Comments of Consumer Reports
In Response to the
California Privacy Protection Agency's
Invitation for Preliminary Comments on
Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals

By

Matt Schwartz, Senior Policy Analyst, Consumer Reports
Justin Brookman, Director of Technology Policy, Consumer Reports

April 6, 2026

Consumer Reports[1] appreciates the opportunity to provide feedback on the California Privacy Protection Agency's (CalPrivacy) Invitation for Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals (OOPSs). We thank CalPrivacy for initiating this rulemaking, which speaks to a willingness to address common points of frustration and sources of failure for consumers in exercising their privacy rights. One of the key lessons we've learned in the eight years since the initial passage of the California Consumer Privacy Act (CCPA) is that rights are only as strong as a consumer's ability to exercise them without undue burden.

In these comments, we share some general thoughts about friction in the exercise of consumer rights, specific feedback about how the process of submitting requests to opt-out, know, correct, and delete could be better facilitated to ease burdens on consumers, and recommendations for how to better accommodate authorized agents attempting to help consumers exercise their rights. We also share recommendations for how the Agency could approach the regulation of OOPSs to best capture consumer preferences.

Many of CR's recommendations on these topics are informed by shortcomings in consumer request flows we've observed while helping consumers exercise their privacy rights at scale. For instance, through our Community Reports project, we've partnered with volunteers across the U.S. to investigate marketplace issues, including by crowdsourcing data privacy requests under laws like CCPA.[2] Similarly, CR's Permission Slip app acts as an authorized agent under CCPA and has helped consumers submit more than 2 million data privacy requests over the last several years.[3]

Consumer Reports is also a founding member of the Global Privacy Control (GPC) project, an open-source, web-based OOPS with over 50 million unique users each month.[4] Consumer Reports' Director of Technology Policy Justin Brookman is a contributing editor to the project. However, these comments reflect the views only of Consumer Reports and are not necessarily representative of other project participants.

I. Reducing Friction in the Exercise of Privacy Rights

Businesses Should Have to Plainly State if They Are Covered by CCPA

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] Consumer Reports, Community Reports, https://www.consumerreports.org/community-reports/

[3] Consumer Reports, Permission Slip, https://innovation.consumerreports.org/initiatives/permission-slip/

[4] Global Privacy Control, https://globalprivacycontrol.org/. Consumer Reports is a founding member of the Global Privacy Control initiative and regularly participates in the management of the protocol.

As a preliminary matter, it should be simple for consumers to understand whether the company they are interacting with constitutes a "covered entity" under the CCPA and thus is legally required to honor their rights requests. Unfortunately, companies do not always offer clear indications of whether they meet the legal thresholds defined in CCPA Section 1798.140(d) (e.g., the $25 million revenue threshold or the 100,000 consumer data processing trigger) and consumers lack any ability to independently verify these figures.

Many companies' privacy notices are vague about their compliance status per jurisdiction, only offering that consumer rights "may" apply depending on the location of the requester, such as in the following example:

> The additional disclosures that we provide in this Notice are required in a growing number of jurisdictions ("Data Privacy Laws"), and we believe are simply good business practice. Depending on where you live and subject to certain exceptions, you may have some or all of the following rights:

The uncertainty that such disclosures engender may result in a form of informational friction that discourages consumers from even attempting to exercise their rights in the absence of clear evidence that such efforts will be worthwhile. And while the presence of certain design features (e.g. the existence of a "Do Not Sell My Personal Information" footer) or privacy policy verbiage (e.g. a California-specific section of the privacy policy) *imply* that a company is required to comply with CCPA, these are imperfect indicators and in any case are likely only to be interpreted as such by the most sophisticated consumers.

We therefore recommend a plain disclosure of compliance status along the following lines:

> *"The description of consumer rights must unambiguously indicate those rights are available to California residents. Statements such as "you may have rights" or "if your state has a data privacy law" are not sufficiently clear to inform California residents of their rights. Businesses must state the described consumer rights may be exercised by either (i) all users or all United States users or (ii) clearly describe the subset of users, including explicitly identifying California residents, among residents of other states.*"[5]

<u>Expectations for Addressing Broken Links Should Be Higher</u>

Another key source of friction is the presence of broken links within company privacy policies, request forms, or other key privacy documentation. Obviously, without access to these resources, consumers cannot complete requests and are more likely to simply give up than to redress these issues with companies. Section 7004(a)(5)(B) already states that "a business that knows of, but does not remedy, circular or broken links…may be in violation of this regulation," but clearly this warning has not been heeded as well as it should be. CalPrivacy should

[5] This formulation is derived from the Delaware AG's Delaware Privacy Act FAQs, https://attorneygeneral.delaware.gov/fraud/personal-data-privacy-portal/frequently-asked-questions/

strengthen this provision to state that businesses that don't fix broken links within a reasonable time-frame *are* in violation of the law and should monitor compliance with this provision as an element of any future enforcement sweeps.

CalPrivacy Should Amend Rules to Clarify Methods for Submitting Requests

Under CCPA Section 1798.130(a)(1)(A), covered entities that do not operate exclusively online must provide "two or more designated methods" for submitting requests to access, correct, or delete personal information. Unfortunately, even though many businesses purport to support rights requests via email, it is relatively common for those businesses to respond to such submissions by referring users back to a privacy request form, even if the emailed request included all of the information necessary to honor the request. This flow adds unnecessary extra steps for consumers, which is likely to depress the amount of successfully submitted requests.

The below response was received in response to an emailed privacy request:

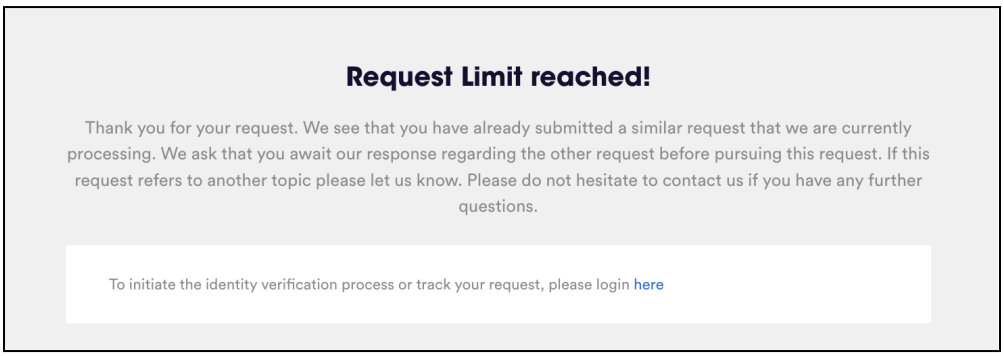
Section 7020 of the Rules should be amended to clarify that if businesses offer a method to submit a request, they must honor the request through that method. Relatedly, the Rules should be clarified to state that in order for a business to satisfy their obligation to provide two methods for submitting requests, requests must actually be honored through both of those methods. For instance, a business' toll-free telephone number should allow consumers to complete a request through that method and not simply direct the consumer to the online webform.

A related point of friction for consumers is the back-and-forth that often ensues when businesses do not disclose in their privacy documentation all of the necessary information needed from consumers in order to make a successful request. For example, consumers may submit requests to access, correct, or delete through email or the webform only to find out days or weeks later that they must in fact log-in to their existing account to complete the request (as provided for under Section 7061(a) of the Rules). Additionally, some businesses have complained about consumers submitting *too much* personal information in emailed rights requests, despite not clearly delineating in their privacy policy the minimum information necessary to successfully action a request. Businesses should be required to disclose the required verification steps to consumers either in the privacy policy, or, ideally, at the point of the

privacy request itself so that consumers do not waste time by submitting insufficiently detailed requests. And if the business accepts requests via a mechanism that does not automatically delineate the necessary submission fields (e.g. email, or toll-free phone number), it should also be required to disclose the minimum information necessary to action a request in their privacy policy.

Finally, some businesses only allow consumers to make a single privacy request at a time. Given that businesses are permitted up to 90 days to complete requests, this is an unreasonable burden on consumers — it should not take 6 months for businesses to complete two privacy requests. Though this practice likely constitutes a "dark pattern" forbidden by the law, CalPrivacy should consider explicitly prohibiting limiting consumer requests in this manner.

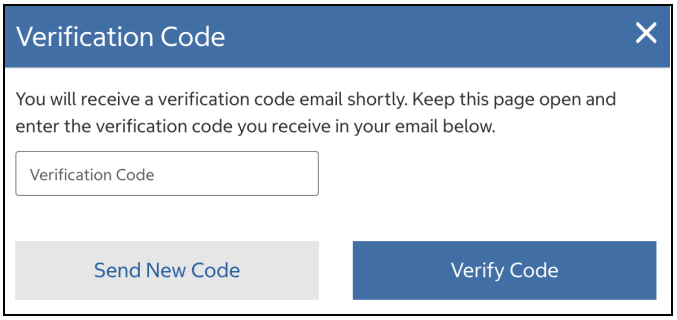
Example:



<u>Many Businesses Impermissibly Require Email Verification for Opt-Out Requests</u>

One of the most common points of friction we've encountered in helping consumers execute their right to opt-out of sales or sharing of their personal information is that many businesses continue to require consumers to verify themselves in spite of CCPA's clear prohibition on such behavior. In a recent audit of 120 businesses required to comply with CCPA, CR found 30 percent of companies engaging in this practice.[6]

For example, as of April 2026, a large national grocery chain requires consumers to verify their emails prior to making *any* privacy request (including opt-outs), as seen below:



[6] This audit was conducted in the course of producing a forthcoming CR publication.

CCPA attempts to address this issue by only requiring verifiable consumer requests to access, correct, and delete, and clarifying in the Rules that businesses "shall not require a verifiable consumer request for a request to opt-out of sale/sharing."[7] In turn, "verifiable consumer request" is defined as any request "that the business can verify, using commercially reasonable methods."[8] CalPrivacy adopted this framework "because the potential harm to consumers from nonverified requests is minimal" and "that some businesses have misused the verifiable request process to impede consumers' exercise of their right to opt-out of sale."[9]

What we often see today flies in the face of CalPrivacy's careful approach. As CalPrivacy has already agreed, there is no compelling public policy reasoning for allowing businesses to throw hurdles in front of consumers attempting to execute opt-out requests. While fraudulent access, deletion, or correction requests can pose real consumer harm, such as identity theft or stalking, opt-out rights do not carry similar risks to consumers and therefore should not be subjected to this heightened standard.

While this ultimately may be more of a matter of enforcement, given the prevalence of these activities CalPrivacy should consider providing additional clarity in the Rules to plainly state that requiring consumers to respond to email verification links constitutes requiring a verifiable consumer request and thus is impermissible under CCPA.

Some Businesses Do Not Provide Inferences in Response to Right to Access Requests

CCPA stands above many other state privacy laws in that it clearly includes inferences within the definition of "personal information."[10] That means that businesses must provide inferences they have created about consumers in response to a verified request to access personal information. Yet, in our experience, several businesses have failed to voluntarily provide this information to consumers the first time around. To combat this, we've helped our members craft responses to companies to request full disclosure of their personal information. And while this has proved successful in some instances, few consumers independently have the wherewithal to engage in extended back-and-forths with businesses to remind them of their compliance obligations.

We recommend that CalPrivacy review this requirement as an area for possible enforcement, and it may be worth the Agency clarifying in the Rules or providing separate guidance that businesses must provide *all* of the personal information they maintain about consumers upon the first time of asking.

---

[7] CCPA Rules Section 7026(d)
[8] CCPA Section 1798.140 (ak)
[9] California Privacy Protection Agency, Initial Statement of Reasons for California Privacy Protection Agency Regulations (July 8, 2022), https://cppa.ca.gov/regulations/pdf/20220708_isr.pdf
[10] CCPA Section 1798.140(v)(1)(K)

Authentication for Rights to Access, Correct, and Delete Remain a Significant Point of Failure

Unlike requests to opt-out of sale or sharing, businesses are allowed to require consumers to submit verifiable requests to access, correct, and delete. Verification methods are required to be reasonable in light of the information being requested, the risk of harm from its unauthorized deletion, correction, or access, and the likelihood of fraudulent or malicious actors seeking it.[11] Despite this, we continue to observe businesses enacting cumbersome authentication flows for consumers that do not correspond with the risks.

A few illustrative examples:

- In order to delete personal information collected by a national office supply store, consumers must accede to multiple rounds of two-factor authentication.
    - When the primary personal information maintained by a business is contact information and non-sensitive purchase history, deletion requests should be easy to execute.
- A national vehicle rental chain requires consumers to make accounts with the business for the purpose of verifying their identity, as well as to *track* the status of their requests.
    - While the statute already clearly prohibits requiring consumers to create an account to *submit* a verifiable request,[12] requiring consumers to create an account to *track* requests also unnecessarily subverts consumer autonomy and should be prohibited, especially if consumers have already provided multiple contact methods that the business could use to provide updates.
- In addition to its webform, a national news service requires consumers to manually fill out a separate "written declaration form" to confirm additional personal details (under penalty of perjury) in order to delete personal information.
    - To the extent possible, businesses should refrain from directing consumers to external platforms or separate form-fills. In this case, the additional requested information could have been just as easily collected through the original webform.

Similar to our recommendation above, CalPrivacy should prioritize a review of authentication standards to determine whether businesses are placing unduly high burdens on consumers. It should also clarify that requiring consumers to make accounts to track requests is unlawful.

Support for Authorized Agents Should Be Improved

We've also encountered a variety of issues when attempting to assist consumers in the submission of rights requests in our capacity as an authorized agent. One issue is that some businesses refuse to communicate with authorized agents, instead directing all communications about rights requests to consumers instead of their authorized representative. This is especially troublesome given that businesses are already permitted to require the authorized agent to

[11] CCPA Rules Section 7060(c)(3)
[12] CCPA Section 1798.130(a)(2)(A)

provide proof that the consumer gave the agent permission to submit the request and to meet other verification standards — which would seem to address possible fraud concerns.[13] Relatedly, in some instances when businesses *do* provide status updates to authorized agents, they fail to provide any identifiers to link the consumer to the request in question — making the tracking of the request functionally impossible.

Leaving agents out of the communications loop even after verification (or providing incomplete information) makes it very difficult for them to assist consumers — creating a scenario whereby agents lack insight into whether the business has simply ignored a request or whether they responded to the consumer via separate outreach. Keeping agents out of the communication loop is bad for businesses as well, given that agents may be under the impression that companies are not complying with the law, when in fact the company has been corresponding solely with the user.

We recommend that CalPrivacy require that businesses that have received verified requests from authorized agents, at a minimum, copy authorized agents in any correspondence relating to the status of a request and include in any such correspondence the relevant information needed to monitor the request.

Future rulemakings may help consumers

We note that in addition to the current rulemaking, CalPrivacy is considering future rulemakings on the topic of standardized privacy forms and notices.[14] Having reviewed hundreds of company rights requests forms, we've found that there is a high degree of variance in their appearance, functionality, and how consumers can locate them. While some degree of differentiation amongst divergent industry participants is inevitable, we agree that driving toward standardization to the extent possible would be helpful in reducing the burden on consumers to understand and execute rights requests across businesses.

II. Opt-Out Preference Signals

CalPrivacy Should Create an OOPS Registry

As we previously commented,[15] we recommend that CalPrivacy create and regularly update a registry of OOPSs that should be treated as legally binding opt-out requests under the CCPA. Having a definitive registry would provide more clarity to consumers and businesses than the current regulations, which only state that OOPSs "shall be in a format commonly used and

---

[13] CCPA Rules Section 7063(a)
[14] California. Privacy Protection Agency, Board Meeting Agenda Item 8: Regulations Update (Feb. 27, 2026), https://cppa.ca.gov/meetings/materials/20260227.html
[15] Justin Brookman, Comments of Consumer Reports in Response to the California Privacy Protection Agency Text of Proposed Rules under the California Privacy Rights Act of 2020, (August 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/08/CPPA-regs-comments-summer-2022-1.pdf

recognized by businesses" and that the signal clearly is "meant to have the effect of opting the consumer out."[16] While § 7025(b)(1) lists "an HTTP header field" as an example of a commonly-used format, it is unclear if any HTTP header — no matter how widely used — created by a developer with the intent of opting users out must be treated as a valid request. Offloading to companies the responsibility for judging whether signals are valid introduces unnecessary ambiguity that bad-faith actors may exploit to frustrate the effectiveness of OOPSs.

This will become especially important with the coming effective date of the California Opt Me Out Act, which will require browser companies to natively support OOPSs by January 1, 2027.[17] This is likely to increase the number of unique and widely used OOPSs on the market, whereas currently the only OOPS with significant usership (and that has been officially deemed legally-binding in California) is the Global Privacy Control. For ease of compliance, the registry should be relatively stable and slow-changing over time — which would make maintenance of the list practical even if each new addition is contingent upon approval by the CalPrivacy board. As Colorado has already proven, creating and maintaining such a registry is readily feasible.[18]

Interstitials Should Be More Strictly Regulated

As businesses are likely to receive substantially more opt-outs through OOPSs starting in 2027, it is critical to ensure that the intent behind OOPSs — to make it easy to universally opt-out — is preserved.

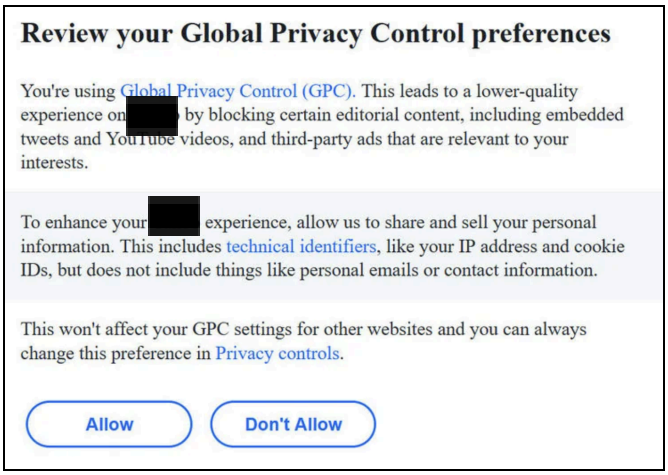
The CCPA Rules currently provide businesses two pathways to respond to OOPSs: the frictionless path and the non-frictionless path. In order to qualify as processing OOPS requests in a frictionless manner, businesses must not respond to OOPSs by charging a fee or requiring valuable consideration, changing the consumer's experience, or displaying notifications or interstitials (though as discussed below this last point potentially clashes with the text of CCPA itself).[19] Satisfying these standards allows businesses to ignore their obligation to provide "Do Not Sell" footer links.

Unfortunately, it appears that many businesses are comfortable with taking the non-frictionless path and have begun responding to OOPSs with interstitials in a manner that, if adopted across the marketplace, is likely to replicate the experience of consent fatigue that OOPSs were meant to alleviate in the first place.

For example:

---

[16] CCPA Rules Section 7025(b)
[17] California AB 566, Section 2 (a)(1), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB566
[18] Colorado Attorney General's Office, Universal Opt-Out and the Colorado Privacy Act, https://coag.gov/opt-out/
[19] CCPA Rules Section 7035(f)



Section 1798.185(a)(19)(b)(v) of CCPA clearly states that CalPrivacy's rules on OOPSs should ensure that businesses do not respond to an OOPS by "displaying any notification or pop-up." CalPrivacy should therefore remove Section 7025(f)(3) from the Rules and instead state that businesses are prohibited from displaying a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal, full-stop. In addition to the text of CCPA itself, the legislature once again expressed its clear intent to make it easy for consumers to universally opt-out with the Opt Me Out Act. However, this intent will be circumvented if every website requires consumers to make individual consent decisions in response to OOPSs.

The current rules also state that a "business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business's sale or sharing."[20] CalPrivacy should amend this provision to clarify that businesses may provide a *separate* link to privacy settings pages or interfaces, but that they may not provide such links in an interstitial or pop-up. The Rules are currently ambiguous on this point.

Additional OOPS Rulemaking Authorities under Section 1798.185(a)(18)(A)

CalPrivacy has so far not exercised all of its authorities under Section 1798.185(a)(18)(A) to issue regulations to specify certain requirements and specifications for opt-out preference signals. We offer thoughts on some of these topics below.

Unfair Disadvantaging of Other Businesses

CalPrivacy is permitted to issue regulations to "ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business."[21] We urge CalPrivacy to consider that there are contexts where OOPSs *should* be

[20] CCPA Rules Section 7025(f)(3)
[21] CCPA Section 1798.185(a)(18)(A)(i)

allowed to treat different controllers differently and that such treatment may not be inherently unfair. A consumer may want to install an OOPS that is targeted specifically at data brokers (or may configure a general purpose OOPS to only target data brokers); in that case, a consumer should be empowered to only send opt-out requests to data brokers. An OOPS may also process re-opt-in exceptions on behalf of the user, keeping track of the companies that a user grants an exception to their general preference not to have used for certain processing. In that case, the OOPS may not send an opt-out signal to those companies to which the consumer has granted an exception. To the extent that CalPrivacy wishes to write regulations on this topic, it should consider allowing for selective OOPS implementations, or at least add an illustrative example of the narrow range of behavior this provision is explicitly intended to prevent, lest it prevent pro-consumer implementations.

Nevertheless, we do recognize that there is a hypothetical risk of a future OOPS engaging in self-preferencing (e.g. a browser creating an OOPS that propagates opt-out requests to all websites except its own or that of its business partners). This behavior should be clearly prohibited.

Consumer Friendly OOPS

CalPrivacy is also permitted to issue regulations to "ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer."[22] In addition, the California Opt Me Out Act allows CalPrivacy to adopt regulations as necessary to ensure that required browser OOPS functionality "shall be easy for a reasonable person to locate and configure."

Section 7004 already provides a strong baseline for how browser OOPSs should be operationalized — especially the requirements for symmetry in choice and the prohibitions on confusing consumer choice architecture. Ideally, browser-supported opt-out signals will be supported directly from the toolbar or with a short navigation through clearly labeled menus. CalPrivacy should consider mandating a maximum number of clicks in order to enable OOPS functionality — or at least that OOPS functionality can be enabled from a browser's main settings or privacy menu and is not buried deep in sub-menus.

Defaults

Finally, CalPrivacy is yet to interpret the requirement that OOPSs "clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent."[23]

In our view, user agents specifically marketed as designed to safeguard privacy should be permitted to reasonably infer a consumer's use of that agent as intent to broadcast an OOPS without further user interaction. Mandating additional consumer dialogues after a user has made the choice of a privacy-focused user agent or browser would introduce unnecessary friction and

[22] CCPA Section 1798.185(a)(18)(A)(ii)
[23] CCPA Section 1798.185(a)(18)(A)(iii)

confusion into what is designed to be a simple option for consumers to exercise universal choices.

We'd also recommend that CalPrivacy clarify that the use of preinstalled privacy-focused user agents to send OOPSs should also count as clearly "representing the consumer's intent" (unlike the Colorado Rules, which proscribe this behavior from user agents).[24] Preinstallation of OOPSs should not automatically be disqualifying — especially if the law otherwise forbids unfair self-preferencing. For example, a mobile phone or laptop could preinstall several different browsers from which a consumer selects in order to access the web. A consumer's choice of a privacy-focused one such as DuckDuckGo should be interpreted as an affirmative choice to stop unwanted tracking just as much as the user's separate installation of the same browser would be. Similarly, a user could choose to purchase a privacy-focused device that uses privacy-focused apps as default options (such as ProtonMail and Brave). In that case, the choice of the phone and use of those apps would be sufficient evidence of intent to protect their information.

****

Thank you very much again for the opportunity to provide feedback on this important proceeding — we look forward to continuing to engage with CalPrivacy as it moves forward. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Justin Brookman (justin.brookman@consumer.org) or Matt Schwartz (matt.schwartz@consumer.org) for more information.

[24] Colorado Privacy Act Rules, Rule 5.04(A), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf