automatic translation capabilities, increasing the burden on the consumer's technical abilities and opening the door to incorrect translations especially as to legal obligations or terms:

We are sorry to tell you that we don't have a privacy policy in the Spanish language. However, you can translate the policy by opening our website from Google Chrome, clicking on the three dots, then selecting "translate". This way you will be able to get the [SimpliSafe Privacy Policy](#) in Spanish.

Please be aware, if you do not understand any aspects of our Privacy Policy, feel free to contact us. We can always be reached at 1-888-910-1215 daily, 8:00 am - Midnight ET, and one of our expert team members will be ready to help you.

SimpliSafe response to our request for a Spanish language privacy policy

Even choosing privacy and other application settings are more difficult for non-Native English speakers. When using a browser or device set to Spanish-language as the default, we found that only some of the customer portals or applications changed to Spanish, but some companies still share an English-language privacy policy or a Spanish-language policy that does not mention Californian's rights.

In California, language barriers are exacerbated by income level and age. Companies should recognize that not all Californians speak English and provide updated, legally-compliant experiences for those customers. Policymakers should recognize that the state's privacy law requirements for understandability by the "average" Californian excludes many of the state's residents. Privacy advocates should also work to support those affected by this disparity unaddressed by the market and the law.

For Californians

Your privacy is important. Show surveillance companies that they need to respect your rights.

Exercise your privacy rights

Send companies requests for your own information even if you are not an active user of that platform. By demanding that they take your rights seriously, companies will be forced to improve how they manage and share your information, as our research has already demonstrated. Understandability of that information, and overall compliance, is improved when there are more people exercising their rights. The business community needs to understand that consumers are interested in their privacy rights, and that regulators and organizations like ours are watching for compliance concerns.

Choose systems from companies that take your privacy seriously

It is difficult to determine how much personal data a company is storing on you, especially when that company only discloses a portion of the information described within their privacy policies. We believe that the quality of their request processes can serve as an indicator for how much resources a company places towards your privacy. Review the results from this report and rely on other credible sources such as Consumer Reports (<https://www.consumerreports.org/>) or Mozilla's Privacy Not Included (<https://foundation.mozilla.org/en/privacynotincluded/>).

Ask privacy advocates for help

Several organizations – Secure Justice included – care about and fight for your privacy rights. The privacy advocacy community realizes that understanding your digital privacy can require technical expertise or language skills to interpret jargon and navigate apps that the average California does not – and should not be expected to – possess. If you have questions or issues when dealing with a surveillance company, reach out for support. Your rights matter to us.

For Companies

You are on notice that California consumers are watching. Our data privacy rights are not simply a compliance exercise that you can put minimal resources towards. The California Attorney General has already shown a strong interest in enforcing the CPRA.

Perform voluntary disclosure of data access and deletion requests

As CCPA regulations tighten, prepare for consumers, advocates, and policymakers to pay attention to how your company respects their rights to know and delete their personal information. We know that some requests will take longer or need to be refused for legitimate reasons, but Californians need to know that these exceptions are not your standard, otherwise they should take their business to companies that care about their privacy. Transparency reports such as Google’s CCPA Transparency Report⁵⁷ should be the norm:

Type of request	Number of requests	Requests completed in whole or in part	Requests denied***	Average time to substantively respond
Download your data <input checked="" type="checkbox"/> usage*	Approximately 3.9 million	Approximately 3.9 million	N/A (requests processed automatically)	Less than 1 day (requests processed automatically)
My Activity deletion <input checked="" type="checkbox"/> usage*	Approximately 18.9 million	Approximately 18.9 million	N/A (requests processed automatically)	Less than 1 day (requests processed automatically)
Requests to know (via contacting Google)**	683	679	4	15 days
Requests to delete (via contacting Google)**	62	62	0	15 days

From Google’s CCPA Transparency Report for 2021

Fix how you inform users how to exercise their rights

California users should not have to hunt for your instructions to exercise their rights. California privacy rights information should be easy to find on your website, your applications, in web search results, and in the application markets such as Apples’ AppStore or Google’s Play store. Stop sending users to outdated or different versions with conflicting contact information based on how they found the information. This is less of a technical challenge and more due to sloppiness and lack of oversight.

Help users to understand information being disclosed

Californians are asking to see their data so that they understand how much data you are collecting from them and how you are respecting their privacy, yet your company places the burden of sifting through archives and deciphering your vague data attribute names. Other companies are learning and putting the effort to address consumers finished with surveillance without oversight. For example, Twitter, as of June 2022, includes a map with each data access response that tells users which files contain which data attributes that are relevant to CCPA's categories of personal information:

```
=== IDENTIFIERS ===
(Real name, alias, postal address, telephone number, unique identifiers (such as a device
identifier, cookies, mobile ad identifiers), customer number, Internet Protocol address, email
address, account name, and other similar identifiers)

account-creation-ip.js
- accountId: Unique identifier for the account.
- userCreationIp: IP address at account creation.
-----
contact.js
- id: Unique identifiers for the contacts imported to the account.
- emails: Emails of the contacts imported to the account.
- phoneNumbers: Phone numbers of the contacts imported to the account.
-----
email-address-change.js
- accountId: Unique identifier for the account.
- changedAt: Date and time the email address was changed.
- changedFrom: Email address associated with the account prior to the change.
- changedTo: New email address associated with the account.
-----
in-audit is
```

Twitter's data archive includes a helpful README file

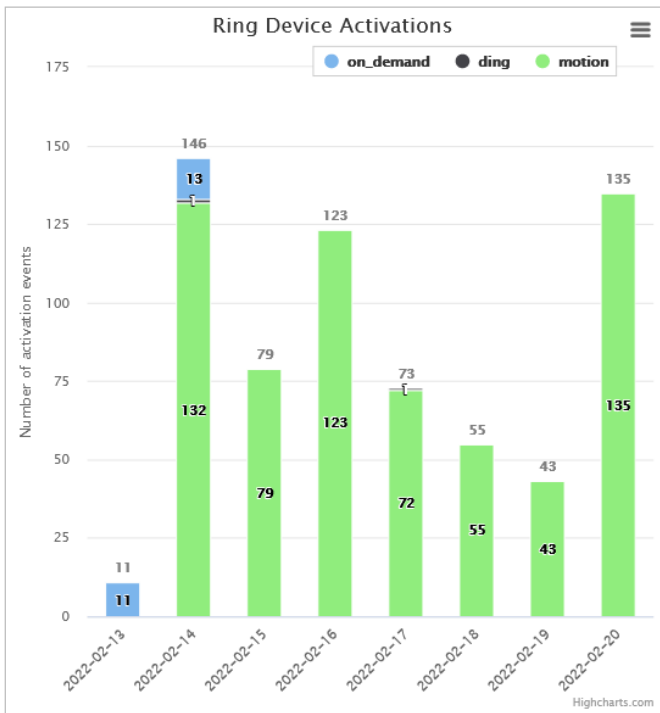
If our non-profit can write scripts to convert your complicated archives into useful charts showing our information, your engineers can too. While your responses might technically comply with CCPA, we don't believe hundreds of logs across dozens of folders is actually understandable to the average Californian. Compare what you send to consumers with what we imagine being a useful, automated view of this data⁵⁸:


```

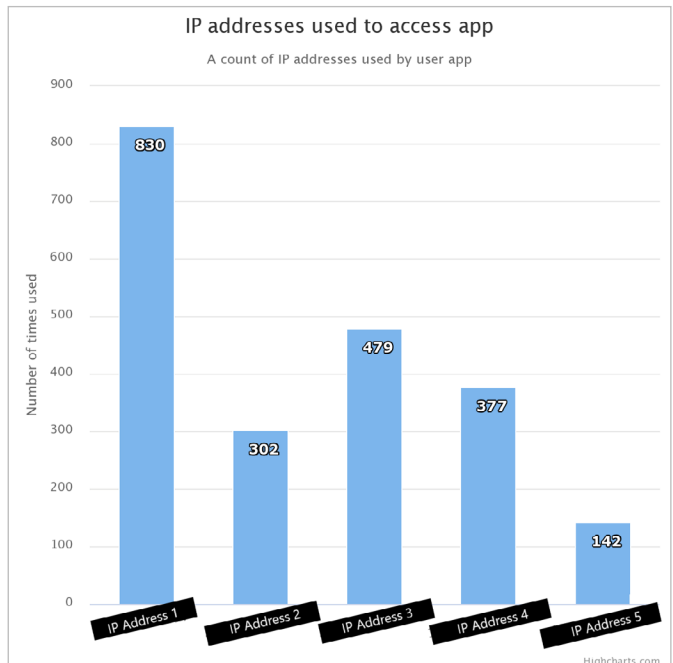
Event,Timestamp,Properties
App Opened,2022-02-14 00:02:19,{"Ip Address": "111.111.111.11", "App Version": "v5.49.0 (5.49.0.12)", "OS": "ios",
"Hardware ID": "0ABC98DE-FA7B-6543-2109-87CD65432EF1", "App Brand": "Ring"}
Toggled speaker,2022-02-14 00:02:23,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Toggled speaker,2022-02-14 00:02:35,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
LV Session Orientation,2022-02-14 00:02:38,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Adjusted Volume Slider,2022-02-14 00:02:38,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
LiveCallStatsMain,2022-02-14 00:02:39,{"Ip Address": "111.111.111.11", "App Version": "v5.49.0 (5.49.0.12)", "OS": "ios",
"Hardware ID": "0ABC98DE-FA7B-6543-2109-87CD65432EF1", "App Brand": "Ring"}
App Opened,2022-02-14 00:07:59,{"Ip Address": "111.111.111.11", "App Version": "v5.49.0 (5.49.0.12)", "OS": "ios",
"Hardware ID": "0ABC98DE-FA7B-6543-2109-87CD65432EF1", "App Brand": "Ring"}
Toggled speaker,2022-02-14 00:08:05,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Tapped renderer,2022-02-14 00:09:56,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App Brand":
"Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
LV Session Orientation,2022-02-14 00:19:19,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}
Adjusted Volume Slider,2022-02-14 00:19:19,{"App Version": "v5.49.0 (5.49.0.12)", "Device Name": "Front Door", "App
Brand": "Ring", "OS": "ios", "Ip Address": "111.111.111.11", "Device ID": "0a9876543bcd", "Hardware ID":
"0ABC98DE-FA7B-6543-2109-87CD65432EF1"}

```

From Ring's data response



- Account/Subscriber Information
- Ring Device Information
- Client Device Information



Our analysis required us to create different views of this information

Disclose the personal information you are collecting and storing with your users

When you don't want to help consumers understand the mountains of data you've collected from them, your company chooses to send only a handful of data attributes despite what we know your company collects and stores. This practice is no longer going to continue unnoticed. If you don't actually have specific categories of information about a specific consumer, tell them so. Californians are smart enough to realize you are storing more (and sharing with other companies and law enforcement) than what you share with us.

For Advocates

There's work to do for the consumer privacy rights of Californians.

Continue investigations of consumer data rights fulfillment

Additional weaknesses in surveillance companies' privacy processes can be identified by learning how companies fulfill responses and how the data actually appears.

- Expand audits to include additional surveillance companies and take longer looks at changes in company processes over time in response to consumer pressure and legislative changes.
- Expand audits to include third party companies that operate services and systems that support surveillance companies.
- Conduct audits by people whose native language is not English.

Support data access rights of non-native English speakers or persons with low technology literacy/ability through grassroots engagement and legal support

The obstacles we, an organization with technology and legal expertise, faced to exercise our privacy rights caused us to envision the difficulty for the average Californian to learn about the information being stored about them by surveillance companies. CCPA rights are not only for the privileged. Advocates can provide clear guidance or personal support to Californians wanting to exercise their rights and push back against companies that do not uphold the law.

Leverage the privacy movement's technical expertise to create resources for better understanding of surveillance company data collection practices

Several privacy advocates have the technical abilities to create simple tools that go a long way to helping Californians understand their personal data. At Secure Justice, we are working on tools to automate the analysis of massive data archives sent by companies like Ring and Google to show users what exactly the company knows about them. We will also be publishing our California Consumer Data Dictionary later this year (see a working preview of the tool at <https://ccdd-prototype.secure-justice.org>).

For Policymakers

Surveillance companies are not taking Californian's rights seriously. You need to change that.

Require disclosure of a company's data access or deletion request history

Surveillance companies operating in California tell users that their data access or deletion requests are taking "longer than usual", that their data cannot be found, or their request needs to be refused, but Californians want to know that these companies actually adhere to the standards of California law. Reports like Google's CCPA Transparency Report (<https://policies.google.com/privacy/ccpa-report?hl=en>) are useful for awareness on how companies fulfill these requests. Make transparency reports mandatory if surveillance companies are not going to provide this information voluntarily.

Mandate that companies provide explanations when data access responses do not match what categories of information described in companies' privacy policies

Why are surveillance companies operating in California only disclosing a portion of users' personal information when required? Common understanding of how their systems and business models work reveal that their privacy teams are not meeting full disclosure as required by CCPA. Even the companies themselves described more categories of information being collected and stored than what is returned in response to a data access request. While companies will say that not all users will generate all information described in their privacy policies, that the personal information may already have been deleted, or that their systems were not designed to store certain collected information, consumers are left questioning what happened to their personal information. Require companies to tell users when and why categories of collected personal data are not included in their data access responses.

Mandate explanations or maps to personal data attributes in access responses

We assess that most surveillance company's data responses do not meet the CCPA standard of being easily understandable to the average Californian. Try requesting your own data and making sense of it. Next, imagine the challenge for those with much less privilege to understand what surveillance companies are storing about them. Sending Californians data archives without explanations on what the information means is contrary to the intent of the Right to Know provisions of CCPA. **Require companies to provide explanations of the data attributes being disclosed, even telling users which categories of personal information that the data attribute represents.**

References & Notes

- 1 “California Consumer Privacy Act (CCPA)”, Office of the Attorney General, State of California Department of Justice ([California Consumer Privacy Act \(CCPA\) - State of California - Department of Justice - Office of the Attorney General](#))
- 2 According to the Office of the Attorney General, “CCPA applies to for-profit businesses that do business in California, collect consumers’ personal information (or have others collect personal information for them), determine why and how the information will be processed, and meet any of the following thresholds: Have a gross annual revenue of over \$25 million; Buy, sell, or share the personal information of 100,000 or more California residents or households; or Derive 50% or more of their annual revenue from selling or sharing California residents’ personal information” (<https://oag.ca.gov/privacy/ccpa>) Organizations are required to “implement and maintain reasonable security procedures and practices” in protecting consumer data.
- 3 <https://oag.ca.gov/consumer-privacy-tool>
- 4 https://cytrio.com/wp-content/uploads/2023/02/5th-State-of-CCPA-GDPR-Compliance-Report_FNL2.pdf
- 5 <https://foundation.mozilla.org/en/privacynotincluded/>
- 6 <https://www.permissionslipcr.com/>
- 7 <https://www.theverge.com/2022/12/16/23512952/anker-eufy-delete-promises-camera-privacy-encryption-authentication>
- 8 <https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant>
- 9 <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers>
- 10 <https://www.forbes.com/sites/daveywinder/2019/06/23/google-confirms-creepy-new-privacy-problem/?sh=1ae7d0ec9d8b>
- 11 Proposed new rule Section 7060(c)(1), approved by CPPA Board February 3, 2022
- 12 On February 3, 2023, the CPPA Board addressed this issue, adopting newly proposed rule Section 7003(b)(2).
- 13 <https://www.enforcementtracker.com/>
- 14 <https://policies.google.com/privacy/ccpa-report?hl=en>
- 15 On February 3, 2023, the CPPA Board addressed this issue, adopting newly proposed rule Section 7102(a)(1).
- 16 <https://www.crunchbase.com/organization/apple>
- 17 <https://www.crunchbase.com/organization/arlo>
- 18 <https://www.crunchbase.com/organization/blurams>
- 19 <https://www.crunchbase.com/organization/d-link>
- 20 <https://pitchbook.com/profiles/company/169180-03>
- 21 https://rocketreach.co/tp-link-technologies-co-ltd-profile_b5c821e1f42e34bb
- 22 <https://www.crunchbase.com/organization/tp-link-839d>
- 23 <https://www.crunchbase.com/organization/google>
- 24 <https://www.crunchbase.com/organization/logitech>
- 25 <https://www.crunchbase.com/organization/ring>

- 26 <https://www.crunchbase.com/organization/simplisafe>
- 27 <https://pitchbook.com/profiles/company/226606-33>
- 28 <https://web.archive.org/web/20220718062344/https://blurams.com/>
- 29 Blurams Privacy Policy linked from website <https://archive.ph/z12wD>
- 30 Nest Products Privacy Page <https://archive.ph/b9xBd>
- 31 Blurams Privacy Policy linked from AppStore and listed on Google search: <https://archive.ph/4XCQT> differs from the policy linked from the Blurams website <https://archive.ph/z12wD>; Kasa Smart's AppStore entry links to TP Link's privacy policy: <https://archive.ph/29gqL> differs from the privacy policy <https://archive.ph/9peuV> listed on the Kasa website (<https://archive.ph/iVFoN>); DLink's privacy policy that is listed first on a Google search and in their AppStore entry <https://archive.ph/6ftZK> mirrors the one on their customer portal (<https://archive.ph/shQ1W>) compared to the one available on their US site: <https://archive.ph/tVYbl>.
- 32 info@blurams.com is listed on their privacy policy, however, our request to this address was unanswered. A subsequent email to support@blurams.com was answered within 48 hours.
- 33 SimpliSafe's California-specific data request form as of Oct 2022: <https://archive.ph/JlxAj>
- 34 <https://www.proofpoint.com/us/threat-reference/email-spoofing>
- 35 DLink does also allow personal data export from MyDLink which requires an account's email address, password, and two-factor authentication if enabled. DLink uses push notifications to the MyDLink app for two-factor authentication.
- 36 For two-factor authentication, Ring uses random codes sent via text message (SMS) or generated with an authentication app.
- 37 <https://support.apple.com/en-ie/guide/security/sec49613249e/web>
- 38 Blurams initially sent us a link to an image file in response to our request. After we were unable to download the image, they sent us our personal information in the body of an email.
- 39 Redaction of personal information performed by us for this publication.
- 40 <https://policies.google.com/privacy/ccpa-report?hl=en>
- 41 The February 3, 2023 approved proposed new rules do attempt to resolve some of these concerns. Secure Justice will continue to test the real-world application with these vendors, to gauge whether greater utility is being realized by consumers.
- 42 <https://www.geeksforgeeks.org/what-is-structured-data/>
- 43 <https://opendatahandbook.org/glossary/en/terms/machine-readable/>
- 44 Note that this data did not contain any information regarding the linked camera and use of Apple HomeKit.
- 45 In this report, we use the phrase "data attribute" (or simply "attribute") to describe the collected pieces of information such as a user's name, address, email address, subscription status, or GPS location. A "data value" (also called "data point") describes the actual stored values for that data attribute. For example, a user may have 10 different data values or data points for an IP address attribute if the company collects and stores information about the various networks the user may utilize to access their devices.

- 46 Read more about this analysis in the Discussion section of this paper.
- 47 See Wired's "All the Data Amazon's Ring Cameras Collect About You" from 8/5/2022 (<https://www.wired.com/story/ring-doorbell-camera-amazon-privacy/>), archived at <https://archive.ph/dC26v>) or BBC's "Amazon's Ring logs every doorbell press and app action" from 3/4/2020 (<https://www.bbc.com/news/technology-51709247>), archived at <https://archive.ph/yrndx>)
- 48 As noted in this article (<https://support.apple.com/en-ie/guide/security/sec49613249e/web>): "HomeKit stores data about the homes, accessories, scenes, and users on a user's iOS, iPadOS, and macOS devices. This stored data is encrypted using keys derived from the user's HomeKit identity keys, plus a random nonce. Additionally, HomeKit data is stored using the Data Protection class Protected Until First User Authentication. HomeKit data is backed up only in encrypted backups, so, for example, unencrypted backups to the Finder (macOS 10.15 or later) or iTunes (in macOS 10.14 or earlier) through USB don't contain HomeKit data".
- 49 https://support.google.com/policies/contact/general_privacy_form
- 50 https://support.google.com/googlenest/answer/9415830?visit_id=638032239927088364-2347190699&p=privacyfaqs&rd=1#zippy=%2Chow-can-i-delete-data-associated-with-my-use-of-nest-and-home-devices
- 51 <https://support.google.com/googlenest/answer/9219185>
- 52 <https://www.connectria.com/blog/password-security/>
- 53 We did not attempt deleting our Apple information as it appeared no information was stored by Apple as confirmed by an Apple representative. See <https://support.apple.com/en-ie/guide/security/sec49613249e/web> for more information about the privacy and security of Apple's HomeKit system.
- 54 This request refers to following the instructions provided by Google for deleting one's entire Google account. If a user only wishes to delete data related to Nest, they are unable to only delete Nest information beyond specific camera and video history.
- 55 Logitech does not send a confirmation when data is deleted. We attempted to login using our account credentials near the 30 day estimation of request completion from the company.
- 56 In our county of Alameda, federal and state law require a combined thirteen languages for voter guides: Chinese (including Taiwanese), Hispanic, Filipino, Vietnamese, Burmese, Cambodian/Khmer, Hindi, Korean, Laotian, Mien, Mongolian, Panjabi, and Telugu. Alameda County is one of the larger and most diverse counties in California, and likely has an above average technology adoption rate compared to more rural counties. California demographics make it all the more necessary that companies understand what language their customers speak in our diverse communities. <https://www.sos.ca.gov/elections/voting-resources/language-requirements>
- 57 <https://policies.google.com/privacy/ccpa-report?hl=en>
- 58 These visual aid tools were built by Secure Justice's Steve Trush, to aid in the interpretation of the data we received from various companies.