Catbagan, Christian@CPPA

From: [redacted]
Sent: Wednesday, April 22, 2026 5:23 AM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear CPPA Team,

I wanted to submit some informal anonymous comments based on what I'm seeing day-to-day working in records and information management within a highly regulated financial services environment.

There is a meaningful disconnect between what companies state in their privacy notices and what is actually happening in practice. On paper, organizations rely on language like "retained as long as necessary," but many do not have fully developed or enforceable retention schedules. Even where schedules exist, they are inconsistently applied across systems. Gaps in retention schedules, combined with the absence of data lineage and de-identification capabilities, make it difficult to operationalize privacy, retention, and disposition requirements in a consistent way.

DSAR processes are often manual, with requests routed to individual business units that review only their source systems. There is limited visibility into downstream systems or analytical environments where the same personal data may reside, creating a risk of incomplete or inaccurate responses.

The use of sectoral exemptions, such as HIPAA and GLBA, can undermine the intent of privacy requirements when applied too broadly. In practice, these carve-outs can create gaps in oversight and allow organizations to rely on regulatory silos rather than implementing consistent, enterprise-wide data governance.

There is awareness of these issues at the executive level, but they are often accepted as a calculated risk, in part because regulatory scrutiny does not always extend to how data is actually managed in practice, companies are rarely forced to prove compliance or defend business justifications of over retention and non-de-identification of PII. This is not a case of "perfect being the enemy of good," but rather a lack of a foundational capability to govern data in a consistent and defensible way.

As a recent example, I've seen internal pushback on data disposition efforts based on the view that there is no explicit regulatory requirement mandating deletion (despite CCPA, NYDFS, and GLBA, SEC,FINRA, CFBP, and FTC implied expectations) and that there is always a "business need" to retain data and the use of AI is amplifying this stance. Similarly, analytics and BI teams may resist de-identification because it impacts the results they are trying to achieve. In some cases, there is an expectation that data should be retained for decades.

The reality is that this is occurring in environments without full visibility into data. Organizations often lack true data lineage capabilities and do not have effective de-identification tools in place. At the same time, retention gaps extend across structured, unstructured, and third-party environments.

Of particular concern is the use of this data in analytical environments. There is a real risk that employee, customer, and consumer data is influencing employment, underwriting, or claims-related decisions without clear governance or alignment to the original purpose of collection.

From my perspective, current notice and disclosure frameworks do not capture this reality. They do not reflect how fragmented data environments are or how much downstream use occurs beyond the original collection point.

Third-party oversight is another area of concern. There is often an assumption that vendors are handling data appropriately, but limited ability to validate retention, access, or deletion practices in practice.

Finally, I strongly encourage the Agency to continue advancing potential whistleblower protections. Individuals in compliance and governance roles are often aware of these gaps, but may face professional risk in raising concerns internally.

Thank you for the opportunity to provide input.

Best

Sent with Proton Mail secure email.

Catbagan, Christian@CPPA

From: Daniel J. Solove <dsolove@law.gwu.edu>
Sent: Saturday, May 16, 2026 1:31 AM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: CPPA Preliminary Comment - Notices and Disclosures and Employee Data - Solove 2026-05-15.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

I write in response to the invitation for preliminary comments on notices and disclosures. I provide my comments below in this email as well as attached as a PDF.

I am the Bernard Professor of Intellectual Property and Technology Law at the George Washington University Law School. I'm co-director of the GW Center for Law & Technology and director of the Privacy, AI, and Technology Law Program. I have written and taught about privacy law for 26 years and have published more than 10 books and 1000 articles on privacy, tech, and AI issues. My most recent book is a short volume called *On Privacy and Technology,* published by Oxford University Press (2025). I served as a reporter for the ALI's Principles of Law, Data Privacy.

I have severe concerns that the general approach of notice-and-choice in privacy law is broken and in need of a significant rethink. I urge the CPPA to think outside of the box and find ways to inject pockets of effective policy into the notice-and-choice framework.

For a long time, the law has used an individual control model to regulate privacy. The idea is to try to inform people about corporate privacy practices, then rely on some form of consent, enabling people to self-manage their privacy. But this approach has been an abysmal failure.

I've pulled some excerpts from recent papers that discuss the problem. In *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U. L. Rev. 1021 (2024), Professor Woodrow Hartzog (Boston University School of Law) wrote:

> Despite writing more than a century ago, Franz Kafka captured the core problem of digital technologies—how individuals are rendered powerless and vulnerable. Over the past fifty years, and especially in the twenty-first century, privacy laws have been sprouting up around the world. These laws are often based heavily on an Individual Control Model that aims to empower individuals with rights to help them control the collection, use, and disclosure of their data.
>
> Although Kafka starkly shows us the plight of the disempowered individual, his work also paradoxically suggests that empowering the individual isn't the answer to protecting privacy, especially in the age of Artificial Intelligence ("AI"). In Kafka's world, characters readily submit authority, even when they aren't forced and even when doing so leads to injury or death. The

> victims are blamed, and they even blame themselves. Although Kafka's view of human nature is exaggerated for darkly comedic effect, it nevertheless captures many truths that privacy law must reckon with. Even if dark patterns and dirty manipulative practices are cleaned up, people will still make bad decisions about privacy. Despite warnings, people will embrace the technologies that hurt them. When given control over their data, people will give it right back. And when people's data is used in unexpected and harmful ways, they will often blame themselves. Kafka's writing provides key insights for regulating privacy in the age of AI.
>
> The law can't empower individuals when it is the system that renders them powerless. Ultimately, privacy law's primary goal should not be to give individuals control over their data. Instead, the law should focus on ensuring a societal structure that brings the collection, use, and disclosure of personal data under control.

In short, tweaking notice to make it slightly more conspicuous or simpler can't cure the fundamental problems at the core of the notice-and-choice approach. Something far more radical is needed.

In *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. Rev. 593 (2024), I wrote:

> The notice-and-choice approach [primarily used in the United States] has been savaged in academic literature. Hardly anyone reads privacy notices, those who try to read them struggle to understand them, the statements in privacy notices are often vague and ambiguous, and the effort to read privacy notices does not scale because there are too many to read. As a result, a remarkably low percentage of people opt out, which allows organizations to use personal data with only the vague self-imposed limits stated in the privacy notices. Even though few can defend the notice-and-choice approach, it has persisted in U.S. privacy law. . . .
>
> I contend that most of the time, privacy consent is fictitious. Privacy law should take a new approach to consent that I call "murky consent." Traditionally, consent has been binary—an on/off switch—but murky consent exists in the shadowy middle ground between full consent and no consent. Murky consent embraces the fact that consent in privacy is largely a set of fictions and is at best highly dubious. Rather than provide extensive legitimacy and power, murky consent should authorize only a very restricted and weak license to use data. Murky consent should be subject to extensive regulatory oversight with an ever-present risk that it could be deemed invalid. Murky consent should rest on shaky ground. Because the law pretends people are consenting, the law's goal should be to ensure that what people are consenting to is good. Doing so promotes the integrity of the fictions of consent. I propose four duties to achieve this end: (1) duty to obtain consent appropriately; (2) duty to avoid thwarting reasonable expectations; (3) duty of loyalty; and (4) duty to avoid unreasonable risk. The law can't make the tale of privacy consent less fictional, but with these duties, the law can ensure the story ends well.

What can be done? The best approaches involve measures that have people's backs. The law shouldn't try to get rid of consent, as it is impractical and undesirable. Instead, the law should prevent gotcha situations where companies use fictitious consent to legitimize whatever uses of personal data they desire.

In *Murky Consent*, I argue that most situations involving privacy consent should be considered "murky" – of dubious legitimacy. Being murky doesn't invalidate consent, but it should mean that consent must

have less power. I suggest several duties that will augment and improve the way consent operates in privacy law:

> Because murky consent lacks much legitimacy, it should not bestow the same degree of power that consent currently grants. Many privacy laws already require limits on the scope and duration of data collection and retention to what is necessary for the purposes of use. Consent is revocable under many laws, such as the GDPR. These components are essential; any law that lacks them is deficient. For example, revocability ensures that there always is a backstop; consent may be quite dubious, even almost nonexistent, but revocability at least guarantees that there is always a way out, that people always have a choice.
>
> Beyond these restrictions on scope and duration, the law must significantly weaken murky consent's power. To do this, the law must impose a series of duties to promote the integrity of privacy consent's fictions. If the law is pretending that people consent, then the pretense should be plausible. Murky consent should be invalid if it is a bad deal for people. If the law is imagining that people are consenting, then the law should require that what they are consenting to is actually good. To put it another way, we can't escape the fact that privacy consent is a fictional story, but we can demand that the story end happily ever after.

For murky consent, the law should impose the following duties:

- *Duty to Obtain Consent Appropriately*. The method for obtaining murky consent must vary proportionately with the risk. Murky consent cannot be obtained fraudulently or unethically.

- *Duty to Avoid Thwarting Reasonable Expectations*. Murky consent shall be invalid whenever it thwarts people's reasonable expectations about how their data will be collected, used, or disclosed.

- *Duty of Loyalty*. The entity seeking murky consent must put the interests of individuals before its own interests.

- *Duty to Avoid Unreasonable Risk*. Murky consent shall be invalid if it involves an unreasonable risk of harm to individuals, their rights, interests, or welfare. Murky consent shall also be invalid if it creates an unreasonable risk of harm to society.

I discuss these duties in detail at the end of the paper. Here are some key excerpts:

> Organizations should have a **Duty to Avoid Thwarting Reasonable Expectations**, not actual expectations, which could be nearly anything. Reasonableness is itself a fiction—it is a standard of care based on an idealized account of common social norms and practices. The gathering and use of personal data must be consistent with these norms. Deviations from reasonable expectations fall outside the scope of murky consent. If organizations want to deviate, they must either find a way to obtain actual consent, which will be quite difficult, or find another basis to collect and use personal data other than consent.
>
> Ensuring that people's reasonable expectations are respected aims to prevent situations where people unwittingly consent to things they wouldn't want if they were truly informed. . . .

> The **Duty of Loyalty** aims to prevent organizations from putting their own interests ahead of the interests of individuals. As I have argued elsewhere, the law should hold that organizations that collect and process personal data about individuals stand in a fiduciary relationship to them. Fiduciary relationships are ones where there is a significant power difference between parties in a relationship, and this power differential justifies imposing special duties on the party with the greater power. The general concept of the fiduciary relationship is that there is a responsibility of the powerful party to look out for the interests of the other party and not capitalize on its position of heightened power. . . .
>
> [Regarding the **Duty to Avoid Unreasonable** Risk, the] law routinely allows certain risk taking and disallows other risk taking. A person can consent to be a firefighter but cannot consent to be put at risk by flammable products. In a supermarket, people consent to buying food that might be unhealthy, but they cannot consent to tainted food. The law must strike a balance between autonomy and protecting people's welfare. When the risks become unreasonable, consent becomes even more dubious and should not be recognized even as murky consent. . . .
>
> Murky consent should also be invalid when it could cause unwarranted societal harm. The law tolerates a widescale freedom in contracting, but it does not allow all transactions, even if consensual. Certain rights are inalienable. Contracts can be void for public policy when they involve certain immoral, troublesome, or dangerous acts—even if desired by individuals. Privacy is not solely an individual interest; it has a social value and is vital to a free and democratic society. This fact does not mean that privacy should be inalienable; but when one person's choices affect others or cause damage to society, there is a societal interest that must be considered.
>
> Contract terms such as requiring individuals to waive rights to litigate in the event of wrongdoing not only hurt individuals but also undermine the rule of law, a larger societal harm. . . .

For further elaboration of these thoughts, I encourage you to review my articles, which are available for free on SSRN.

Sincerely,

Daniel J. Solove
Bernard Professor of Intellectual Property and Technology Law
Faculty Co-Director, GW Center for Law & Technology
Faculty Director, Privacy, AI, & Technology Law Program
George Washington University Law School
www.danielsolove.com

Please subscribe to my free newsletter to keep up with my events, writings, cartoons, videos, and more.

GW | LAW

DANIEL J. SOLOVE
Bernard Professor of Intellectual Property and Technology Law

dsolove@law.gwu.edu
http://danielsolove.com

May 15, 2025

I write in response to the invitation for preliminary comments on notices and disclosures. I have severe concerns that the general approach of notice and disclosures in privacy law is broken and in need of a significant rethink.

For a long time, the law has used an individual control model to regulate privacy. The idea is to try to inform people about corporate privacy practices, then rely on some form of consent, enabling people to self-manage their privacy. But this approach has been an abysmal failure.

I've pulled some excerpts from recent papers that discuss the problem. In *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 Boston University Law Review 1021 (2024), Professor Woodrow Hartzog (Boston University School of Law) wrote:

> Despite writing more than a century ago, Franz Kafka captured the core problem of digital technologies—how individuals are rendered powerless and vulnerable. Over the past fifty years, and especially in the twenty-first century, privacy laws have been sprouting up around the world. These laws are often based heavily on an Individual Control Model that aims to empower individuals with rights to help them control the collection, use, and disclosure of their data.
>
> Although Kafka starkly shows us the plight of the disempowered individual, his work also paradoxically suggests that empowering the individual isn't the answer to protecting privacy, especially in the age of Artificial Intelligence ("AI"). In Kafka's world, characters readily submit authority, even when they aren't forced and even when doing so leads to injury or death. The victims are blamed, and they even blame themselves. Although Kafka's view of human nature is exaggerated for darkly comedic effect, it nevertheless captures many truths that privacy law must reckon with. Even if dark patterns and dirty manipulative practices are cleaned up, people will still make bad decisions about privacy. Despite warnings, people will embrace the technologies that hurt them. When given control over their data, people will give it right back. And when people's data is used in unexpected and harmful ways, they will often blame themselves. Kafka's writing provides key insights for regulating privacy in the age of AI.
>
> The law can't empower individuals when it is the system that renders them powerless. Ultimately, privacy law's primary goal should not be to give individuals control over their data. Instead, the law should focus on ensuring a societal structure that brings the collection, use, and disclosure of personal data under control.

In *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 Boston University Law Review 593 (2024), I wrote:

> The notice-and-choice approach [primarily used in the United States] has been savaged in academic literature. Hardly anyone reads privacy notices, those who try to read them struggle to understand them, the statements in privacy notices are often vague and ambiguous, and the effort to read privacy notices does not scale because there are too many to read. As a result, a remarkably low percentage of people opt out, which allows organizations to use personal data with only the vague self-imposed limits stated in the privacy notices. Even though few can defend the notice-and-choice approach, it has persisted in U.S. privacy law...
>
> I contend that most of the time, privacy consent is fictitious. Privacy law should take a new approach to consent that I call "murky consent." Traditionally, consent has been binary—an on/off switch—but murky consent exists in the shadowy middle ground between full consent and no consent. Murky consent embraces the fact that consent in privacy is largely a set of fictions and is at best highly dubious. Rather than provide extensive legitimacy and power, murky consent should authorize only a very restricted and weak license to use data. Murky consent should be subject to extensive regulatory oversight with an ever-present risk that it could be deemed invalid. Murky consent should rest on shaky ground. Because the law pretends people are consenting, the law's goal should be to ensure that what people are consenting to is good. Doing so promotes the integrity of the fictions of consent. I propose four duties to achieve this end: (1) duty to obtain consent appropriately; (2) duty to avoid thwarting reasonable expectations; (3) duty of loyalty; and (4) duty to avoid unreasonable risk. The law can't make the tale of privacy consent less fictional, but with these duties, the law can ensure the story ends well.

What can be done? The best approaches involve measures that have people's backs. The law shouldn't try to get rid of consent, as it is impractical and undesirable. Instead, the law should prevent gotcha situations where companies use fictitious consent to legitimize whatever uses of personal data they desire.

In *Murky Consent*, I argue that most privacy consent should be considered "murky" – of dubious legitimacy. Being murky doesn't invalidate consent, but it should mean that consent must have less power. I suggest several duties that will augment and improve the way consent operates in privacy law:

> Because murky consent lacks much legitimacy, it should not bestow the same degree of power that consent currently grants. Many privacy laws already require limits on the scope and duration of data collection and retention to what is necessary for the purposes of use. Consent is revocable under many laws, such as the GDPR. These components are essential; any law that lacks them is deficient. For example, revocability ensures that there always is a backstop; consent may be quite dubious, even almost nonexistent, but revocability at least guarantees that there is always a way out, that people always have a choice.

> Beyond these restrictions on scope and duration, the law must significantly weaken murky consent's power. To do this, the law must impose a series of duties to promote the integrity of privacy consent's fictions. If the law is pretending that people consent, then the pretense should be plausible. Murky consent should be invalid if it is a bad deal for people. If the law is imagining that people are consenting, then the law should require that what they are consenting to is actually good. To put it another way, we can't escape the fact that privacy consent is a fictional story, but we can demand that the story end happily ever after.
>
> For murky consent, the law should impose the following duties:
>
> - *Duty to Obtain Consent Appropriately*. The method for obtaining murky consent must vary proportionately with the risk. Murky consent cannot be obtained fraudulently or unethically.
>
> - *Duty to Avoid Thwarting Reasonable Expectations*. Murky consent shall be invalid whenever it thwarts people's reasonable expectations about how their data will be collected, used, or disclosed.
>
> - *Duty of Loyalty*. The entity seeking murky consent must put the interests of individuals before its own interests.
>
> - *Duty to Avoid Unreasonable Risk*. Murky consent shall be invalid if it involves an unreasonable risk of harm to individuals, their rights, interests, or welfare. Murky consent shall also be invalid if it creates an unreasonable risk of harm to society.

I discuss these duties in detail at the end of the paper. Here are some key excerpts:

> Organizations should have a **Duty to Avoid Thwarting Reasonable Expectations**, not actual expectations, which could be nearly anything. Reasonableness is itself a fiction—it is a standard of care based on an idealized account of common social norms and practices. The gathering and use of personal data must be consistent with these norms. Deviations from reasonable expectations fall outside the scope of murky consent. If organizations want to deviate, they must either find a way to obtain actual consent, which will be quite difficult, or find another basis to collect and use personal data other than consent.
>
> Ensuring that people's reasonable expectations are respected aims to prevent situations where people unwittingly consent to things they wouldn't want if they were truly informed. . . .
>
> The **Duty of Loyalty** aims to prevent organizations from putting their own interests ahead of the interests of individuals. As I have argued elsewhere, the law should hold that organizations that collect and process personal data about individuals stand in a fiduciary relationship to them. Fiduciary relationships are ones where there is a significant power difference between parties in a relationship, and this power differential justifies imposing special duties on the party with the greater power. The

> general concept of the fiduciary relationship is that there is a responsibility of the powerful party to look out for the interests of the other party and not capitalize on its position of heightened power. . . .
>
> [Regarding the **Duty to Avoid Unreasonable** Risk, the] law routinely allows certain risk taking and disallows other risk taking. A person can consent to be a firefighter but cannot consent to be put at risk by flammable products. In a supermarket, people consent to buying food that might be unhealthy, but they cannot consent to tainted food. The law must strike a balance between autonomy and protecting people's welfare. When the risks become unreasonable, consent becomes even more dubious and should not be recognized even as murky consent. . . .
>
> Murky consent should also be invalid when it could cause unwarranted societal harm. The law tolerates a widescale freedom in contracting, but it does not allow all transactions, even if consensual. Certain rights are inalienable. Contracts can be void for public policy when they involve certain immoral, troublesome, or dangerous acts—even if desired by individuals. Privacy is not solely an individual interest; it has a social value and is vital to a free and democratic society. This fact does not mean that privacy should be inalienable; but when one person's choices affect others or cause damage to society, there is a societal interest that must be considered.
>
> Contract terms such as requiring individuals to waive rights to litigate in the event of wrongdoing not only hurt individuals but also undermine the rule of law, a larger societal harm. . . .

For further elaboration of these thoughts, I encourage you to review my articles, which are available for free on SSRN.

Sincerely,

Daniel J. Solove

Catbagan, Christian@CPPA

From: Annette Bernhardt [redacted]
Sent: Saturday, May 16, 2026 9:51 AM
To: Regulations@CPPA
Cc: Annette Bernhardt
Subject: Preliminary Comment – Notices & Disclosures and Employee Data April 2026
Attachments: May 2026 CPPA preliminary comment.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Greetings,

Attached please find our submission in response to the request for preliminary comment.

Regards,
Annette Bernhardt

May 16, 2026

California Privacy Protection Agency
Attn: Legal Division – Regulations
400 R St., Suite 350
Sacramento, CA 95811

Dear Executive Director Kemp, Agency Staff, and Board Members,

The signed organizations write to respond to the California Privacy Protection Agency's April 20, 2026 invitation for preliminary comment on Notices & Disclosure and Employee Data as regulated by the California Consumer Privacy Act (CCPA).

We welcome the continued attention by Agency leadership, staff, and board members to the goal of ensuring that workers in California are fully protected by the CCPA in the collection and use of their data.

To that end, we would like to direct the Agency's attention back to the input provided over the last two years by a large working group of labor and civil society groups (including our organizations), which together represent hundreds of thousands of workers and consumers. We invested significant time analyzing draft regulations, gathering evidence from impacted workers, summarizing academic research, writing responses, and giving public comments at board meetings. In 2025, these efforts culminated in two working group letters giving input to the agency's rulemaking on Automated Decisionmaking Systems (ADMTs) and Risk Assessments:

- In our group recommendation letter (January 9, 2025), we laid out a robust, sharply articulated, and fully documented set of worker priorities for the rulemaking process.
- In our group response letter (June 2, 2025), we document and express our profound disappointment that none of our worker priorities were adopted in the final regulations.

While these letters were developed during the previous rulemaking process, all of their major recommendations respond to either question #7 for Notices & Disclosure or question #7 for Employee Data. More generally, the working group's substantive priorities remain the same as articulated last year, including broadening the definition of ADMT so that it works for workers; requiring post-use notification when ADMTs have been used to make a decision about workers; and establishing the right for workers to challenge those decisions.

We therefore respectfully request that the Agency review the two letters referenced above as part of its deliberations on whether or not to commence a new rule-making process.

Sincerely,

California Federation of Labor Unions
California Nurses Association
SEIU California
Tech Equity
UC Berkeley Labor Center

Catbagan, Christian@CPPA

From: Merry Marwig <merry@privacy4cars.com>
Sent: Monday, May 18, 2026 12:24 PM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: 2026-05-18 Privacy4Cars Comments to CalPrivacy - Notices and Disclosures and Employee Data.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear members of the California Privacy Protection Agency,

The team at Privacy4Cars respectfully submits in the ***attached*** PDF our comments regarding the proposed rulemaking on Preliminary Comment - Notices & Disclosures and Employee Data April 2026.

Please confirm receipt of this email.

Kindly,
Merry
--

Merry Marwig
Vice President, Global Communications & Advocacy

Privacy4Cars
https://privacy4cars.com
info@privacy4cars.com

May 18, 2026

California Privacy Protection Agency
https://CalPrivacy.ca.gov
regulations@CalPrivacy.ca.gov

Subject: Privacy4Cars' Preliminary Comment -Notices & Disclosures & Employee Data April 2026

Dear members of CalPrivacy,

Privacy4Cars respectfully submits these comments on notice & disclosures and employee data, based on our extensive experience in the automotive privacy and data security sector.

Cars are among the most expensive and longest-lived connected devices a consumer will likely ever own. The average vehicle on the road is 13 years old, dwarfing the 2–5 year lifespan of a typical smart home gadget. Unlike a fitness tracker or a smart speaker, a vehicle is difficult and costly to walk away from if a consumer later discovers its data practices conflict with their privacy expectations. **That makes it essential for the businesses Californians rely on when transacting on vehicles, from dealerships, lenders, insurers, company fleets, and more, to provide clear, vehicle-specific privacy information at three critical moments: before a transaction, after a transaction, and when a consumer relinquishes control of a vehicle:**

1. **Before transaction:** Require dealerships, lenders, insurers, fleets, and other auto businesses to provide clear, vehicle-specific privacy disclosures to consumers before any vehicle transaction begins, ensuring they know what data is being collected and how it is being used.

2. **After transaction:** Require these same businesses to proactively present consumers with clear, vehicle-specific privacy choices, including the right to opt out of data selling/sharing, once a transaction has concluded.

3. **When a consumer gives up a vehicle:** Require these same businesses to proactively offer consumers clear, vehicle-specific options to delete their personal data from the vehicle whenever they relinquish control of it (e.g., trade-in, lease return, total loss), to prevent what would otherwise constitute unauthorized data sharing or a breach of the personal data retained on the vehicle's systems.

California's recent settlement with GM and its emphasis on data minimization further supports this recommendation. When a consumer relinquishes a vehicle, personal data persists both in the vehicle itself and on the servers of manufacturers and third parties, including data brokers. Consumers should be proactively notified of this fact and reminded of their rights under the law to have that data deleted from all locations where that data resides.

Meeting CA Consumers Where They Are — Reducing Privacy Friction at Points of Transaction

Vehicles are among the most data-intensive consumer products on the market, and we commend CalPrivacy for recognizing the sector needs much more scrutiny. The current sweep has already identified cases in which lack of prominent disclosures, excessive complexity in explaining choices, and non-compliant friction and deceptive design ("dark patterns") caused consumers and their appointed agents to be unable to take privacy-preserving actions in the manners intended by the law. CalPrivacy has so far focused its actions towards manufacturers of vehicles, reaching already three separate settlements: two (American Honda Motor Co., Ford Motor Company) regarding the online interfaces they offer consumers to make choices and most recently one with General Motors (GM), which required improved processes to inform consumers, data minimization remedies, and fines of $12.75 million.

Knowing Is a Different, Much Higher Standard Than Simply Disclosing

In the Attorney General Office's press release on the May 2026 GM settlement,[1] San Francisco District Attorney Brooke Jenkins stated that, "Californians must have confidence that they know what data is being collected, how it is being used, and what their opt-out rights are." ***Knowing* is a different, much higher standard than simply *disclosing*,** which is why we urge regulatory clarification and enforcement requiring the businesses Californians rely on when transacting on vehicles, from dealerships, lenders, insurers, company fleets, and more, to provide clear, vehicle-specific privacy information at three critical moments: before a transaction, after a transaction, and when a consumer relinquishes control of a vehicle.

[1] https://oag.ca.gov/news/press-releases/when-it-comes-data-privacy-consumers-must-be-driver%E2%80%99s-seat-attorney-general

> "Modern cars are rolling data collection machines," **said San Francisco District Attorney Brooke Jenkins.** "Californians must have confidence that they know what data is being collected, how it is being used, and what their opt-out rights are. Those duties fall on the automobile companies. This case sends a strong message that law enforcement will take action when California privacy laws are not scrupulously followed. I want to extend my appreciation to both the Attorney General's Privacy Unit and to CalPrivacy for their work in this field, and my fellow District Attorneys for taking action to enforce and protect California's privacy laws."

This distinction between *knowing* and *disclosing* matters because there is an inherent tension between exhaustive technical detail (what current privacy policies are doing, resulting in hour-long reading of complex legal documents most consumers don't have the reading level proficiency to understand) and genuine consumer understanding. For the first time, a judgement signaled that the current standard of complex and lengthy privacy policies and terms of service written, requiring "easy to read and understandable to consumers, such as by using plain, straightforward language and avoiding technical or legal jargon, and otherwise be truthful, accurate, and not misleading."[2] The GM settlement's framing prioritizes a consumer's actual ability to understand what is happening with their data over the legal breadth of a disclosure document. This reinforces our position that disclosures must be clear, concise, and vehicle-specific rather than buried in pages of legalese that few consumers read and fewer still comprehend.

> 21 23. GM shall provide CALIFORNIA ONSTAR CUSTOMERS with clear and
> 22 conspicuous privacy notices as part of the enrollment process for OnStar or OnStar features
> 23 regarding GM's collection and, use of any COVERED DRIVING DATA, and disclosure of any
> 24 COVERED ONSTAR DATA to THIRD PARTIES. Such privacy notices shall be easy to read and
> 25 understandable to consumers, such as by using plain, straightforward language and avoiding
> 26 technical or legal jargon, and otherwise be truthful, accurate, and not misleading.

As we pointed out in a recent article published by the International Association of Privacy Professionals on May 11th, 2026,[3] it is important to recognize that Californians who are interested in procuring transportation via an automobile do not do so by interacting with the manufacturers directly (with uncommon exceptions). Instead, Californians make vehicle purchase choices in B2C retailer settings: at dealerships (including both franchised affiliates of the manufacturers and independent retailers), through lenders (e.g. from pre-approval to

---

2 https://oag.ca.gov/system/files/attachments/press-docs/Received%20Stamped%20Proposed%20Final%20Judgment.pdf

3 https://iapp.org/news/a/california-authorities-announce-largest-ccpa-fine-to-date?mkt_tok=MTM4LUVaTS0wNDIAAAGhtvUDm6ChEKdGPVkvjJqpKj_QwihFqtCKOYbD8gj_wZNZPt6hliOFruRgDKoeBpH-6VZGz6ifA3mPZmqXG-TSZSx04NXCOMzzrxQ6teFr3a0z

financing), with insurers (which is mandatory under the law), or, for employees (who are also covered under California law as privacy rights-holders) via their corporate fleets (including both corporate and rental/sharing). Californian regulators already recognized this reality when they chose to amend Cal. Code Regs. Tit. 11, § 7012 (g) (Notice at Collection of Personal Information) mentioning the obligations of businesses and third parties notice requirements, specifically in retail stores or in a vehicle, which recites:

> *(g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing.*
>
> > *(1) For purposes of giving Notice at Collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a Notice at Collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a Notice at Collection. The first party and third parties may provide a single Notice at Collection that includes the required information about their collective information practices.*
> >
> > *(2) A business that, acting as a third party, controls the collection of personal information on another business's physical premises, such as in a retail store or in a vehicle, shall provide a Notice at Collection in a conspicuous manner at the physical location(s) where it is collecting the personal information.*

The law also has a specific illustrative example for car rental companies:

> *(C) Business J, a car rental business, allows Business K to collect personal information from consumers within the vehicles Business J rents to consumers. Business J may give its Notice at Collection to the consumer at the point of sale (i.e., at the rental counter) either in writing or orally. Business K may provide its own Notice at Collection within the vehicle, such as through signage on the vehicle's dashboard directing consumers to where the notice can be found online.*

Since the law, as amended, points out the role of retail and the importance of automobiles, it should therefore follow that, if CalPrivacy's goal is to ensure the entire population of consumers whose data is (or is about to be) collected, used, shared, or sold through an automobile is presented with prominent disclosures, clear choices, and to make it as easy for Californians to share their data as it is to opt-out and have it deleted, CalPrivacy should consider taking the following three actions:

1. **Issue guidance clarifying that under existing regulations dealerships, lenders, insurers, and fleets have to proactively show easy-to-understand, vehicle-specific privacy disclosures** before data collection starts, i.e. before a vehicle transaction is entered - as now required by the amended Cal. Code Regs. Tit. 11, § 7012 (Notice at Collection of Personal Information). Guidance should be at minimum in the form of a letter, from CalPrivacy or the Office of the Attorney General (and possibly by the Insurance Commissioner for auto insurers), addressed to the main national and Californian chapters of the relevant industry associations. We have to point out that disclosures made by vehicle manufacturers (e.g. their privacy policies and terms) are excessively long, require a mastery of legal language that most Californians do not possess, and most importantly because this is not how Californians gain information about vehicles they are about to transact on: most consumers rely on those aforementioned B2C companies to gain information about a vehicle and/or make automotive mobility purchasing decisions in California - hence asking consumers to go check the website of a manufacturer adds excessive friction and does not reduce the risk that the consumer is either misinformed during the sale process or is too late for them to make a different choice if they already purchased the vehicle.

2. **Issue guidance clarifying that under existing regulations dealerships, lenders, insurers, and fleets, once a transaction has concluded (e.g. after purchasing, leasing, financing, or insuring a vehicle) have to proactively show easy-to-understand, vehicle-specific ways for consumers to make privacy choices for the vehicle** including the right to opt-out of the selling/sharing of their data. Similar considerations to recommendation (1) apply.

3. **Issues guidance clarifying that under existing regulations, whenever** a consumer enters a transaction in which they stop controlling a vehicle that contains their personal data (e.g. a total loss collision, a trade-in, the return of a lease or a rental) the business they are transacting with (e.g. **dealerships, lenders, insurers, and fleets) have to proactively show easy-to-understand, vehicle-specific ways for consumers to make privacy choices for the vehicle** including the right to delete any data collected by the vehicle in line with NIST 800-88 Rev. 2 "reasonable security" standards. Not doing so prior to the business re-selling or re-renting the vehicle would result in an unauthorized sharing/selling of personal data and a data breach.

Additional Comments on Notice & Disclosures

We have previously submitted comments to CalPrivacy on April 2nd, 2026 via email that cover additional areas of concern regarding notice and disclosures, which include:

- 87% of car buyers say data privacy and security influences their purchase, yet lack the accurate information to act on it.
- Disclosure responsibility should extend beyond manufacturers to dealerships, lenders, insurers, and rental companies, whoever holds the consumer relationship at the point of transaction.
- Require written, VIN-specific disclosures before vehicle purchase.
- In-vehicle screens are impractical for disclosures (excessive scrolling, seen only post-purchase), and finance companies rarely disclose vehicle data-sharing practices.
- "Vehicle" should be added as an example device in CCPA opt-out and sensitive-data regulations (§§ 7013–7014).

Please reference our previously submitted comments emailed on 02 April 2026 for further information on these topics.

Employee Data

Three to five million vehicles are being used in an employment context on California roads at any given time out of the 36.2 million total registered. Similar to the retail examples explained above, before assigning a connected fleet vehicle to an employee, California employers should provide a plain-language, VIN-specific privacy disclosure (Notice at Collection (Cal. Code Regs. Tit. 11, § 7012) under CCPA that clearly states what personal data the vehicle collects (such as geolocation, driving behavior, and biometrics), whether the vehicle transmits data via telematics, and which third parties receive that data, including the manufacturer, fleet management providers, insurers, and data brokers.

When the employee returns, surrenders, or is separated from the vehicle, the employer should ensure that all personal data stored on the vehicle such as contacts, call logs, navigation history, saved credentials, paired devices, and similar, is deleted and all personal accounts are disconnected before the vehicle is reassigned, returned to the lessor, sold, or otherwise disposed of, with the departing employee receiving written confirmation that this has been completed.

Conclusion

We recommend regulations be updated to explicitly address the complexities of personal data in the vehicle context, including the broader ecosystem of businesses that collect, process, and profit from this information.

We urge CalPrivacy to act on the recommendations outlined at the start of this letter. Vehicles are among the most expensive, data-intensive consumer products on the market, yet the current regulatory framework does not adequately address the points of transaction where consumers most need transparency and choice. By adopting clearer disclosure requirements at the varying stages of transaction, along with clear personal data deletion obligations, CalPrivacy can ensure that privacy protections remain effective as vehicles evolve into increasingly sophisticated data platforms. As California's law extends to employees, the same should go for vehicles used in an employment context.

These changes will provide much-needed clarity for businesses while ensuring consumers maintain meaningful control over their personal information across the full lifecycle of vehicle use, ownership, financing, insurance, and resale. We welcome the opportunity to discuss these recommendations further.

Respectfully,
The Team at Privacy4Cars
https://privacy4cars.com
info@privacy4cars.com

Catbagan, Christian@CPPA

From: Ridhi Shetty <rshetty@cdt.org>
Sent: Monday, May 18, 2026 1:47 PM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: CDT comment to CalPrivacy on employee data.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

The Center for Democracy & Technology respectfully submits the attached comments in response to the California Privacy Protection Agency's request for preliminary input regarding the necessity of regulatory changes related to notices and disclosures concerning employee data pursuant to the California Consumer Privacy Act.

Best,
Ridhi Shetty

Ridhi Shetty | Senior Policy Counsel, Privacy & Data Project
Center for Democracy & Technology | cdt.org
E: rshetty@cdt.org | P: 202-407-8830 | [she/her/hers]

CDT is celebrating its 30th Anniversary! Please join the fun by staying updated on our work, connecting with us, or making a contribution.

CENTER FOR DEMOCRACY & TECHNOLOGY

May 18, 2026

To: California Privacy Protection Agency
Attn: Legal Division — Regulations
400 R Street, Suite 350
Sacramento, CA 95811

Re: Invitation for preliminary comments regarding regulations related to notice and disclosures and employee data

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the California Privacy Protection Agency's (CalPrivacy) request for preliminary input regarding the necessity of regulatory changes related to notices and disclosures concerning employee data pursuant to the California Consumer Privacy Act (CCPA). CDT is a nonpartisan, nonprofit 501(c)(3) organization that works to advance civil rights and civil liberties in the digital age.

As CalPrivacy evaluates the CCPA's requirements for notice, disclosure, and the exercise of CCPA rights with respect to job applicants and workers in the employment lifecycle, CalPrivacy should consider two overarching issues:

- Ensuring that businesses' privacy policies and notices of CCPA rights clearly distinguish how they treat workers' personal information from how they treat other consumers' personal information, and
- Not allowing exceptions in the CCPA to undermine workers' ability to exercise their CCPA rights.

I. Businesses' privacy policies and notices should specify how employment-related information is treated.

Under Sec. 7001(o) of the CCPA regulations, "employment-related information" is personal information that a business collects about a person in the course of the person acting as a job applicant or employee of the business when the collection and use is solely within the context of the person's job application or employment.[1] This provision states that the collection of employment-related information is a business purpose. However, "employment-related

[1] The definition refers to Cal. Civ. Code §1798.145(m)(1)(a).

information" could include any of the categories of personal information enumerated in the statute as they pertain to workers, and businesses may use the employment-related information they collect in a variety of ways within the employment context.

Sec. 7011(e)(1) of the regulations require privacy policies to identify categories of personal information collected, categories of personal information disclosed, and the business purposes for collecting and disclosing personal information. Privacy policies that satisfy these requirements can give workers an idea of the breadth of a business's overall data collection and use, but do not necessarily clarify which of the listed categories of data are used and disclosed for each listed business purpose. Further, because collection of employment-related information is itself a business purpose, businesses could simply let workers know that employment-related information is collected generally without elaboration.

The regulations should require businesses to specify in their privacy policy the types of employment-related information that are collected. Businesses should also be required to differentiate the purposes for which each type of employment-related information is used and disclosed from how non-employment consumers' personal data is treated.

In addition, the definition of "automated decision-making technology" (ADMT) was narrowed to apply only when the technology is used to replace or substantially replace human decision-making, so that employers can avoid complying with the ADMT regulations by having personnel who *can* override decisions that rely on these outputs even if they do not exercise that discretion. To avoid this easily-exploitable loophole to compliance, the regulations should expand the definition of ADMTs to include technologies that assist in employment decisions.[2]

Sec. 7011(e)(1) of the regulations also requires privacy policies to identify categories of third parties to whom personal information is sold or shared, but not to whom it is otherwise disclosed. "Sharing" is limited to the disclosure of personal information for cross-contextual advertising, but workers' data may be disclosed for other purposes other than advertising, such

[2] Center for Democracy & Technology, Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations – Modifications to Text of Proposed Regulations (June 2, 2025), https://cdt.org/wp-content/uploads/2025/06/CDT-Public-Comment-on-Modifications-to-Proposed-CCPA-Regulations-on-ADMTs.pdf; Center for Democracy & Technology, Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations (Feb. 19, 2025), https://cdt.org/wp-content/uploads/2025/02/CDT-Public-Comment-on-CCPA-Updates-Cyber-Risk-ADMT-and-Insurance-Regulations.pdf.

as to third parties providing employment or income verification services to other parties.[3] Under Sec. 7011(e)(2)(A), workers can, upon request, exercise the right to know the categories of third parties to whom personal information is disclosed, whereas the statute requires privacy policies to list these categories.[4] Sec. 7011(e)(1) should therefore include a provision requiring privacy policies to identify the types of service providers and other third parties to whom employers provide employment-related information for other purposes without receiving compensation in exchange.

II. Businesses should not use the employment relationship to undermine job applicants' and workers' privacy or ability to exercise CCPA rights.

"Employment-related information" covers personal information collected in the course of a person acting as an employee or independent contractor to the extent it is used solely within the context of their role with the business. The regulations should clarify that this does not give employers free reign to collect any personal information from employees or independent contractors so long as these workers have been notified of such collection, or to collect personal information of employees or independent contractors outside of those workers' working hours through devices or apps that employers have their workers use.[5]

Businesses are required to provide a right to limit the use or disclosure of sensitive personal information for any business purposes other than those enumerated under Sec. 7027(m) of the regulations, and to provide a notice to consumers of this right. The exceptions provided under Sec. 7027(m) would mean businesses would not need to provide workers with a right to limit the use or disclosure of any sensitive employment-related information for the following purposes:

- To perform services or provide goods reasonably expected by an average consumer who requests them,
- To resist malicious or illegal actions directed at the business or consumers,
- To ensure people's physical safety,

[3] Chris Chmura, *A Data Broker Has Millions of Workers' Paystubs: See If They Have Yours* (Feb. 9, 2022), https://www.nbcbayarea.com/investigations/consumer/data-brokers-have-millions-of-workers-paystubs-see-if-they-have-yours/2806271/.
[4] Cal. Civ. Code §1798.130(a)(5)(B).
[5] Incogni Research, *Workplace Apps Are Watching, Keeping Tabs, and Sharing What They Learn* (2026), https://blog.incogni.com/workplace-apps-on-personal-devices-research/.

- To perform services on behalf of the business, or
- To verify or maintain the quality or safety of, improve, or enhance the business's services.

The statute also states that a business does not have to comply with a request to delete personal information if it is reasonably necessary for the business to retain the information to perform a contract between the business and consumer.

These exceptions may put workers in a difficult position. For example, employees of SoFi Stadium and Legends Global are reportedly being required to provide sensitive personal information to FIFA so that they can work at the 2026 World Cup.[6] Per a complaint filed by their union, employees are being notified by FIFA that it is collecting their Social Security numbers, current residential addresses, nationality, and country of birth, all of which would be the type of information subject to the CCPA's right to limit. However, FIFA itself is likely not a "business" within the CCPA's definitions because it is a nonprofit, and the employers that are businesses are not providing the employees with the means to limit the collection and use. The employees were notified that their data will be shared with government authorities or a third party for purposes of conducting a security background check, which arguably would be within the scope of the business purposes enumerated under Sec. 7027(m) of the regulations, but can also lead to government abuse of this data.

If employees cannot limit the use and disclosure of their sensitive information or have their information deleted, they would have to choose between protecting their privacy and being able to work. To prevent FIFA's use and disclosure from extending beyond these enumerated purposes, the regulations should require the employers to conduct a risk assessment for this data collection. The regulations should provide that employers need to contractually require the party to which sensitive data is disclosed (e.g., FIFA) to cooperate in conducting the risk assessment, identify the limited and specified business purpose to which that party's use and disclosure must be restricted, and require that party's cooperation in complying with workers' requests to exercise CCPA rights.

III. Conclusion

[6] Adam Crafton, *SoFi Stadium Workers' Union Complains About FIFA to California Attorney General*, NY Times (May 8, 2026), https://www.nytimes.com/athletic/7261918/2026/05/08/sofi-union-workers-union-complaint-fifa/.

The CCPA now applies to employee data, but the regulations should ensure that workers realize the benefits of this change. CalPrivacy has an opportunity to fill gaps in the regulations by initiating a rulemaking process that better protects workers' privacy. We look forward to collaborating with the agency in these efforts.

Catbagan, Christian@CPPA

From: Robert Mather <robert.m@myemployment.com>
Sent: Tuesday, May 19, 2026 11:31 AM
To: Regulations@CPPA
Subject: Preliminary Comment – Notices & Disclosures and Employee Data April 2026
Attachments: CCPA_Preliminary_Comment_Notices_Employee_Data_May2026_v4 (1).pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear CalPrivacy Legal Division,

Please find attached my preliminary comment in response to the April 2026 Invitation for Preliminary Comments on Notices & Disclosures and Employee Data.

The comment addresses Cal. Code Regs. tit. 11 §§ 7012 and 7050-7053, and Civ. Code § 1798.100(c), as applied to employee, applicant, and independent contractor data. It engages with Notices & Disclosures Questions 1, 3, 4, and 7, and Employee Data Questions 1, 3, 5, 6, and 7.

I would welcome the opportunity to provide additional information or participate in any workshops or working sessions the Agency may convene.

Respectfully,

Robert Mather Founder, MyEmployment robert.m@myemployment.com (702) 508-6474

California Privacy Protection Agency
Attn: Legal Division – Regulations
400 R Street, Suite 350
Sacramento, CA 95811
regulations@cppa.ca.gov

May 19, 2026

Re: Preliminary Comment – Notices & Disclosures and Employee Data April 2026

To the California Privacy Protection Agency:

I am writing in my capacity as Founder of MyEmployment, an FCRA-aligned employment verification platform. With thirty years in the consumer reporting industry, including founding and exiting one of the largest independent consumer reporting agencies in the United States, I submit this comment as someone who has been in this industry since these data commercialization practices first emerged. During this period I processed over 10 million employment verification requests for downstream verifiers with permissible purposes under Federal and California consumer reporting laws. This comment addresses Cal. Code Regs. tit. 11 §§ 7012 (Notice at Collection) and 7050-7053 (service providers and contractors), and the purpose-limitation requirement at Civ. Code § 1798.100(c), as they apply to employee, applicant, and independent contractor data, and engages with the following Invitation questions: Notices & Disclosures Questions 1, 3, 4, and 7, and Employee Data Questions 1, 3, 5, 6, and 7. I write not as a regulatory drafter, but to bring to the Agency's attention a real-world problem I believe CalPrivacy should address in any forthcoming amendments.

In the 1990s, when I began in this industry, the employer was the protector of its employees' personal data. When a verifier needed to confirm employment or income, the request went to the employer directly, with a signed release form authorizing the disclosure, and the employer made the disclosure for the specific transaction at hand. The information stayed within that transaction. I watched the industry move away from that model. Responsibility for protecting employee data has been progressively outsourced, first to payroll processors and HRIS providers, and from them to third-party aggregators that store and resell the data downstream for commercial use. The employer, who once held both the data and the duty, today often holds neither.

A core principle I believe in, and would ask the Agency to keep in mind throughout this comment, is this: when an employee accepts employment from an employer, the employment relationship should not, by itself, authorize the employer, knowingly or unknowingly, to transmit that employee's data to a third-party data aggregator for storage and downstream commercial use, in many cases in perpetuity, and without giving the employee any ability to deny the release of their data at the time of any specific request. Yet under the current framework, that is precisely what frequently happens.

What has prompted me to write is what I have observed in the employment verification market. Employees frequently react with real anger upon discovering that their employer has allowed their personal payroll data to be transmitted to a third-party data aggregator. Sometimes the employer knew the data flow was occurring. More often, the employer did not. I have personally spoken with business leaders who flatly did not believe their employees' data was being shared with a third-party data

aggregator, until I walked them through the language in the payroll services agreement they had signed. The current disclosure framework produces these conversations as a matter of course. That is the problem the Agency needs to examine.

Here is the opportunity to correct what is, in my opinion, a major blind spot in the current employment verification ecosystem for both employees and employers. The CCPA's service-provider rules (Cal. Code Regs. tit. 11 §§ 7050-7053) assume that a service provider works solely for the business that hired it, with the business directing its activities and the contract limiting the provider's use of data. That model works for ordinary vendor relationships. Take a CPA preparing tax filings, a health insurance broker managing benefits, or an outside firm maintaining IT systems. In each of these the service provider works for the business that hired it, and the data the provider handles does not generate a separate revenue stream from a third party. In these cases it is safe to assume that the employee has no fear of their personal information being stored and resold for downstream commercial use. In fact, most employees would be upset to learn that every vendor their employer chose to contract with was monetizing their data. It breaks down when the “service provider” is also being paid, on an ongoing basis, by a third party that wants to commercialize the employee's data. The existing Notice at Collection rules (§ 7012) do not require anyone in the chain to tell the employee that this is happening.

The issues and examples I describe below draw on multiple public sources, including Equifax's annual reports and SEC filings, and the federal antitrust case *Greystone Mortgage, Inc. v. Equifax Workforce Solutions LLC*, now pending in the Eastern District of Pennsylvania. What I describe does not depend on the outcome of that litigation. The court could rule for Equifax on every contested legal question, and the underlying facts would remain accurate because they rest on Equifax's own admissions on the federal court record, which stand regardless of how the antitrust theory is ultimately resolved.

The dominant architecture and its principal participant

The architecture I describe is not unique to any one employment verification platform. The major player in this industry is Equifax and its division The Work Number, which I use throughout this comment as the working illustration. The recommendations at the end of this comment are not addressed to one company; they are directed at the structural framework in which any party operating this architecture would currently sit.

Industry estimates place The Work Number's share of the automated employment and income verification market at over 80%, making it the dominant pathway through which a verifier (lender, landlord, prospective employer, or other party with a permissible purpose) confirms an applicant's income or employment, rather than contacting the employer directly. Equifax states publicly that nearly 5 million employers contribute data to The Work Number directly or through payroll providers. In its 2025 annual reporting, Equifax disclosed that the database held 813 million total employee records at year-end 2025, of which 209 million were categorized as “active records,” meaning more than 600 million records held are non-active by the company's own classification. By any reasonable measure these are not marginal numbers; the data flow I am describing touches a substantial share of the working population, including a majority of Californians.

The data reaches employment verification platforms primarily in two ways. Some large employers contract directly with the verification platform; Walmart and Home Depot are documented as direct data providers in the *Greystone v. Equifax* complaint. Most others do not. Their employee data arrives

through the payroll processor or HRIS provider the employer uses, and multiple major payroll and HRIS providers are publicly identified as integration partners with the dominant aggregator. When an employer signs the standard contract with one of these processors, it typically authorizes transmission of payroll data to the verification platform. The employee, who has never seen that contract, has no way of knowing this is occurring.

The data being aggregated is comprehensive. A standard employment verification report from a third-party verification company can include employer name and address, job title and employment status, hire and termination dates, base pay and pay frequency, year-to-date and historical earnings (in some reports spanning up to thirty-six months of pay history), bonuses and commissions, Social Security Number, and historical employment records across an employee's prior employers where data exists in the database. The aggregated record is frequently built and maintained whether or not the employee ever generates a verification request.

The financial structure of the arrangement

In many cases, payroll processors are paid for participating. In its sworn answer to the complaint in *Greystone Mortgage, Inc. v. Equifax Workforce Solutions LLC*, No. 24-2260 (E.D. Pa.), Equifax stated the following in March 2025:

> *Equifax admits that it competes for relationships with data providers, including by paying some data providers a "revenue share" for each transaction matching their data to a verification request.*

(Dkt. 58 ¶ 7.) The court has denied Equifax's motion to dismiss the antitrust case. *Greystone Mortgage, Inc. v. Equifax Workforce Solutions LLC*, 2025 WL 5400112 (E.D. Pa. Feb. 18, 2025). In footnote 2 of that memorandum, the court observed that "data contributors would get reduced revenue shares" if Equifax lowered its prices to verifiers, confirming that the revenue-share arrangement is operationally tied to downstream commercial activity.

In operational terms, the payroll processor an employer hires to handle payroll has an ongoing financial stake in how often the employee's data is queried by third parties. The more the data is used downstream, the more the processor is paid. This is not the agency relationship the CCPA service-provider rules contemplate. It is a supplier relationship in which the employee's data is the supplied good.

The employer occupies a structurally different position in this arrangement. The employer signed the payroll services agreement to handle a routine business function and typically has no direct financial stake in the downstream commercialization of its employees' data. The employer is, in effect, the contracting party who unwittingly authorizes the downstream data flow without receiving any benefit from it and, in many cases, without being told in operationally useful terms what is being authorized. Both the employer and the employee end up bound to an arrangement whose economic logic belongs to parties neither of them has chosen to deal with.

Why the existing rules do not address this

The service-provider framework (§§ 7050-7053) requires the contract between the business and the service provider to prohibit use of personal information for any purpose other than the services performed for the business. It assumes the provider's incentives are aligned with the business's. It does not account for a parallel financial relationship with a third party that compensates the provider per downstream query of the data.

The Notice at Collection requirements (§ 7012) are similarly silent. They do not require the business to identify by name any downstream data broker to which the service provider transmits data. They do not require disclosure of any revenue-share or similar payment. They do not require disclosure that the consumer's data is being aggregated into a separate commercial product sold to other businesses. They do not require disclosure that the consumer's data will be retained by the downstream aggregator indefinitely, including long after the consumer's employment with the contributing employer has ended. They do not require notification to the consumer at the moment the consumer's data is released by the downstream aggregator to a third-party verifier, nor any opportunity for the consumer to approve or deny that specific release.

The result is exactly the situation described at the outset: employees receive a Notice at Collection that is technically accurate yet almost entirely uninformative about what is actually happening to their data. Employers often lack the information needed to disclose more, because their own service-provider agreements do not explain the downstream product or the consideration flowing back to the processor. The current rules place the disclosure obligation on the business but do not require the service provider to supply the business with the information it needs to comply.

The §§ 7050-7053 framework also depends on businesses overseeing their service providers' compliance, including through audits where appropriate. Employee Data Question 6 in the Invitation asks specifically about this oversight function, including whether and how businesses conduct audits or testing to assess service-provider compliance. The active/total record split disclosed at the outset of this comment (209 million active records out of 813 million total) is, among other things, evidence that the oversight is not reaching the downstream retention practices of the aggregator. Bulk retention of non-active records has persisted at scale, untouched by whatever audit or oversight is happening between contributing employers and the aggregator receiving their data.

A documented illustration that the consent mechanism is broken

The consent problem is not theoretical. In February 2026 the same federal court documented an instance of the precise consent-mechanism failure the CCPA's notice rules are meant to prevent. Approximately two months after the antitrust lawsuit was filed, Equifax inserted a new arbitration clause into its Online Universal Membership Agreement, the click-through contract presented to verifiers, without disclosing the pending lawsuit about the very product they were using. The court refused to enforce the clause, finding the post-complaint notice mechanism misleading and requiring curative notice. *Greystone v. Equifax*, Dkt. 138-139 (E.D. Pa. Feb. 17, 2026).

While the arbitration ruling is not itself a CCPA matter, it illustrates on the federal record the pattern of opaque consent the CCPA is designed to prevent. If sophisticated commercial parties experience the agreement this way, ordinary employees whose data moves through the same system have even less

protection.

Responses to the Invitation's Questions

I am not a regulatory drafter, and I leave the specific language to the Agency. The following responds to the specific Invitation questions, with recommended changes that seem to me worth the Agency's consideration.

I. Notices and Disclosures

Question 1. *"When reviewing a privacy policy or similar disclosure, what is the most important information to consumers? What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?"*

The current Notice at Collection rules do not surface, at the consumer level, the information that is most material to an employee whose payroll data is being aggregated by a third party. Two specific items rise to the top.

The Notice at Collection should identify the third-party data aggregator by name. Generic references to "service providers" and "third parties" do not tell the employee what is actually happening to their data. If an employer's payroll processor feeds an employment verification platform that aggregates and resells the data downstream, the Notice should identify that platform by name.

The Notice should disclose the existence of any revenue-share or similar payment arrangement between the service provider and the third party. Consumers cannot evaluate whether a service provider is acting in their interest without knowing whether the service provider has a financial stake in downstream use of their data. The disclosure does not need to include dollar amounts; it needs to disclose that the arrangement exists and what kind of arrangement it is.

See also the data-minimization principle under Employee Data Question 1 below, which addresses what consumers should be told about retention duration.

Question 3. *"What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this issue?"*

In my experience, the most significant challenge is information asymmetry. The business is required to disclose its information practices to consumers, but is not itself told what its service provider is doing with the data downstream. The recommendation that follows addresses this directly.

The service-provider contract requirements in § 7051 should reach the third-party payment side of the relationship. Without a flow-through obligation that requires the service provider to tell the business about any third-party payment arrangement tied to the business's data, even a business that wants to comply with the disclosure recommendations above will not have what it needs to do so. The service-provider contract is the natural place for such an obligation, because § 7051 already specifies what the contract must contain.

Question 4. *"What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights?"*

Real-time notification at the moment of data release is, in my view, the single most effective notice mechanism the Agency could require. The technology to deliver it is mature and in routine commercial use.

Consumers should receive real-time notification of each release of their employment and income data from a third-party aggregator, with the ability to approve or deny that specific release before it is provided to the downstream requester. Under the current system, when a verifier queries an employment verification platform, the aggregator releases the consumer's data without notifying the consumer that a release is occurring and without giving the consumer any opportunity to consent to that specific release. The consumer learns of the release, if at all, only by discovering later that a particular party obtained their information. The technology to implement real-time consumer notification and approval is mature; consumers routinely encounter multi-factor authentication and transaction-confirmation prompts for far less consequential financial activity. CalPrivacy should consider whether a notification-and-approval mechanism, at the point of release from the third-party aggregator, should be required.

Question 7. *"What else should CalPrivacy consider regarding CCPA notice and disclosure requirements?"*

One additional consideration relates to the quality and meaningfulness of consent in operational agreements.

A generic terms-of-service clause embedded in an operational agreement should not be treated as meaningful authorization for downstream commercialization of personal information. The court in *Greystone* has now described what an opaque click-through looks like in practice. The CCPA framework should not give bundled, undifferentiated authorization the same weight as a specific, separately presented, and knowing consent.

All of the recommendations in this comment respond, in some form, to this catch-all question. See also the Employee Data recommendations below.

II. Employee Data

Question 1. *"What are your expectations or concerns regarding why businesses collect, use, disclose, or retain your personal information as a job applicant or employee?"*

The principal concern, drawing on the observations earlier in this comment, is the gap between what employees would expect (limited collection, retention only for purposes they have authorized, no commercialization without notice) and what actually occurs (bulk transmission, indefinite retention, downstream commercial use without notice to the employee).

The Agency should examine whether bulk upstream transmission and indefinite retention of employee payroll data, including for employees who never have and may never have any verification need, is consistent with the CCPA's purpose-limitation requirement at Civ. Code § 1798.100(c). The scale of non-current retention in the current architecture is substantial. In its 2025

annual reporting, Equifax disclosed that The Work Number held 813 million total records at year-end 2025, of which 209 million (approximately one-quarter) were classified as “active.” That leaves more than 600 million records of historical or non-current employment data held by the aggregator for purposes that have no reasonable nexus to the underlying employee's current circumstances. An employee may work for the same employer for two months or twenty years and never apply for a mortgage, an apartment, or another job that triggers a verification request. Yet under the current model, that employee's payroll record is transmitted and held by the aggregator indefinitely. The infrastructure to implement purpose-limited retention already exists in the current data flow: payroll processors routinely transmit termination dates to verification platforms as part of normal updates. There is no technical or operational obstacle to flagging a record for deletion upon termination, or for non-renewal after a defined period of non-use.

More broadly, the bulk-storage architecture itself is not the only available option. A request-at-time-of-need architecture, in which employee data is queried from the employer or payroll processor at the moment a specific verification is requested, would produce the same verification result without the bulk upstream transmission or the indefinite retention this recommendation addresses. The 209-million-active-out-of-813-million-total ratio is itself evidence of what bulk storage produces when most of the stored data is never queried.

The disclosure-related recommendations under Notices & Disclosures Question 1 above also respond to this concern.

Question 3. *“What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?”*

Two recommendations from the Notices and Disclosures section above apply directly to this question: the recommendation that the Notice at Collection identify the aggregator by name (under Notices & Disclosures Question 1), and the recommendation that the service-provider contract requirements in § 7051 reach the third-party payment side (under Notices & Disclosures Question 3), so that businesses have the information they need to make accurate disclosures.

Question 5. *“What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights? How can the regulations address this issue?”*

A core challenge is that the original consent moment (typically at the application or hire stage) is fixed in time, while data releases from the aggregator continue for years afterward. Granting employees a real-time mechanism to refuse specific subsequent releases addresses this directly.

The mechanism is this: when a consumer applies for an apartment, a loan, or a job, they typically sign a release form authorizing the verifier to obtain employment and income data. That signed authorization is what legally permits the verifier to query the aggregator, and it does in fact give that permission. The problem is that once signed, the authorization persists; there is no operational mechanism for the consumer to withdraw it, even after the underlying transaction has been completed, declined, or abandoned. A renter who applied to four apartments and signed a lease on one has, in practice, given four separate verifiers ongoing authority to pull their employment record, with no way to revoke the three they no longer have any relationship with. A car buyer who walked away from a loan should not have the dealership continuing to query their employment record. A job candidate who accepted one

offer should not have four other interviewers still pulling verifications on them. The signed authorization was meant to enable a specific transaction; in operation it functions as an open-ended license that the consumer has no practical means to close.

Consumers should have a real-time right to deny release of their employment and income data on a per-query basis, after the original consent moment has passed. The current framework assumes a single act of consent at the application moment. By the time a downstream verifier actually pulls the consumer's record, the consumer's situation may have changed entirely. CalPrivacy should consider establishing a consumer right to block specific downstream verifier queries once the underlying business relationship with that verifier has ended or been declined, and a parallel right to affirmatively revoke a previously signed authorization once it is no longer needed for its original purpose.

See also the real-time notification recommendation under Notices & Disclosures Question 4 above.

Question 6. *"What steps do businesses take to oversee their service providers' and contractors' CCPA compliance, and what challenges do businesses face when doing so?"*

As discussed in the analytical section earlier in this comment, the oversight contemplated by §§ 7050-7053 is not, in practice, reaching downstream retention practices of the aggregator. The active/total record split (209 million out of 813 million) is direct evidence of this gap. The recommendation responding to this question is the service-provider contract flow-through provision (under Notices & Disclosures Question 3 above), which would equip the business with the information it needs to actually conduct meaningful oversight.

Question 7. *"What else should CalPrivacy consider regarding CCPA requirements for job applicants and workers in the employment lifecycle (hiring, working, and offboarding)?"*

All of the recommendations in this comment respond, in some form, to this catch-all question.

Closing

The employment verification industry is no longer a marginal back-office function. It now touches a substantial share of the working population, and its operation is documented in detail across public corporate disclosures and the federal court record. The CCPA's existing notice and service-provider rules predate much of that documentation. CalPrivacy has the opportunity to update those rules now, in light of what the public record shows about how this market actually operates, and to spare the employees and employers I work with from discovering, after the fact, what they had unknowingly authorized.

The technology to implement these protections, real-time notification, per-query consent mechanisms, and request-at-time-of-need verification architectures, already exists in commercial use. The choice before the Agency is not whether such protections are feasible, but whether the regulatory framework should require them.

I would welcome the opportunity to provide additional details or participate in any workshops or working sessions the Agency may convene.

Thank you for the opportunity to submit this preliminary comment.

Respectfully submitted,

Robert Mather
Founder, MyEmployment
robert.m@myemployment.com
(702) 508-6474

Catbagan, Christian@CPPA

From: Jane Faull <jfaull@calbankers.com>
Sent: Tuesday, May 19, 2026 12:30 PM
To: Regulations@CPPA
Cc: Jason Lane
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: CalPrivacy Preliminary Comments.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Good afternoon,

Please see attached the preliminary comments from the California Bankers Association regarding Notices & Disclosures and Employee Data from the April 2026 inquiry. Please let me know if you have any questions.

Best,
Jane

CALIFORNIA BANKERS ASSOCIATION

Jane Faull
Government Relations Assistant & PAC Coordinator
1303 J Street, Suite 600| Sacramento, CA 95814
T: (916) 438-4419
www.calbankers.com
Connect: Website | Twitter | LinkedIn

Bringing members together. Making our banks better.

CALIFORNIA BANKERS ASSOCIATION

May 19, 2026

To: California Privacy Protection Agency

Subject: Preliminary Comment – Notices & Disclosures and Employee Data April 2026

Dear California Privacy Protection Agency,

On behalf of the California Bankers Association (CBA), we appreciate the opportunity to provide preliminary comments regarding the California Privacy Protection Agency's (CalPrivacy) exploration of regulatory changes for notices, disclosures, and employee data.

The following comments reflect the practical challenges faced by financial institutions in balancing comprehensive privacy protections with the complexities of employment law and operational scalability.

I. Notices and Disclosures

Challenges in Describing Information Practices

A primary challenge for businesses is determining the appropriate level of granularity when describing data elements and processing purposes. This is particularly difficult in an employment context where data use is multifaceted.

We recommend that the Agency provide specific examples of 'baseline expectations' for disclosure. Clearer templates or use-case scenarios would help businesses ensure they are meeting the 'correct' level of detail without creating overly dense disclosures that ultimately confuse the consumer or employee.

Notices and Opt-Out Links Across Platforms

For many of our members, specific opt-out links are not currently applicable as they do not 'sell' or 'share' employee data in a manner that triggers those specific CalPrivacy requirements. In these environments, participation in optional programs (e.g., wellness initiatives, alumni networks, or employee resource groups) is the primary mechanism for choice; if an individual does not wish to participate, they simply do not provide the data.

II. Employee/Applicant/Contractor Data

Challenges in Providing Notices

While businesses successfully utilize job application portals and onboarding tools to deliver CalPrivacy notices, the logistics of 'off-cycle' notices present significant hurdles. Annual delivery to

1303 J Street, Suite 600, Sacramento, CA 95814 tel 916.438.4400 fax 916.441.5756 calbankers.com

existing employees is integrated into 'business-as-usual' (BAU) cycles. However, a regulatory requirement to deliver mid-year or off-cycle notices for minor updates creates a substantial administrative burden. We encourage the Agency to allow for flexible delivery methods that align with existing corporate communication cycles.

Challenges in Exercising Privacy Rights

Financial institutions face specific friction points when fulfilling employee data requests:

1. Retention vs. Privacy: Tension between privacy 'deletion' rights and HR legal requirements (e.g., litigation risk). Without a clear regulatory POV on retention, employers make inconsistent, risk-based decisions.

2. Authentication: Verifying former employees/applicants without collecting excessive data is difficult. Safe harbor guidelines for minimum authentication would be helpful.

3. Scope of Access: Unclear which HR documents (like investigative reports) are subject to access. Clear direction on excluded categories is necessary.

Service Provider Oversight

CBA members manage compliance through rigorous third-party management protocols. When data access requests involve third-party processors, businesses partner directly with those providers. This collaborative model is effective but relies on clear definitions of 'Service Provider' vs. 'Third Party'.

The Employment Lifecycle & Emerging Technology

Balancing process automation (AI/ADMT) with privacy risk is complex. In high-volume environments, a strict 'opt-out' requirement is not always operationally feasible. Overly rigid requirements may prevent large employers from adopting efficiencies that could improve the employee experience.

We look forward to further engagement as the Agency moves toward formal rulemaking.

Sincerely,
Jason Lane
Senior Vice President and Director of Government Relations
California Bankers Association

JL:jf

Catbagan, Christian@CPPA

From: Kevin De Liban <kdeliban@techtonicjustice.org>
Sent: Tuesday, May 19, 2026 1:58 PM
To: Regulations@CPPA
Subject: Preliminary Comment – Notices & Disclosures and Employee Data April 2026
Attachments: 26.05.19 CCPA Preliminary Comment.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please see comment attached. Thank you!

--
Kevin De Liban, President and Founder (he/him)
TechTonic Justice
Cell: [redacted]
Sign up for our newsletter!

TECHTONIC JUSTICE

May 19, 2026

California Privacy Protection Agency
Attn: Legal Division – Regulations
400 R St., Suite 350
Sacramento, CA 95811

Re: Preliminary Comment – Notices & Disclosures and Employee Data April 2026

Dear Executive Director Kemp, Agency Staff, and Board Members,

TechTonic Justice writes to respond to the California Privacy Protection Agency's April 20, 2026 invitation for preliminary comment on Notices & Disclosure and Employee Data as regulated by the California Consumer Privacy Act (CCPA).

TechTonic Justice is a 501(c)(3) national nonprofit organization advocating for the interests of poor and working-class communities whose basic human needs are impacted by artificial intelligence and emerging technologies. We leverage multidimensional, legal, and organizing strategies to strengthen local justice movements serving the communities that AI is leaving behind. We have trained thousands of legal aid attorneys, youth defenders, and other community-based advocates to defend the rights of economically vulnerable communities against harmful technologies and automated systems that disrupt access to public benefits, healthcare, employment, education, housing, and human rights.

We welcome the continued attention by Agency leadership, staff, and board members to the goal of ensuring that workers in California are fully protected by the CCPA in the collection and use of their data.

To that end, we would like to direct the Agency's attention back to the input provided over the last two years by a large working group of labor and civil society groups, which together represent hundreds of thousands of workers and consumers. We invested significant time analyzing draft regulations, gathering

evidence from impacted workers, summarizing academic research, writing responses, and giving public comments at board meetings. In 2025, these efforts culminated in two working group letters giving input to the agency's rulemaking on Automated Decisionmaking Systems (ADMTs) and Risk Assessments:

- In our group recommendation letter (January 9, 2025), we laid out a robust, sharply articulated, and fully documented set of worker priorities for the rulemaking process.

- In our group response letter (June 2, 2025), we document and express our profound disappointment that none of our worker priorities were adopted in the final regulations.

While these letters were developed during the previous rulemaking process, all of their major recommendations respond to either question #7 for Notices & Disclosure or question #7 for Employee Data. More generally, the working group's substantive priorities remain the same as articulated last year, including broadening the definition of ADMT so that it works for workers; requiring post-use notification when ADMTs have been used to make a decision about workers; and establishing the right for workers to challenge those decisions.

We therefore respectfully request that the Agency review the two letters referenced above as part of its deliberations on whether or not to commence a new rule-making process.

Sincerely,

Kevin De Liban, President
TechTonic Justice

Catbagan, Christian@CPPA

From: Jennifer E. Kooper <jkooper@cefcu.com>
Sent: Tuesday, May 19, 2026 2:58 PM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Comment from CEFCU:

Any updates to either should prioritize alignment with existing processes and disclosure protocols, avoid duplicative or conflicting requirements, emphasize usability, and minimize added complexity or confusion.

Thank you,

Jen Kooper
CA-Compliance Coordinator
670 Lincoln Ave. San Jose, CA 95126
T: 408.955.1304
www.cefcu.com | jkooper@cefcu.com | Secure File Drop

CEFCU Not a bank. Better.

This promotional email was sent to you by Citizens Equity First Credit Union located at P.O. Box 1715, Peoria, IL 61656-1715. If you no longer wish to receive promotional emails from us, please go here.

The information contained in this e-mail is intended only for the addressee and may contain confidential and/or privileged material. Any interception, review, retransmission, dissemination or other use of this information by persons or entities other than the intended recipient is prohibited by law and may subject them to criminal or civil liability. If you received this communication in error, please contact the sender immediately by reply email and delete all copies of the original message.

Catbagan, Christian@CPPA

From: [redacted]
Sent: Tuesday, May 19, 2026 9:28 PM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: 20260520_Cal_Privacy_comments.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hi!

Thank you for the opportunity to comment!

I am a California resident/consumer who wishes to remain anonymous and has created the attached comments reflecting my opinions for your consideration.

Thank you!

Thank you for the opportunity to provide comment and for your questions.
My responses are in blue font below.

CalPrivacy is particularly interested in receiving comments addressing the questions provided below. Additionally, stakeholders may want to propose specific language for new regulations related to notices and disclosures, or employee data. Commenters are encouraged to review the short "Tips for Submitting Effective Comments" guide for help formulating and submitting effective comments.

Questions for Preliminary Comment
I. Notices and Disclosures
1. When reviewing a privacy policy or similar disclosure, what is the most important information to consumers?

I care most about sensitive data (health and health-related, inferences about the functioning of the mind, audio and video recordings, is biometric info extracted form them on a routine basis, how long they are kept). I want to know whether the sensitive data is being collected/generated, what specifically it is being used for (not just the general business reason). I care about whether data is being sold, for any reason, not just for cross-context behavioral advertising. Here is more detail on things I am searching for in a privacy policy:

A. Handling of inferences about the functioning of the mind

1. Are inferences about the functioning of the mind (e.g. intelligence, psychological trends, aptitudes) **being collected or generated**?
2. If yes, what specifically are they being used for?
    1. Are they being used to **set prices** for an individual?
    2. Are they used for **adversarial reasons**, for example, to discredit a customer on social media it deems a threat to the commercial interests of the company? (A grocer's Washington state disclosure has said that it may use your consumer health data to "administer our relationship with our customers." What does this mean?)
3. Are inferences about the functioning of the mind **being sold for any reason**, not just for cross-context behavioral advertising? If so, for **which specific reasons** are they being sold? And what are the **allowed uses** of this data once it is sold?

B. Health-related and Medical data

1. Same questions as for inferences about the mind, plus the following:
2. Does a company commit to never creating inferences about my health or mental health without my consent, because such data may be considered as medical data as AI becomes better, thus preventing me from ever having it deleted.
3. Does a company commit to never to having my data reviewed by a medical professional without my consent? (which, even more than inferences by

themselves, might be considered to create medical data and so prevent me from ever having it deleted).

4. Does the company require the same commitment from any service providers or people who buy my data?
5. What data specifically does the company collect that it considers health-related information (which is thus subject to 'sensitive data' restrictions)? Not just examples, but a full listing of the health-related info it collects. For example, intelligence, psychological trends and aptitudes might be considered health-related information, is this treated as such by the company? Is a security video in which an ailment is visible treated as health-related?
6. What info specifically does the company collect that it deems true medical data (subject to other laws such as HIPAA or Confidentiality of Medical Information Act)?

C. Data that is sold

1. Which data is being sold for which specific reasons?
    1. Does a company sell for "security purposes" identifying information about me such as a from video of me on its premises? In other words, does it sell info not subject to my 'do not sell' instruction, because the information is being sold for security reasons, not marketing reasons? After it is sold for 'security reasons', can it be used for anything else?
    2. Does a company sell information about me for use by another party for free speech, commercial speech (but which is not cross-context behavioral advertising to me) or legal purposes?

D. Video & audio recordings

1. Are video/audio recordings being made in the place of business (including in small business restaurants)?
2. If yes, where are these stored (cloud or onsite only) and who owns/has access to them?
3. If yes, are these recordings being processed to extract biometric info on a routine basis or is biometric info extracted only if there is probable cause due a security incident that actually happened on site?
4. If biometric info is being extracted from videos of me on its site, will this ever be used to deduce my ailments (by the company, its service providers or anyone who may receive the data)?
5. How long are video/audio retained for "security purposes" if there has been no security incident between consumer and the company?
6. If biometric info is extracted from video/audio before it is deleted, how long is this kept?
7. Does the company commit to providing copies of audio/video recordings as part of a Right-To-Know request, particularly given that so many audio recordings are stated to have been made for 'quality control and training purposes'?
8. Will the company commit to providing transcripts of customer service interactions as part of its Right-To-Know request?

9. Does the company request explicit consent before extracting biometric info from recordings?

What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?

1. Much of the **information listed in answer to your first question above** (which info consumer finds important) often seems unavailable
2. Specific **retention period information** — I have found something akin to "as long as necessary" nearly every time I've looked for this
3. Disclosures **in situ for doorbell and other outdoor cameras** for non-owners of the camera, where people may not be aware they are being recorded. I believe the public previously had a certain expectation of privacy in public places (of not being recorded):
    1. I myself did not know that I was being recorded as I went house-to-house for a civic reason — I would have dressed differently had I known this and perhaps not spoken to my neighbors
    2. An acquaintance told me she was not worried about being recorded in restaurants because she always eats outside…not realizing that often restaurants can have cameras aimed at parklets recording you as you eat/ interact with others (aimed at a public space)
4. Specifically disclosures **on the door at grocery stores** about whether you are being identified as an individual via security cameras or other indirect measures (i.e. against your will or without your awareness) and under what circumstances?
5. When a company is "unsure" whether I am the data subject of information they have after I've submitted a Right-To-Know request, **which fields of information are they unsure about** and **what do I need to provide** that will confirm I am the data subject? Often I am told something like: we have information but we are not sure it's yours, so we're not giving it to you — followed by non-response to my follow up.
6. When a company doesn't delete your data, responding that it is a service provider, but also may be a service provider for many, many companies (e.g. Square, logistics companies), and you don't know who the original companies are you interacted with, what is the list of **original companies you interacted with**? (I asked one such firm for this info and did not receive an answer.)
7. CPRA disclosures from firms governed by Gramm-Leach-Blily
8. CPRA disclosures from firms governed by ERISA
9. If the company has biometric information about me in particular, and I have made a Right-to-Know request, **which biometric info exactly do they have about me**? (I would like to see field level names for this data which they will not provide me).
10. After I've submitted a delete request, **exactly which info has been retained** about me after the delete request was executed and **under which exception/ code** section has each piece been retained? For example, if a company

continues to retain after my delete request biometric info about me or inferences about the functioning of my mind for a 'security' reason or due to the legal, medical or free speech exception, it needs to go on record regarding this. I believe this is crucial to stem abuses of the exceptions. If there has been no 'security' incident involving me or it claims work product protection and there is no hint of anticipation of litigation, forcing them to provide written justification for retention of such data could go a long way.

Because I have come to believe (after submitting many privacy requests) that many companies are operating in bad faith/exploiting consumers, I am particularly interested in notice/disclosure requirements that force companies to make statements **that can be either proved or disproved**.

2. What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?

1. When companies have a **privacy popup window that does not explain what the sliders turned on/off actually mean** — for example, I have seen a company label the entire privacy slider window as the opposite of what one might expect without explaining what the right/left state mean for the sliders. This can lead you to potentially set the sliders to the opposite of what you intended. Yes, the slider rows have a description, but it is not clear what turning on or off the sliders themselves does. And, when I asked a company what the meaning of the slider to the right or left meant, the company did not respond.
2. A tech company that provides operating system, computer applications and web applications **having many different places you need to set privacy settings** and which **also engages in "account switching."** I recall this company logged me in to my entire computer with the login I used to purchase a spreadsheet application (i.e. logged me in to my computer with an id where it knew who I was, whereas I had originally created and used a computer login without the tech company knowing who I was as a person.)
3. **Not knowing whether I have to navigate elsewhere to effectuate my privacy selections or not**. For example, a tech company has a button to limit use of sensitive data that I thought effectuated my request to limit, but then also says there is another page with more info about choices. When I navigate to the other page, there are 30 sliders listed under 6 different sub-brands, all *set permissively* invalidating my request to limit (for example, turned on is consent to sell or share my data.) The company says I previously set these this way (every time I visit)? If I have indicated via button intention to limit I would hope this would be honored if I make no other active selections.
4. **Not knowing where to find the applicable privacy controls**— I would have said "no" if a ridesharing app had asked me upon installing if I agreed to sell or share my data. I did not realize until later there was a privacy control in the app itself *in addition* to the Apple privacy control setting for the app, that had been set without my awareness to my consenting to sell or share. I would prefer to be asked up front, especially when there is no way for me to restore my privacy situation to the state it was before I made the error.

5. When companies do not address specifically in their policy the how to request data **for a user who doesn't have an account**, which cunsumers may not know is a right. For example, a company may state that you must login to make the a right-to-know request.
6. When a company makes a statement that may be true about itself but it is **not clear who else it is true for**. Is it true also for its service providers or for others whom the company sells the data to? For example, a company states that "We do not analyze customer data to make inferences about our customers' past, present, or future physical or mental health status." But it is not clear who "we" is. Does its service providers do this very task and provide the inferences to it? Does it buy such inferences from third parties and use them to set prices or to discredit a consumer on social media, since it also states that it uses consumer health data to "administer our relationships with our customers"?
7. Confusion around whether you have a right to limit because of an issue with "and/or" language in the law/regulations —-the wording of the exception under 7027(a) and 1798.121(d) can be exploited by companies claiming that they do not have to offer or abide by limit request because they **only collect but do not process the data with the intent of inferring characteristics**. I have run into a company that claims it does not have to offer the right to limit because it does not "process" the data for this purpose. When I asked if it SHARED sensitive info for the purpose of developing a profile, it simply repeated its claim that it does not 'process' the data for the purpose of inferring characteristics.

3. What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this issue?

4. What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights?

For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?

- I would like an option to have my 'opt out of sale or share' and 'limit sensitive data to minimum' selections to **apply to all devices, apps etc for me as a natural person for a particular company**— i.e. a global selection for me that cannot be overridden by anything else that I have not actively changed subsequently.
- I would like an **interaction required during installation of an app or first use** asking me if I want to 'opt out of sale or share' and whether to 'limit use of sensitive data to minimum' — not just link to privacy policy. I was dismayed to find I had allowed the default "sell or share my data" setting by Lyft application to remain permissive because I did not know this was set or how to access this setting. Of course, I cannot "undo" this error, which may have been known to Lyft when specifying design of the application. If we must have an 'opt out' framework, I would still like to be asked upon first use whether I agree with being opted in and presented the option right then and there to opt out of everything where there is an option to do

so, including ability to limit use of sensitive data. In other words, opted-in by default, but allow up-front opt-out of everything.

- I would like an option to **"mimimize" information collection & use for all products from a company to bare minimum** and still function at all for me as a natural person. For example, I am bothered how Apple is always installing new apps and setting the apps' settings permissively.
- I would love the **Drop system to apply to all businesse**s, not just data brokers — in essence for Calprivacy to provide the standardized notification regarding delete request.
- I would love to set a **"do not sell" setting at the Drop system** and have all businesses be required to honor for all products/applications/settings — in essence, CalPrivacy provides the standardized notification of opt-out of sale for cross context behavioral advertising
- I would love to set a **"limit use of sensitive data" setting at Drop system** and have all businesses be required to honor.
- I would love for there to be a **'delete my info as soon as transaction is complete'** button included in every confirmation email/purchase screen.

5. What challenges do businesses face when providing notices, including opt-out links, across different devices or platforms? How can the regulations address this issue?
6. Please provide examples of effective consumer notices and disclosures. If possible, please provide information about specific testing, studies, or data demonstrating their effectiveness.

I personally find **tables** helpful, so that you can see when info is missing and know that data in each column is all supposed to be of the same type. I also would like to see **full lists of data collected/used, not just examples** of data that is in each category, which I find can be misleading.

I would personally find useful **a set of yes/no questions** to be answered such as:

- Does your company collect or create inferences about the functioning of the mind such as intelligence, psychological trends, aptitudes?
- If yes, please answer:
  - Have you ever used this data to set prices for an individual?
  - Have you ever used this data to negatively impact the reputation of a consumer online?
  - Have you ever used this data to negatively impact a consumer in a legal proceeding?
  - Does your company commit to not ever causing such data to be reviewed by a medical professional without the active consent of the data subject?

- Does your company sell inferences about the abilities of the mind for any reason?
  - If yes, please list all the reasons for the sale and
  - the full set of allowed uses of the inferences by the buyer

- Does your company extract biometric data from video footage other than after a security incident that actually happened between you and the consumer in which the consumer is a suspect?
- Does your company attempt to identify consumers on your premises, from any source such as security footage in which the customer has not consciously & directly given you their identity information, when there has been no current security incident involving the consumer on your premises?
- Please give a retention range for the following types of data if there has been no suspected security incident involving the consumer and your company and no specific indication from the consumer that he/she may sue your particular company. (choices: 0-3 mo, 3-6 mo, 6mo-1 yr, 1 yr-3 yr, greater than 3 yrs)
  - Video footage
  - Biometric information
  - Call recordings
  - Call transcripts
  - Health-related information
  - Location information
  - Inferences
  - Health-related information
- Does your company have in its possession a list of websites visited by a consumer who has not visited one of your sites (online or in person).
- Does your company generally have in its possession a list of websites thought to have been visited by a consumer who has visited one of your sites (online or in person).

7. What else should CalPrivacy consider regarding CCPA notice and disclosure requirements?

I understand the effectiveness of the Opt-Out framework in California depends on the effectiveness of notifications/disclosures to ensure that consumers are providing informed consent. Likewise I understand the effectiveness of notifications/disclosures depends on how much risk (likelihood of prosecution + cost) businesses perceive from violating the regulations/laws.

Thus I wonder if it would be remiss not to discuss here **perceived risk from violating the notification/disclosure regulations**. Below I try to do this.

Given how often I have received:

a) No response whatsoever to my Right-To-Know requests
b) A response misconstruing my request (e.g. suggesting I submitted a 'Delete' rather than 'Right-To-Know' request)
c) Non-response to my followup after a business's misconstrual of my request
d) When I do receive any data at all, the frequency that it contains no inferences at all (I think ~90% of the time)
e) The fact that I have never received inferences about the functioning of my mind (estimates of my intelligence, psychological trends over time, aptitudes) despite all the requests I have made and
f) the number of times I have received info about me as a user that is not logged in (0),

….I am concerned that the **risk businesses perceive for violating the disclosure regulations may be too low**.

Likewise, many individuals I speak with are not aware that inferences about intelligence, psychological trends or aptitudes are commonly available to businesses and have been for a long time. This to me suggests a disconnect between the disclosures/fulfillment of privacy requests in practice and the intent of the laws laws/regulations. Many individuals I speak with are also not aware that different prices may legally be offered to different customers. Additionally, many individuals I speak with are not aware that wellness application information, because is not generated by a doctor's office, is not subject to HIPAA and so can be readily sold, including psychological data, and that this data could be used against them if they were to get into a dispute with a business.

For the above reasons, I am wondering if the opt-out framework with its reliance on notifications/disclosures would be **more appropriately paired with a private right-to-sue or, barring that, a PAGA-like mechanism** to assist CalPrivacy's dedicated enforcement division and Attorney General's office?

Thirdly I have heard the suggestion that American society is 'litigous' and that companies are burdened by compliance obligations. While there may be truth to these observations, many people may not realize that there are many practical limitations to getting justice in our society having to do with resources available to prosecutors and agencies, or training issues, unintentional biases pervasive in our society, and even the economics of lawyering.

Suffice it to say, while businesses may validly complain of compliance obligations associated with doing business in California, I believe these companies are still many times more powerful than the average resident, whom I believe desperately needs any protection that the Calfornia Legislature or CalPrivacy may provide.

II. Employee Data

For purposes of these questions, "employee" includes current and former employees as well as current and former independent contractors.

1. What are your expectations or concerns regarding why businesses collect, use, disclose, or retain your personal information as a job applicant or employee?

I am concerned that many businesses may present a veneer of respectability but too often act in unprofessional, arbitrary, biased and even brutal ways if challenged. I also believe many regular employees facilitate corporate misconduct because they are afraid to speak up and endanger the source of their paycheck. Thus, the more power commerical organizations have, the more I worry.

I would like to see organizations forced to provide all data they have about an employee or former employee, even if the data is designated as security data or any other type of

data. If a company is truly concerned about creating a security issue by giving out the data, it can give it to a person's health care provider or representative — but they must allow access. If there is any data a company has but is not providing, I would like to see them provide a detailed listing of this data and the reasons why not providing each piece.

I would like to see executives subjected to any data treatment they subject their employees to, and provide employees access to this. (Thank you for the opportunity to provide this comment).

I am concerned that many companies spend their resources fighting employee lawsuits through the conduct of their HR departments instead of learning about bias and trying to reduce it. I would like to see companies be forced to publish and investigate differences they may uncover about employees in protected classifications when analyzing employee data.

I would be concerned if private conversations between employees are recorded, while I actually believe that discussion regarding every business decision should be recorded and retained.

2. Have you received a copy of a business's privacy policy, Notice at Collection, or CCPA rights' notices as a job applicant or employee? Probably, but don't recall.
a. Identify each notice you have received and describe your experience receiving the notice.
For example, how did you receive the notice(s), at what point in the employment life cycle (hiring, working, offboarding) did you receive the notice(s), and what was the most helpful information in the notices.
b. Do you have any suggestions on how to improve the effectiveness of the notice?
3. What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?

4. Have you exercised your CCPA rights as a job applicant or employee? Yes
a. Describe your experience exercising your rights. I submitted a request online, I think I was not allowed to express how far back I wanted the request to go using the form. It was fulfilled within I think 90 days.
b. Describe any challenges you experienced when exercising your rights.
I was not provided with any inferences — it only included routine employment data or data I provided. It was not mentioned whether the data included data from its service providers, what data it has about me but which it did not provide and the specific reason for withholding each piece of data it has but did not provide. It is known to have service providers that collect data extensively and may be providing such data to it under ERISA.

c. Do you have any suggestions on how to improve the experience? I would like an detailed (field level) accounting of data that it has but it is not providing and the reasons why not providing each piece.

5. What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights? How can the regulations address this issue?

6. What steps do businesses take to oversee their service providers' and contractors' CCPA
compliance, and what challenges do businesses face when doing so?
For example, do businesses conduct audits of these entities or test the service provider's
or contractor's systems? How effective are these audits and tests to assess a service provider's or contractor's CCPA compliance?

7. What else should CalPrivacy consider regarding CCPA requirements for job applicants
and workers in the employment lifecycle (hiring, working, and offboarding)?

Catbagan, Christian@CPPA

From: Matt Schwartz <matt.schwartz@consumer.org>
Sent: Wednesday, May 20, 2026 8:29 AM
To: Regulations@CPPA
Subject: Consumer Reports Submission --- Preliminary Comment – Notices & Disclosures and Employee Data April 2026
Attachments: _Comments of Consumer Reports In Response to the California Privacy Protection Agency's Invitation for Preliminary Comments on Notices & Disclosures and Employee Data.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Good morning,

Attached please find comments from Consumer Reports in response to CalPrivacy's Invitation for Preliminary Comments on Notices & Disclosures and Employee Data.

Best,
-Matt

--
Matt Schwartz
Senior Policy Analyst
o (914) 378-2169 | m[redacted]
Pronouns: he, him, his
CR.org

***
This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.
***

Comments of Consumer Reports
In Response to the
California Privacy Protection Agency's
Invitation for Preliminary Comments on
Notices & Disclosures and Employee Data

By

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

May 20, 2026

Consumer Reports[1] thanks the California Privacy Protection Agency (CalPrivacy) for the opportunity to provide feedback on its Invitation for Preliminary Comments on Notices & Disclosures and Employee Data. We appreciate the spirit of this rulemaking, though we think it is worth considering whether privacy policies can or should play a central role in the consumer experience of privacy laws. We've long argued that instead of doubling-down on the failed notice-and-choice regime, privacy laws should move toward more substantive default protections, such as data minimization, that alleviate the burden on consumers to manage privacy choices in an untenably complex ecosystem.[2]

That said, we understand that CalPrivacy must operate under the constraints of the statute—and that the ancillary benefits of privacy notices that may accrue to other stakeholders, such as regulators, journalists, and advocates, justify further attention. We therefore offer several suggestions for how CCPA's rules around disclosures and notices can be improved, some of which were shared in a previous comment.[3]

Our recommendations include:

- Requiring businesses to plainly state whether they believe themselves to be covered by CCPA;
- Requiring businesses to share the precise list of third parties with whom they have sold or shared consumers' personal information;
- Requiring businesses to detail their process for verifying consumer requests;
- Strengthening enforcement against businesses with broken privacy request links.

Please note that CR does not take a position on the employer-facing aspects of this comment proceeding.

---

[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 and EPIC, How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking, (January 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf

[3] Matt Schwartz and Justin Brookman, 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, (April 6, 2026), https://advocacy.consumerreports.org/wp-content/uploads/2026/04/CR-Comments-CalPrivacy-Friction-and-OOPSs.pdf

General Views

Before describing how we believe that CCPA's existing notice requirements could be improved, it is worth taking stock of the role of notices in privacy laws and assessing who the audience for any such improvements should be. On the positive side of the ledger, there is some evidence that privacy policies and other consumer-facing notices and disclosure can play an important role for expert audiences and those with a particular interest in holding companies accountable for promises made to consumers—such as regulators, journalists, and advocates. As enforcers have noted, privacy policies are often a leading indicator of deeper data governance issues within a business.[4] If a business cannot clear the low bar of writing a legible or legally compliant privacy policy, it may suggest that privacy is not a priority for the business. Conversely, the very act of writing privacy policies can sometimes improve business' own understanding of their internal procedures and external relationships in a way that can improve privacy outcomes for consumers.[5]

More thorough inspection of privacy policies can also sometimes reveal prima facie privacy issues. For example, Consumer Reports' investigation of several major exercise equipment companies found that it was common for companies to give themselves permission to share health-related information with marketing and social media companies.[6] And an earlier Consumer Reports investigation into seven of the leading mental health apps showed that they had significant privacy issues: many shared user and device information with social media companies and all had confusing privacy policies that few consumers would understand.[7]

However, there is substantially less evidence that privacy notices currently serve an systemically important role for consumers themselves—or that tinkering with the form of privacy notices can make a tangible improvement to consumers' understanding of inherently complex company data processing activities. The vast majority of consumers do not read privacy policies,[8] and if even they did, it would likely not be a productive use of time. More than 15 years ago, researchers from Carnegie Mellon University estimated that the average internet user encounters an average of 1,462 privacy policies a year, and that it would take a user an average of 244 hours

---

[4] Josh Hansen, From Policies to Practice: What Regulators Expect from Privacy Programs, (April 14, 2026), https://www.jdsupra.com/legalnews/from-policies-to-practice-what-2886801/

[5] Peter Swire, The Surprising Virtues of the New Financial Privacy Law, 86 MINN. L. REV. 1263, 1316 (2002), https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=3082&context=mlr

[6] Catherine Roberts, Your Exercise Bike Knows a Lot About You—and It Doesn't Keep Every Secret, Consumer Reports, (January 14, 2025), https://www.consumerreports.org/health/health-privacy/exercise-machine-privacy-a3907557984/

[7] Thomas Germain, Mental Health Apps Aren't All As Private As You May Think, Consumer Reports, (March 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/

[8] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information 5 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf

per year to read the privacy policy of every website they visited.[9] The number, length, and complexity of privacy policies have surely only skyrocketed since then and Carnegie Mellon's estimate does not account for the time it would take for consumers to *comprehend* the privacy notices, only to read them.

The obvious pushback is that privacy policies should therefore be made simpler and more legible for the average consumer. But as privacy scholar Helen Nissenbaum has pointed out, there is an inherent "transparency paradox" whereby the more readable and simpler privacy policies are, the less meaningful and accurate they are likely to be.[10] Simplified privacy "nutrition labels" appear to modestly improve consumer understanding,[11] but risk obfuscating more complex risks associated with data collection or transfer and are often inaccurate in practice.[12] This is likely to become an even greater issue as company data processing activities increase in complexity or further rely on "black box" algorithms that the companies cannot even themselves fully explain.

It is also worth mentioning at the outset that CCPA and the regulations already include fairly detailed requirements for the content and form of privacy notices. Privacy notices and disclosures are required to use "straightforward language and avoid technical or legal jargon"[13], to offer a "comprehensive description of the business' online and offline information practices,"[14] and to clearly disclose how certain categories of personal information are collected and with whom they are shared.[15] Anecdotally, it appears that many businesses are not complying with these baseline requirements, especially those around readability (subjective as the standards may be). In practice, more vigorous enforcement of existing privacy policy requirements may go further than additional requirements, especially if those additional requirements are not backed up with additional enforcement resources.

These concerns around the efficacy of privacy policies are part of the reason why CR supports the concept of data minimization—the idea that privacy laws should restrict businesses to only collect and use personal information that is necessary to provide the service requested by consumers. By putting the onus of protection on businesses, consumers are spared from making endless consent choices or having to read company privacy policies.

---

[9] Aleecia M. McDonald and Lorrie Faith Cranor, I/S: A Journal of Law and Policy for the Information Society, The Cost of Reading Privacy Policies, (2008), https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[10] Helen Nissenbaum, the Journal of the American Academy of Arts & Sciences, A Contextual Approach to Privacy Online, (2011), https://nissenbaum.tech.cornell.edu/papers/Contextual%20Approach%20to%20Privacy%20Online.pdf

[11] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, Robert W. Reeder, Carnegie Mellon University, A "Nutrition Label" for Privacy, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf

[12] Mozilla Study: Data Privacy Labels for Most Top Apps in Google Play Store are False or Misleading, February 23, 2023, https://www.mozillafoundation.org/en/privacynotincluded/articles/mozilla-study-data-privacy-labels-for-most-top-apps-in-google-play-store-are-false-or-misleading/#:~:text=The%20study%20%E2%80%93%20%E2%80%9CSee%20No%20Evil,provide%20false%20or%20misleading%20information.

[13] CCPA Rules Section 7003(a)

[14] Id., Section 7011(e)(1)

[15] Id.

That said, while we continue to believe that strengthening the data minimization provisions in privacy laws is the best way to improve privacy outcomes for consumers, we do have some suggestions for how CCPA's notice and disclosure requirements could be improved.

Responses to Select CalPrivacy Questions

When reviewing a privacy policy or similar disclosure, what is the most important information to consumers? What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?

While businesses are already required to disclose some of the most relevant information to consumers about business' collection, use, disclosure, and retention of personal information, we believe additional requirements may help consumers better understand their rights.

We offer the following recommendations.

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

As described in a previous comment,[16] we believe that businesses should be required to plainly state if they believe themselves to be covered by CCPA. 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

[16] Matt Schwartz and Justin Brookman, 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, (April 6, 2026), https://advocacy.consumerreports.org/wp-content/uploads/2026/04/CR-Comments-CalPrivacy-Friction-and-OOPSs.pdf

(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."*[17]

Businesses Should Disclose List of Third Parties to Whom they have Sold or Shared Personal Information

One of the privacy policy-related areas we've seen states improve on the CCPA is by requiring covered businesses to disclose the precise list of third-parties to which the business has sold or shared the consumers information (rather than just the categories of third-parties). Other states require businesses to either disclose this information in a section of the privacy policy itself,[18] or to do so upon the request of the consumer.[19] Businesses typically have the choice of either disclosing the list of third-parties that they have sold or shared a particular consumer's data to, or disclosing the list of *all* third-parties to which they have sold or shared personal information.

In some cases, a list of data recipients is likely to be highly material to a consumer's consent choice. For example, if a health website shares personal data with social media companies, a consumer may think twice about providing especially sensitive information. In addition, such disclosures are very helpful for enforcers and advocates to trace the flow of personal information and to hold companies accountable for their promises.

A third-party disclosure requirement could be created via rulemaking under the authority granted to CalPrivacy through Section 1798.185(a)(6), which allows the Agency to create rules and procedures to "facilitate" a consumer's ability to obtain information pursuant to Section 1798.130.

---

[17] 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/

[18] Rhode Island General Laws. § 6-48.1-3(a)(2), "Information Sharing Practices", https://webserver.rilegislature.gov/Statutes/TITLE6/6-48.1/6-48.1-3.htm.

[19] Minnesota Statutes, 325M.14(Sub. 1(a)(h)), https://www.revisor.mn.gov/statutes/cite/325M/full; Oregon SB 619, Section 3(1)(a)(B), https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled

Businesses Should Be Required to Disclose Verification Procedures

Another 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.

Expectations for Addressing Broken Links Should Be Higher

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 attempt 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 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.

What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?

One possibility would be to require businesses to share the subset of key information about their practices required in the Notice at Collection at the very top of a privacy policy. This would prevent consumers from having to hunt down the most relevant information, which may be hiding in far-flung regions of the privacy policy and may better facilitate their ability to make decisions.

A list of key information for the short-form notice may include:

- Whether the business is covered by CCPA.

- Whether or not the business is selling or sharing personal information to third-parties and for what purposes.
- Whether or not the business is selling or sharing sensitive information.
- A brief description of the categories of personal information being collected.
- A direct link to make a rights request.

What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights? For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?

Please provide examples of effective consumer notices and disclosures. If possible, please provide information about specific testing, studies, or data demonstrating their effectiveness.

While CR does not maintain a list of effective consumer notices and disclosures, we have encountered a variety of *ineffective* disclosures.

Some key examples:

- Consent flows that are presented to consumers in high-stress situations or part of a larger onboarding processes, such as when consumers purchase a car through a dealership, can lead to major gaps in consumer understanding. For example, the New York Times reported how the consent screens shown to millions of GM car purchasers were deceptive and led to consumers unknowingly consenting to having their personal information shared for insurance pricing purposes.[20]
- Modern smart televisions often collect invasive information from consumers under the guise of "automatic content recognition" are similarly euphemistic terminology. These settings are often difficult to identify and require multi-step processes to turn-off.[21] The Texas Attorney General recently sued several major TV manufacturers for alleged deficiencies in those companies' privacy policies and consent flows.[22]
- Recent research has demonstrated significant issues with the privacy disclosures of smart home devices.[23] In 14 percent of cases, researchers needed to use a smart device's companion app to review the privacy policy; in 49 percent of cases, researchers stated that the privacy policy was "difficult to obtain" (in one particularly perverse example, researchers were required to submit personal information to even access the

[20] Kashmir Hill, the New York Times, How GM Tricked Millions of Drivers into Being Spied On (Including Me), (April 25, 2024), https://www.nytimes.com/2024/04/23/technology/general-motors-spying-driver-data-consent.html
[21] James Wilcox, Consumer Reports, How to Turn Off Smart TV Snooping Features, (October 19, 2025), https://www.consumerreports.org/electronics/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/
[22] Office of the Texas Attorney General, Attorney General Paxton Sues Five Major TV Companies, Including Some with Ties to the CCP, for Spying on Texans, (December 15, 2025),
[23] Sunil Manandhar, Kaushal Kafle, Benjamin Andow,, Kapil Singh, Adwait Nadkarni, USENIX 2022 Proceedings, Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage, https://www.adwaitnadkarni.com/downloads/manandhar-sec22.pdf

privacy policy); and in 10% of cases, the manufacturer simply did not supply a privacy policy. This is especially concerning given the scale and invasive nature of data collection often implicated in this product category.[24]

****

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] Daniel Wroclawski, Consumer Reports, Smart Appliances Promise Convenience and Innovation. But Is Your Privacy Worth the Price?, (July 24, 2023), https://www.consumerreports.org/electronics/privacy/smart-appliances-and-privacy-a1186358482/

Catbagan, Christian@CPPA

From: Robert Boykin <rboykin@technet.org>
Sent: Wednesday, May 20, 2026 8:43 AM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: TechNet Preliminary Comments CalPrivacy - NOTICES & DISCLOSURES AND EMPLOYEE DATA 5.18.26.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hi CalPrivacy,

Please find TechNet's preliminary comments on the specified questions attached to this email.

Thank you,

--
Robert Boykin
Executive Director | California & the Southwest
TechNet | The Voice of American Innovation
(c) [redacted] | rboykin@technet.org
Twitter: @TechNetSouthwest

TECHNET
THE VOICE OF AMERICAN INNOVATION

TechNet Southwest | Telephone 408.898.7145
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org

May 20, 2026

California Privacy Protection Agency (CalPrivacy)
2101 Arena Blvd.
Sacramento, CA 95834

Re: Preliminary Comment - NOTICES & DISCLOSURES AND EMPLOYEE DATA

Dear CalPrivacy,

On behalf of TechNet, I am writing to provide preliminary comments in response to CalPrivacy's invitation regarding potential regulatory changes related to notices and disclosures, and employee data. TechNet appreciates the opportunity to contribute to CalPrivacy's preliminary rulemaking activities and offers the following observations.

As an initial matter, TechNet urges CalPrivacy to refrain from initiating new rulemakings on these topics at this time. California businesses are currently navigating a period of significant regulatory expansion. CCPA obligations are being layered alongside new requirements tied to risk assessments, automated decisionmaking technology (ADMT), cybersecurity audits, and other requirements which carry compliance deadlines that are still being interpreted and operationalized. Before introducing additional requirements, CalPrivacy should allow businesses adequate time to implement and stabilize compliance with existing rules. A measured, sequenced approach to regulatory development will ultimately serve both businesses and consumers better than continuous expansion.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of American innovation by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes more than 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

I. Notices and Disclosures

Privacy Policies (Questions 2-3)

- *What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?*

- *What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this issue?*

Privacy policies have become increasingly lengthy and complex as businesses work to satisfy the requirements of a growing number of state privacy laws, each with distinct terminology, defined terms, and disclosure obligations. Paradoxically, this accumulation of jurisdictionally specific requirements is undermining the very transparency these laws seek to achieve. Consumers are presented with dense, legally precise documents that satisfy technical compliance standards but fail to communicate effectively. The predictable result is information fatigue as consumers encounter long, unfamiliar text, disengage, and may click through without understanding the choices available to them.

TechNet believes the most important information for consumers is a clear, accessible explanation of what personal information is collected, how it is used, and what choices and rights the consumer has. Consumers are best served when this information is presented in plain language, with consistent terminology across jurisdictions, rather than through jurisdiction-specific legal disclosures that fragment the user experience.

A key challenge businesses face is the proliferation of divergent defined terms across state privacy frameworks. Core concepts such as what constitutes a "sale" of data, how "targeted advertising" is defined, and what categories of information qualify as "sensitive" vary across state laws, forcing businesses to either maintain separate, state-specific privacy policy sections or adopt imprecise umbrella language that satisfies no jurisdiction well. CalPrivacy can meaningfully address this challenge by prioritizing the alignment of its defined terms with the broader national landscape of state privacy laws. Harmonized terminology would produce clearer, more accessible privacy notices for consumers while reducing unnecessary compliance complexity for businesses.

Rather than mandating specific structural formats, prescribed text, or particular interface elements, CalPrivacy should articulate the intended outcome that consumers understand what data is collected, how it is used, and what rights they have, and allow businesses the flexibility to determine how best to achieve that outcome within their own platforms and services. Requirements that lock in particular layouts or language can quickly become outdated as technology and consumer expectations evolve and may actually impede the user-centered design innovations that produce real comprehension. CalPrivacy should also consider permitting alternative approaches such as layered or contextual notices that present the most relevant information at the point where it matters most to the consumer.

Notice of CPPA Rights (Questions 4-5)

- *What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights?*
- *What challenges do businesses face when providing notices, including opt-out links, across different devices or platforms? How can the regulations address this issue?*

The existing statute and CalPrivacy's current implementing regulations already contain robust notice provisions that adequately inform consumers of their CCPA rights, including requirements for privacy policies, notices at collection, and notices regarding the right to opt out of the sale and sharing of personal information. These requirements provide a comprehensive framework that, when properly implemented, gives consumers the information they need to understand and exercise their privacy rights.

TechNet urges CalPrivacy not to impose additional notice requirements that would layer further compliance obligations without corresponding consumer benefit. Additional prescriptive requirements risk compounding the information fatigue problem described above, producing more notices that consumers are less likely to read or understand. The goal should be making existing notices more effective, not adding new ones.

With respect to notice mechanisms across non-traditional interfaces, TechNet emphasizes the importance of affording businesses flexibility to offer contextually appropriate privacy notices based on the medium through which users interact with a service. Mobile apps, internet-connected devices, smartwatches, smart TVs, home appliances, gaming systems, smart speakers, home appliances, and other interfaces that lack traditional webpage-based displays present fundamentally different user experience constraints. A notice framework designed for a desktop web browser will not translate effectively to a smartwatch screen or a voice-activated home device. CalPrivacy should recognize these practical limitations and allow businesses to develop notice solutions tailored to the specific capabilities and user expectations of each platform, rather than prescribing uniform approaches that may be technically infeasible or counterproductive on certain devices. This is consistent with the principle that privacy regulations should be technology-neutral and should not mandate specific design choices.

Regulations can also adopt outcome-based standards that require providing consumers effective notice without mandating specific formats. CalPrivacy can ensure reasonable consumers understand what type of data is being collected and how to opt-out by endorsing alternative notice mechanisms rather than prescribing rigid disclosure formats that do not account for diverse consumer devices or device-specific mandates that quickly become outdated.

II. Employee Data

Employee Privacy Notices (Question 3)

- *What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?*

The existing rules already provide employees sufficient detail to understand and exercise their privacy rights in the employment context. The CCPA and CalPrivacy's implementing regulations require businesses to furnish employees and job applicants with a privacy policy, Notice at Collection, and notices regarding their privacy rights, covering the full range of information necessary for employees to understand how their personal information is collected, used, disclosed, and retained. TechNet urges CalPrivacy not to impose new requirements that would create compliance burdens without meaningfully enhancing employee protections.

The employment relationship involves the collection and processing of personal information for a wide range of legitimate purposes, including payroll, benefits administration, workplace safety, regulatory compliance, and performance management. Employees generally understand and expect this processing. The current framework adequately protects employee privacy while allowing employers to maintain necessary business operations. CalPrivacy should allow employers flexibility to determine the most effective methods and timing for delivering privacy notices across the employment lifecycle, rather than prescribing specific delivery mechanisms that may not account for the diversity of employer sizes, industries, and workforce structures.

Exercise of Employee Privacy Rights (Question 5)

- *What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights? How can the regulations address this issue?*

The current framework adequately protects employee privacy while allowing employers to maintain necessary business operations. Businesses have developed tailored processes for responding to employee rights requests that function well under the existing rules. These processes already provide employees sufficient detail to understand and exercise their privacy rights in the employment context, and imposing additional procedural requirements would create compliance burdens without meaningfully enhancing employee protections. Additional protections, such as rights like access and deletion, could also introduce unintended consequences that harm business's operations such as requesting the deletion of information related to an employment dispute.

Businesses already face challenges interpreting and applying existing employee data protections. For example, data access rights that allow employees to request

"all my personal information" scopes in a broad range of data, and disclosing certain categories including security and loss prevention records, investigation records, or proprietary workforce analytics can compromise business interests or harm others. This same principle applies to active investigations or lawsuits, as accessing or correcting data related to an active complaint, lawsuit, or investigation can compromise evidence and be abused to enable retaliation. We ask that CalPrivacy consider creating exemptions for employers that account for the operational realities and sensitivity of certain categories of employee data.

CalPrivacy should also account for the fact that employers are often required by law to collect and retain specific categories of employee information for defined periods, and that certain employee data may be subject to legal holds or regulatory retention requirements that constrain deletion or correction requests. Any future regulatory guidance should acknowledge these constraints and avoid creating conflicts with employers' obligations under other applicable federal and state laws.

Service Provider and Contractor Oversight (Question 6)

- *What steps do businesses take to oversee their service providers' and contractors' CCPA compliance, and what challenges do businesses face when doing so?*

Businesses employ a range of mechanisms to oversee their service providers' and contractors' privacy practices, including contractual requirements, due diligence questionnaires, compliance certifications, and, where appropriate, audits. The appropriate level and form of oversight varies significantly depending on the nature and sensitivity of the data being processed, the scope of the service provider relationship, and the overall risk profile of the engagement.

TechNet urges CalPrivacy not to mandate specific audit or testing requirements for service provider oversight. A one-size-fits-all approach to service provider oversight would impose significant costs, particularly on small and mid-sized businesses, without proportionate benefits. Mandated audits are resource-intensive, and the costs are ultimately borne by businesses and their customers. Moreover, rigid audit requirements can be counterproductive: they may incentivize checkbox compliance rather than meaningful risk assessment and may not account for the wide variation in service provider relationships across industries and business models.

Instead, CalPrivacy should allow businesses to retain flexibility in how they oversee service providers and contractors regarding privacy-related contractual commitments. A flexible, risk-based approach that allows businesses to tailor their oversight activities to their specific circumstances will prove more effective than prescriptive regulatory mandates. This is consistent with the broader principle that privacy regulations should be proportionate to the risks involved and should leverage existing industry standards, including the NIST Privacy Framework, rather

than creating new, California-specific requirements that add to the patchwork of obligations businesses must navigate.

Other Considerations (Question 7)

- *Question: What else should CalPrivacy consider regarding CCPA requirements for job applicants and workers in the employment lifecycle (hiring, working, and offboarding)?*

TechNet urges CalPrivacy to harmonize their obligations with other California employment laws. The CCPA/CPRA interacts with FEHA, Labor Code, CalWARN, and other statutes that include data obligations. CalPrivacy should ensure any regulations do not conflict with other requirements, such as allowing the deletion of data required for compliance elsewhere. This also includes rules around sensitive data, which employers must use for legitimate business purposes or to remain compliant with other state and federal laws.

Thank you for inviting our feedback. TechNet looks forward to continued engagement with CalPrivacy on these issues and stands ready to participate constructively in any formal rulemaking.

If you have any questions regarding our responses, please contact Robert Boykin at rboykin@technet.org or 408.898.7145.

Sincerely,

Robert Boykin
Executive Director for California and the Southwest
TechNet

Catbagan, Christian@CPPA

From: Kate Goodloe <Kateg@bsa.org>
Sent: Wednesday, May 20, 2026 8:48 AM
To: Regulations@CPPA
Subject: Preliminary Comment – Notices & Disclosures and Employee Data April 2026
Attachments: 2026.5.20 - BSA Comments on Employee Data - Final.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Attached, please find comments by the Business Software Alliance (BSA) on the treatment of employee data under the California Consumer Privacy Act (CCPA).

We appreciate CalPrivacy's focus on this issue and would welcome an opportunity to further discuss BSA's views.

Best,

Kate Goodloe

Kate Goodloe
Managing Director, Policy
Business Software Alliance

bsa.org
Sign up for BSA News | LinkedIn

May 20, 2026

Business Software Alliance
Comments on Employee Data Under CCPA

The Business Software Alliance (BSA) appreciates the opportunity to provide comments about how the California Consumer Privacy Act (CCPA) applies to employee data.

BSA is the leading advocate for the global software industry.[1] Our members create business-to-business technologies that power companies across every sector of the economy. BSA members offer tools including cloud storage, customer relationship management software, cybersecurity solutions, human resources management programs, identity management services, and collaboration software. Businesses entrust some of their most important information — including personal information — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security are a fundamental part of BSA members' operations.

Although BSA supports strong protections for consumer privacy, we remained concerned with California's unique approach of extending consumer-facing privacy protections to employees. Of the 22 states to enact comprehensive consumer privacy laws, California is the only state to treat employees as consumers — creating significant concerns for companies.

We appreciate CalPrivacy's focus on these issues and its recognition that regulations may provide important clarity to businesses and individuals about appropriate protections for employee data. We recognize that employees have legitimate privacy interests that are worthy of protection. At the same time, it is important to ensure that applying the CCPA's rights and obligations to employees does not inadvertently undermine the security or privacy of other individuals and ultimately aligns with other employee protections already in place in California.

Our comments focus on six issues:

- ***Rights to access and delete personal information***. The CCPA creates important rights, including for consumers to access and delete their personal information. But when employees exercise those rights, it creates both operational and privacy concerns — like employees that seek to delete performance evaluations or workplace investigations. *We strongly recommend that CalPrivacy recognize appropriate limits on these rights.*

- ***Right to limit processing of sensitive personal information***. Employers often need to process sensitive personal information of their employees, not only to provide payroll and administer benefits, but also in connection with securing an organization's internal operations and providing products and services to consumers. *More clarity is needed about honoring employees' requests to limit use of their sensitive personal information*.

- ***Applying data minimization requirements to employee data***. Under the CCPA, businesses are to limit their collection and use of personal information in line with data minimization obligations and limits on secondary uses. These obligations focus on using

[1] BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

personal information in line with "reasonable consumer expectations" — but it is not clear how that term applies in an employment context, particularly when data is often reused. For example, businesses may collect badge and location data for security purposes but also use it during subsequent investigations of security incidents. *More guidance is needed about how these standards apply to employees' information.*

- ***Ensuring risk assessments are not required for routine employment uses of sensitive personal information***. Businesses are required to conduct risk assessments under the CCPA for six types of processing, including processing of sensitive personal information. Although some employment-related processing is excepted, that exception is too narrow. *The regulations should be revised to ensure that routine employment-related processing of sensitive personal information does not require a risk assessment.*

- ***Promote consistency between application of CCPA regulations on automated decisionmaking technologies (ADMT) to employee data and other legal frameworks.*** The use of automated decisionmaking technologies is addressed not only by the CCPA regulations but also by regulations adopted by the California Civil Rights Council (CCRC) that took effect last October and by several proposed new legal frameworks under consideration by the California Legislature. *Regulations should promote consistency across legal frameworks and ensure that the CCPA regulations do not reach routine uses like assigning workflow tickets.*

- ***Ensure the right to opt out of sale does not reach standard employment disclosures***. Employers may need to disclose employees' personal data for a range of employment-related purposes, such as supporting legal compliance, and/or supporting workplace safety, security, or operations. *Sale should not include, for example, an employer's disclosure of personal information to an employee benefits provider that independently determines the means and purposes of processing for purposes of benefits administration*.

We detail these concerns below and would welcome an opportunity to further discuss them.

I. Consumer Rights to Access and Delete Personal Information

Consumers should have important rights over their personal information, including the rights to access, correct, delete, and port that information. California is the only state to extend these consumer-facing privacy rights to employees — creating a range of concerns.

Put simply: consumer privacy rights were not designed for employees. A business's relationship with its consumers is fundamentally different than its relationship with its employees. Employers must collect and use substantial amounts of personal information to administer employee payroll and benefits, manage performance, ensure workplace safety, and comply with legal obligations. As a result, employee requests to access, correct, and delete personal information often collide with employers' operational, legal, and risk-management responsibilities in ways that the CCPA does not adequately address.

Responding fully to an employee's request to access personal information, for example, may require disclosing sensitive information tied to internal investigations, security practices, trade secrets, or legally privileged communications, including attorney-client materials. At the same time, withholding or heavily redacting information is not only time and resource-intensive, but can also expose employers to claims that they have failed to comply with the law. Similarly, an employee's request to delete personal information could seek to erase core employment information, like negative performance reviews or complaints of misconduct.

CalPrivacy should expressly recognize appropriate limits on how the CCPA's privacy rights apply to employees. Although employers may rely on existing exceptions and legal

interpretations to limit the impact of some employee requests to access or delete their personal information, we strongly recommend that CalPrivacy formalize these exceptions to create clarity for both businesses and individuals.

1. Right to Access Personal Information Held by Employer

Consumers are given broad rights to access five types of information under the CCPA. Because this right extends to employees, an employee may require an employer to disclose:

- Categories of personal information the employer collects about that employee;
- Categories of sources from which that personal information is collected;
- Business or commercial purposes for collecting, selling, or sharing personal information;
- Categories of third parties to whom the employer discloses personal information; and
- Specific pieces of personal information the employer has collected about that employee.

The CCPA places few statutory limits on this right to access. Employers therefore face significant uncertainty about responding to an employee's request to access personal information — particularly when an employee seeks to access information that is confidential or that may affect the privacy or security of other employees.

For example, employees may submit an access request seeking:

- Documents on promotion, discipline, compensation, or other information in an employee's personnel file;
- Information about workplace harassment investigations;
- Information about *other* employees whose emails or documents refer to the employee; or
- Information about the employer's security measures and the specific types of data collected about the employee to safeguard data the employer maintains.

The CCPA did not account for requests to access this type of information because it was designed to provide important rights over the more limited information that a business maintains about its customers. Requiring employers to honor such requests creates bad incentives and undermines good data governance practices. For example, if employers must provide employees with access to internal investigations, it will undercut workplace safety protections. If employers must provide access to documents on promotion and compensation decisions, it creates incentives to avoid candid written feedback and documentation. The CCPA does not clearly intend those results.

The CCPA was intended to create important transparency about the data companies collect about their customers, to better protect their privacy. But employees are also using new privacy rights created by CCPA for purposes that are not related to privacy. For example, businesses routinely receive access requests from employees that function as pre-litigation discovery demands. This puts businesses in the difficult position of responding to requests for litigation-related information without the guardrails that attach to the discovery process — and without clear rules for handling confidential information or materials that are subject to attorney-client privilege or work product protection. This use of privacy rights for non-privacy purposes should be curtailed.

These uses of CCPA's privacy rights are particularly concerning because the California Legislature has already established a specific framework for workplace transparency. Labor Code Section 1198.5 provides employees the right to inspect personnel records while maintaining critical safeguards. It excludes investigative files, letters of reference, and, under Section 1198.5(n), explicitly stays the right to access once a lawsuit has been filed. Furthermore, with the recent implementation of SB 513 in January 2026, the Labor Code now explicitly covers performance-related education and training records. CalPrivacy should harmonize CCPA regulations with these existing statutes to ensure that privacy rights are not used in ways that undermine the existing judicial process.

Alignment across legal frameworks is important because companies should not be forced to navigate two disparate legal frameworks for the exact same set of documents. Under the current legal landscape, a request for a personnel file triggers the specific, balanced protections of Labor Code Sec. 1198.5, while a CCPA data request for that same file suggests a much broader, consumer-style disclosure. These duplicative requirements should be harmonized, to provide a clear and unified compliance standard for California businesses.

Recommendations. CalPrivacy should recognize appropriate limits on employees' rights to access personal information, including:

- **Recognizing that a business can decline an employee's request to access information** when the request seeks: (1) access to core employment documents including personnel files or internal investigations; (2) documents subject to attorney-client privilege or work product protections; and (3) documents that, if disclosed, would undermine the privacy and security protections of either the business, its employees, or its consumers.

- **Allowing employers to decline requests to access information** if they can demonstrate that the employee requesting access is abusing the right to access for purposes other than privacy protections.

- **Harmonizing CCPA requirements with established standards in Labor Code Sec. 1198.5.** California law already distinguishes employee data from consumer data. Labor Code Sec. 1198.5 sets out a right for employees to inspect and receive a copy of their personnel records. That right is balanced by specific, necessary exemptions for investigative files, letters of reference, and promotional exams. As this law was recently updated to cover training and performance records, it remains the primary authority for workplace transparency. Aligning the CCPA with these standards would avoid creating conflicting obligations for employers regarding the same categories of information.

- **Adopting a "reasonableness" standard for access.** Labor Code Sec. 1198.5 allows for employees to inspect and receive a copy of their personnel records at "reasonable intervals," whereas CCPA rights often lack such a qualification. We encourage CalPrivacy to adopt such a reasonableness standard under the CCPA.

- **Codifying a litigation exception.** Under Labor Code Sec. 1198.5(n), an employee's right to inspect personnel records ceases once they file a lawsuit related to a personnel matter. We encourage CalPrivacy to adopt a similar limitation on the CCPA rights, to ensure that the CCPA is not used to circumvent the established discovery process in civil litigation, as recognized by the Labor Code.

2. Right to Delete Personal Information Held By Employer

Consumers are also given the right to request that a business delete their personal information. Because this right extends to employees, an employee may require an employer to delete "any personal information" about the employee that the employer has collected from that employee. Similarly, a job applicant may require a business to delete "any personal information" about the applicant that the business collected, whether their application was successful or not.

The deletion right is subject to eight exceptions, which recognize that a business may decline to delete information if it is reasonably necessary for the business to maintain the personal information in order to:

- Complete "the transaction for which personal information was collected" or "provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the

context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer"';
- Help to ensure security and integrity;
- Debug to identify and repair errors that impair existing or intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act;
- Engage in certain research;
- Enable internal uses reasonably aligned with the expectations of the consumer; or
- Comply with a legal obligation.

Companies need more certainty about how both the right to delete and its exceptions apply to requests by employees to delete data their employer maintains.

For example, employees may submit a request to delete:
- Records relating to performance reviews or other aspects of an employee's personnel file;
- Complaints or investigations involving the employee, or that the employee made about other employees;
- Emails and other internal communications involving the employee;
- System logs and monitoring data about the employee; or
- Background check and hiring records.

These concerns also arise in the context of job applicants, which are similarly treated as consumers under the CCPA. Job applicants may submit a request to delete a company's entire record of their application, including the application, interview notes, scoring records and reasons for rejection (if unsuccessful). Businesses have a well-recognized need to retain this information for a reasonable and proportionate period, including for the protection of the business's legal interests. For example, applicants may bring discrimination claims related to the hiring process a year or more after an adverse action, and businesses must be able to retain applicant records for appropriately defined periods to demonstrate that hiring decisions were made on lawful grounds. The retention of applicant records by businesses should, moreover, be reasonably anticipated by applicants as part of the hiring transaction and in the context of the applicant-business relationship, as contemplated by Sec. 1798.105(d)(1).

Recommendations. CalPrivacy should recognize appropriate limits on employees' and job applicants' requests to delete personal information, including by:
- Specifically stating that requests to delete "employment records" may be rejected, instead of requiring employers to rely on broader exceptions to decline requests to delete core employment records like personnel files, performance records, disciplinary records, and compensation history.
- Providing examples of how the exception for "internal uses reasonably aligned with expectations" applies in the employment context.
- Adding a new exception clarifying that a company can decline a deletion request if deletion would impair the rights or records of others.
- Broadening the security exception, to clearly allow employers to reject a deletion request if it would adversely affect the security or privacy rights of the business or other consumers.
- Clarifying that retention of job applicant records falls within the exception for personal information "reasonably anticipated by the consumer within the context of" the hiring process and the relationship between an applicant and a prospective employer. Alternatively, CalPrivacy could add a new exception to the regulations permitting businesses to deny a deletion request and retain certain records when doing so is reasonably necessary for the establishment, exercise, or defense of legal claims.

II. Right to Limit Employers' Use of Sensitive Information

Consumers are given a right to limit the use and disclosure of their sensitive personal information. As a result, when an employee exercises this right, an employer must limit its use of sensitive information to:

- Uses "necessary to perform the services or provide the goods reasonably expected by an average [employee] who request those goods or services."
- Uses set out in the statute under Sec. 1798.140(e)(2), (4), (5), and (8), which allow for "security and integrity," "short-term, transient use" including nonpersonalized advertising, performing services on behalf of the business including customer service and fulfilling orders and transactions, and undertaking activities to maintain the quality or safety of a service or device that is owned or controlled by the business.
- Uses set out in regulations, which echo the statutory uses and also recognize that businesses can continue to use sensitive personal information "[t]o perform services on behalf of the business" among other additional uses.

More clarity is needed on the bounds of an employee's right to limit use of their sensitive personal information. Neither the CCPA nor the regulations implementing it address how this right applies across the full range of circumstances in which employers may need to collect and use employees' sensitive personal information. As a result, employers must often decide whether routine uses are "necessary" to perform services "reasonably expected" by an average employee. That uncertainty is unnecessary — and should be replaced by clear guidance that recognizes employers need to use sensitive personal information in a range of scenarios.

Employers must process the sensitive personal information of employees for a host of reasons — not only to administer payroll and benefits, but to prepare the business's tax documents, process expense requests, and maintain the security of both the business's network and its physical facilities. These activities also vary greatly across different types of businesses. For example, a small business bidding for government contracts may need to provide information about the diversity of their workforce and ownership. Companies that provide buses or other transportation services will collect copies of their employees' drivers license and use geolocation information in cars and buses to ensure they stop at assigned routes. If employees can opt out of having sensitive personal information used for such purposes, it will undercut the ability of companies to provide the goods and services their customers expect.

We appreciate that the CCPA regulations already recognize several circumstances in which employers can decline to honor an employee's request to limit processing of sensitive personal information. For example, the regulations clearly recognize that a business can collect biometric information of employees to authenticate their identity for access into secured areas of the business. The regulations also clearly state that businesses can scan employees outgoing emails to prevent employees from leaking sensitive personal information outside the business. However, more clarity is needed across the broader range of situations in which employers regularly process the sensitive personal information of employees.

Recommendation.

- CalPrivacy should recognize clear boundaries on employees' right to limit their use of sensitive personal information. Specifically, it should clearly state that employers may refuse such requests when processing the sensitive information of an employee is necessary to carry out routine or expected functions of the business.

III. Data Minimization

Under the CCPA, a business's "collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve" either the "purpose(s) for which the personal information was collected or processed" or another "disclosed purpose that is compatible with the context in which the personal information was collected."

Regulations set out factors for a business to assess in determining whether activities are consistent with reasonable consumer expectations, including the relationship between the consumer and the business and the type, nature, and amount of personal information to be collected or processed. However, none of these examples address employee data. Similarly, the regulations also address whether other disclosed purposes are compatible with the context in which information was collected, including the consumer's expectations, and whether the processing is for a business purpose under the CCPA. Again, however, the regulations do not address how these examples apply to employee data.

In the employment context, businesses will need to collect a variety of information from employees to both administer employment benefits and payroll and to ensure employees can perform their work-related duties. Employment data may also be reused for a range of employment-related purposes, such as performance data that can form the basis of promotion decisions and IT logs that are used to monitor safety incidents that can later be reused in misconduct investigations.

Recommendation.

- CalPrivacy should expressly recognize that businesses need to collect and reuse employee data to perform a range of expected functions.

IV. Risk Assessments

Data protection assessments are an important part of privacy compliance programs. BSA has supported a range of state and global privacy laws that require businesses to conduct data protection assessments of high-risk processing activities, which help companies identify and assess potential privacy risks and to adopt appropriate mitigation measures.

Under the CCPA, businesses are required to conduct risk assessments for six types of processing, including processing of sensitive personal information. Businesses must not only carry out these risk assessments, but an executive must submit information about those assessments to CalPrivacy under penalty of perjury.

Although the CCPA regulations create an exception that recognizes risk assessments are not required for certain employment-related processing of sensitive information, this exception is too narrow. That language should be expanded to exclude a wider variety of processing employee information conducted in the ordinary course of business operations. For example, an employer may need to process the contents of communications sent over its network to maintain the security of that network; it may also process biometric information to limit access to certain facilities to specific employees. Businesses should be encouraged to adopt these types of strong security-related practices, which help safeguard the personal information they hold. Requiring risk assessments of such activities undermines that goal, creating incentives for companies to adopt lesser security standards in ways that do not align with the CCPA's broader goals of improving both privacy and security practices for handling personal information.

The current language should be revised to expand this exception and ensure that risk assessments are not required for routine employment-related processing, including processing for security purposes, compliance activities, internal audits, and fraud detection. These standard employment uses of sensitive personal information should not require risk assessments.

Recommendation.

- Regulations on risk assessments should be revised to ensure that businesses are not required to conduct risk assessments when processing the sensitive personal information of employees for standard employment-related uses. Specifically, language should be added to Section 7151(b)(2)(A) to this effect. Alternatively, CalPrivacy should provide more clarity about when employee-related risk assessments are required and the content of those assessments.

V. Automated Decisionmaking Technology

Business will be required to provide new pre-use notices, opt out rights, access rights, and risk assessments relating to automated decision-making technology (ADMT) under the CCPA regulations. These obligations will be triggered when a business uses ADMT to make a "significant decision" about a consumer, which includes employees. The definition of significant decision contemplates several employee-related use cases, which should be further clarified, particularly around decisions allocating or assigning work for employees.

The use of automated decisionmaking technologies in the workplace is also addressed by a range of other existing and proposed laws and regulations. For example, the California Civil Rights Council (CCRC) recently underwent an extensive process to modify employment regulations around automated decision systems. Those regulations took effect on Oct. 1, 2025. The state legislature is also active on this issue, with bills in both the California Assembly (AB 1898) and California Senate (SB 947).

We strongly encourage CalPrivacy to ensure that the application of its ADMT regulations account both for existing legal frameworks like the CCRC regulations and for potential new legal frameworks that may be adopted by the California Legislature in coming years.

Recommendations.

- Clarify what "allocation or assignment of work for employees" means within the definition of "significant decision" under the ADMT regulations. This term should be applied to ensure that common administrative functions — like assigning workflow tickets — are not captured. CalPrivacy can avoid this by focusing this term on decisions that impact, for example, the substantive nature and scope of an employee's role.
- Ensure the application of ADMT regulations to employees aligns with existing California laws, including the Labor Code and the CCRC regulations. Over time, ensure the continued application of these regulations aligns with any new legal requirements adopted by the California Legislature. Without clear alignment, businesses may be subject to three or more different sets of rules on employment-related uses of automated tools in just one state.

VI. Limits on the Sale of Personal Information

We appreciate that the CCPA creates a right for consumers, including employees, to opt out of the sale of their personal information. However, we encourage CalPrivacy to clarify that standard disclosures of employees' personal information are not "sales" when their purpose is to administer the employment relationship.

Employers may need to disclose employees' personal information for a range of employment-related purposes, such as supporting legal compliance, and/or supporting workplace safety, security, or operations. Sale should not include, for example, an employer's disclosure of personal information to an employee benefits provider that independently determines the means and purposes of processing for purposes of benefits administration.

The CCPA already recognizes several exceptions to the definition of sale. We encourage CalPrivacy to ensure that these sorts of employment-related disclosures fall under the exception for disclosures made when a consumer uses or directs the business to internationally interact with one or more third parties, under Sec. 1798.140(ad)(2)(A).

Recommendation.

- Regulations on "sale" should be revised to clarify that the "intentional use or interactions" exclusions from the definition of "sale" covers third-party transfers of employee personal information by an employer where the primary purpose is administering the employment relationship, ensuring legal compliance and/or supporting workplace safety or operations, all fundamental parts of employment relationship.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to discuss these important issues.

___

For further information, please contact:

Kate Goodloe
Managing Director, Policy
kateg@bsa.org

Business Software Alliance

Catbagan, Christian@CPPA

From: Lewis, Dan (CORP) <dan.lewis@adp.com>
Sent: Wednesday, May 20, 2026 9:14 AM
To: Regulations@CPPA
Subject: NPRC Response to Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: NPRC Comments 05.20.26.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To Whom it May Concern:

I am writing on behalf of the National Payroll Reporting Consortium (NPRC) in my capacity as President.

NPRC appreciates the opportunity to provide preliminary input in response to the California Privacy Protection Agency's invitation for comments regarding notices, disclosures, and employee data under the California Consumer Privacy Act.

NPRC is a non-profit trade association which represents payroll processing service providers that serve roughly 48% of the U.S. workforce. NPRC members provide human capital management solutions. NPRC represents organizations that process workforce and payroll data on behalf of employer clients and therefore have a strong interest in clear, workable, and balanced regulatory requirements governing privacy notices, disclosures, and employee data. If you have any questions , please do not hesitate to contact me.

Best Regards,

Dan

Dan Lewis
VP, Compliance Programs & Government Affairs

One ADP Blvd, Roseland, NJ 07068
T: 973 974 5273

dan.lewis@adp.com

This message and any attachments are intended only for the use of the addressee and may contain information that is privileged and confidential. If the reader of the message is not the intended recipient or an authorized representative of the intended recipient, you are hereby notified that any dissemination

of this communication is strictly prohibited. If you have received this communication in error, notify the sender immediately by return email and delete the message and any attachments from your system.

Docusign Envelope ID: 6667D5FE-6EE9-8034-8266-BF303D5E6C0B

NPRC
National Payroll Reporting Consortium
PO Box 850 ★ Henrietta, NY 14467-0850 ★ www.NPRC-Inc.org

May 20, 2026

California Privacy Protection Agency
Legal Division – Regulations
400 R St., Suite 350
Sacramento, CA 95811

Re: Preliminary Comment - Notices & Disclosures and Employee Data April 2026

Dear Board Members,

On behalf of the National Payroll Reporting Consortium (NPRC), we appreciate the opportunity to provide preliminary input in response to the California Privacy Protection Agency's (CalPrivacy) invitation for comments regarding notices, disclosures, and employee data under the California Consumer Privacy Act (CPPA).

NPRC is a non-profit trade association which represents payroll processing service providers that serve roughly 48% of the U.S. workforce. NPRC members provide human capital management (HCM) solutions, NPRC represents organizations that process workforce and payroll data on behalf of employer clients and therefore have a strong interest in clear, workable, and balanced regulatory requirements governing privacy notices, disclosures, and employee data.

In particular, NPRC encourages CalPrivacy to:

- Promote concise, user-friendly privacy notices focused on key information;
- Provide flexibility in how notices are delivered across platforms and devices;
- Support structured and efficient mechanisms for submitting consumer requests; and
- Maintain clear allocation of responsibilities between businesses and service providers, particularly in the employment context.

I. Notices and Disclosures

NPRC encourages CalPrivacy to prioritize clarity, usability, and proportionality in any updates to privacy notice requirements. As a general matter, there is an inherent tension between providing comprehensive disclosures and ensuring that those disclosures are understandable and useful to consumers. Businesses are incentivized to include extensive detail to mitigate compliance risk, but this often results in lengthy notices that may unintentionally obscure the most important information for consumers.

Regulatory approaches that strike an appropriate balance would benefit both consumers and businesses by:

- Providing greater certainty as to what constitutes sufficient disclosure; and
- Promoting more concise, intelligible notices enables consumers to meaningfully understand their rights and choices.

Docusign Envelope ID: 6667D5FE-6EE9-8034-8266-BF303D5E6C0B

This balance is particularly important in environments with limited display space, such as mobile applications, connected devices, and other non-traditional interfaces.

From NPRC's perspective, the most important information for consumers can be effectively conveyed by focusing on:

- Categories of personal information collected (rather than exhaustive data element-level detail);
- The purposes for which the information is used;
- The categories or types of recipients with whom information is shared (rather than static, comprehensive lists that can quickly become outdated); and
- Clear, accessible explanations of how consumers can exercise their privacy rights.

With respect to exercising rights, businesses benefit from mechanisms that facilitate complete and well-structured requests at the outset. In practice, webform-based submission tools are often the most effective approach because they allow businesses to collect the information necessary to authenticate and process requests efficiently. By contrast, unstructured intake channels such as email frequently result in incomplete submissions, duplicative communications, and significant operational burden, including the need to triage unrelated inquiries or spam. Regulations that recognize and support structured intake methods would improve both consumer experience and compliance outcomes.

II. Employee and Applicant Data

NPRC appreciates CalPrivacy's effort to examine how notice and rights obligations operate in the employment context. Workforce data raises distinct considerations given the volume, sensitivity, and operational necessity of data processing in the employment lifecycle.

With respect to notice, NPRC's experience suggests that businesses are generally able to provide employee notices at appropriate points in the lifecycle, such as during onboarding, and to incorporate privacy disclosures into existing HR processes. For job applicants, notices are often provided through application platforms or career portals, and in some cases in coordination with employer clients. Flexibility in how and where these notices are delivered remains important to accommodate differing recruiting models and technologies.

Regarding the exercise of rights, employers and their service providers share an interest in ensuring that requests are directed to, and managed by, the appropriate entity. NPRC notes the importance of maintaining clear lines of responsibility between businesses (employers) and service providers acting on their behalf. Requirements that could be interpreted as shifting responsibility for responding to employee or applicant requests from the business to service providers could create confusion, operational inefficiencies, and inconsistent outcomes for individuals.

This issue is particularly relevant in the applicant context, where individuals may submit applications to multiple employers using shared platforms or service providers. While individuals may seek a centralized mechanism for managing their data across multiple employers, imposing such an obligation on service providers would be complex and could conflict with the principle that the business retains responsibility for responding to employee rights requests related to its

own data processing activities.

III. Oversight of Service Providers

As a general matter, NPRC members are subject to significant oversight by their employer clients with respect to privacy and security practices. Service providers routinely:

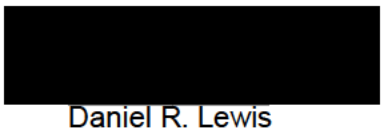
- Provide detailed information regarding their data handling, privacy, and security controls;
- Undergo due diligence reviews by clients and prospective clients; and
- Support audit rights or other verification mechanisms.

These existing accountability structures provide meaningful oversight of service provider compliance and should be considered when considering whether additional regulatory requirements are necessary.

IV. Conclusion

NPRC appreciates CalPrivacy's efforts to evaluate the effectiveness of existing CCPA regulations surrounding notices, disclosures, and employee data and to ensure that related requirements are clear, practical, and appropriately tailored. We appreciate the opportunity to provide input and would welcome further engagement as the Agency continues its work. If we can provide any additional information, please do not hesitate to contact me at 973.974.5273.

Sincerely,



Daniel R. Lewis
President
National Payroll Reporting Consortium

Catbagan, Christian@CPPA

From: Mayu Tobin-Miyaji <tobin-miyaji@epic.org>
Sent: Wednesday, May 20, 2026 11:28 AM
To: Regulations@CPPA
Cc: Sara Geoghegan
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: EPIC 05-20-26 Privacy Notices Comments.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

On behalf of the Electronic Privacy Information Center, please find attached comments in response to the agency's invitation for preliminary comments on Notices & Disclosures and Employee Data.

Best,

Mayu Tobin-Miyaji (she/her)
Law Fellow
Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

California Privacy Protection Agency

on

Invitation for Preliminary Comments

Notices & Disclosures and Employee Data

May 20, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the invitation of the California Privacy Protection Agency ("Agency" or "CalPrivacy") for preliminary comment on notices, disclosures, and employee data, published on April 20, 2026.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has previously provided comments on the California Consumer Privacy Act (CCPA),[3] published a detailed analysis of the California Privacy Rights Act before its approval by

---

[1] Invitation for Preliminary Comments: Notices & Disclosures and Employee Data, Cal. Privacy Protection Agency (Apr. 20, 2026), https://cppa.ca.gov/regulations/pdf/notices_disclosures_employee_data.pdf.
[2] *About Us*, EPIC, https://epic.org/about/ (2025).
[3] Comments of the Electronic Privacy Information Center (EPIC) and the Consumer Federation of America (CFA) in Response to the California Privacy Protection Agency's Proposed Rulemaking Regarding Cybersecurity, Risk Assessments, and Automated Decisionmaking Technology (Feb. 19, 2025), https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/; Comments of Consumer Reports, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) and Privacy Rights Clearinghouse (PRC) In Response to the California Privacy Protection Agency's Invitation for Preliminary Comments On Proposed Rulemaking Under Senate Bill 362 (June 25, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/06/Comments-of-Consumer-Reports-In-Response-to-the-California-Privacy-Protection-Agencys-Invitation-for-Preliminary-Comments-On-Proposed-Rulemaking-Under-Senate-Bill-362.pdf; Comments Of The Electronic Privacy Information Center, Center For Digital Democracy, and Consumer Federation Of America, to the California Privacy Protection Agency (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/; Comments of EPIC to Cal. Privacy Prot. Agency (Nov. 20, 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-CPPA-Comments-Nov-20.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Aug. 23, 2022), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Nov. 8, 2021), https://epic.org/wp-content/uploads/2021/11/PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf; Comments of

California voters,[4] and presented oral testimony to the Agency to encourage the strongest protections for Californians.[5]

The CCPA established important rights for Californians to know, correct, delete, and opt out of sale of information, and includes strong data minimization requirements to protect Californians from harmful overcollection of personal information, out-of-context impermissible secondary data uses, and excessive data retention.[6] Because privacy policies and disclosures are the primary means for data subjects and the public to understand the practices of the covered entities, they should be as clear as possible and directly tied to actionable steps for Californians to exercise their rights under the CCPA. EPIC asks the Agency to consider the following suggestions to that end:

- Privacy policies should be easily accessible and consolidated in one easy-to-find link rather than spread out across many documents through multiple links;
- Covered entities should provide all published versions of privacy policies, with their effective dates, in an easily accessible manner; and
- Policies and disclosures should directly link to where individuals can exercise their rights under the CCPA, and these regulations should prohibit dark patterns.

These recommendations should apply to privacy policies and disclosures for consumers and workers alike, and EPIC also echoes the comments submitted by the Berkeley Labor Center on worker privacy.

Privacy policies should be accessible and should not span a web of documents. As a recent Stanford study on the privacy policies of six frontier AI model developers has found, all of the developers rely upon a web of documents in addition to their primary privacy policies to govern their

---

EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf.

[4] EPIC, California's Proposition 24 (2020), https://epic.org/californias-proposition-24/.

[5] EPIC Calls Out CPPA as Board Votes to Adopt Weak Risk Assessment, ADMT, and Cybersecurity Regulations, EPIC (July 24, 2025), https://epic.org/cppa-votes-to-adopt-weak-cybersecurity-risk-assessments-and-admt-regulations/.

[6] EPIC, *Data Minimization*, https://epic.org/issues/consumer-privacy/data-minimization/; EPIC, *California Consumer Privacy Act (CCPA)*, https://epic.org/california-consumer-privacy-act-ccpa/.

use of users' chat data, with OpenAI relying on at least six different policies.[7] Finding, reading, and synthesizing six different privacy policies is untenable for an ordinary person and undermines Californians' ability to effectively exercise their rights under the CCPA. Some of these policies also have ambiguous language that states that the entity "may" use data collected across other products owned by the umbrella company to train AI models,[8] which clouds transparency around which data categories from which products are used this way. These sorts of sprawling webs of difficult-to-parse privacy policies and disclosures are common across many companies, and CalPrivacy should consider adopting regulations that would prohibit these practices.

Multiple privacy policies and disclosures can also lead to overlapping and conflicting messages about the company's policies and the data subject's rights. For example, in *Calhoun v. Google*, Google argued that an individual's "agreement" to their Privacy Policy and Google Account Holder agreements meant that they had consented to all potential data collection described not only in the policies and agreements, but also in any other linked disclosures, FAQs, and other documents.[9] Google contended that even when it has explicitly promised its users that it will protect their data, it didn't have to abide by that promise so long as it points to contrary terms in its general user agreement and statements posted in a sprawling web of disclosure pages.[10] Google's arguments did not succeed in the Ninth Circuit because when the disclosures are read together, "a reasonable user would not necessarily understand that they were consenting to the data collection at issue."[11] Overlapping and conflicting policies thus increase the burden on individuals attempting to understand the data practices of the entity and undermine their privacy rights by potentially misleading them. The Agency should develop regulations that place the burden on the covered entity to ensure its policies and disclosures are internally coherent and kept to a minimum number of

---

[7] Jennifer King, Kevin Klyman, Emily Capstick, Tiffany Saade and Victoria Hsieh, *User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies*, arXiv (Sept. 5, 2025), https://arxiv.org/abs/2509.05382.
[8] *Id*.
[9] Brief for the Elec. Priv. Information Ctr. as Amicus Curiae in Support of Plaintiffs-Appellants and Reversal, Calhoun v. Google, _ F.4th _, 2024 WL 3869446 (9th Cir. 2024) (No. 22-16993).
[10] *Id.*
[11] *Id*.

documents and that there is accountability if covered entities publish conflicting or deceptive policies.

Another aspect of privacy policies and disclosures that make them untenable for data subjects and the public to understand is their ever-changing nature. As a recent whitepaper by EPIC Counsel Caroline Kraczon and EPIC Scholar in Residence Justin Sherman on manipulative design elements in consumer opt-out processes points out, researching privacy policies is difficult in part because privacy policies are difficult to archive, and are often replaced by new versions.[12] There is often no clear way to compare prior versions of privacy policies and disclosures. The Agency should consider rules that require covered entities to post accessible links to previous versions of privacy policies and other disclosures with dates when the policies were in effect and changes noted so that consumers can easily decipher the new terms.[13]

Lastly, privacy policies and disclosures should provide actionable steps to Californians. Regulations on privacy policies and disclosures should require direct links to where individuals can exercise their rights under the CCPA, and they should prohibit manipulative design practices. As EPIC's whitepaper points out, some websites also offered no clear way to exercise opt-out rights.[14] Further, many of the companies surveyed exhibited some evidence of manipulative design in the opt-out process, including confusing or contradictory language.[15] Regulations should address confusing or misleading language in policies and disclosures, such as those that suggest key functionalities will not be available or that exercising their rights would be futile.[16] Requiring direct

---

[12] Caroline Kraczon & Justin Sherman, EPIC, *Good Luck Opting Out: Manipulative Design Patterns in Opt-Out Processes* 26–27 (May 2026), https://epic.org/wp-content/uploads/2026/05/Good-Luck-Opting-Out-Manipulative-Design-Patterns-in-Opt-Out-Processes.pdf.
[13] For example, see EPIC's privacy policy for its own website. *Updates to EPIC's privacy policy posted on July 26*, 2024, EPIC (July 26, 2024), https://epic.org/wp-content/uploads/2024/07/EPIC-changes-to-privacy-policy.pdf.
[14] Kraczon & Sherman, *supra* note 12, at 27–28, 35-36.
[15] *Id*. at 30–33. *See also* EPIC, Comments to the Colo. Dept. of Law on Proposed Rulemaking Under the Colorado Privacy Act of 2021 (Aug. 5, 2022), https://epic.org/documents/epic-comments-on-colorado-privacy-act-rulemaking/.
[16] Kraczon & Sherman, *supra* note 12, at 30–33.

links in privacy policies and disclosures would be a straightforward way to lessen the burden on Californians who are trying to exercise their CCPA rights.

When Californians encounter hard-to-understand privacy policies and friction while trying to exercise their privacy rights, the important work that California has done to enshrine privacy rights into law is undermined. We hope that EPIC's whitepaper aids CalPrivacy in its efforts to ensure that Californians can exercise their privacy rights. We thank CalPrivacy for the opportunity to provide preliminary comment on this topic, and we look forward to working with the Agency in the future to continue protecting the privacy of all Californians.

Respectfully Submitted,

/s/ Mayu Tobin-Miyaji
Mayu Tobin-Miyaji
EPIC Law Fellow
tobin-miyaji@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

Catbagan, Christian@CPPA

From: Lindsey Stewart <lindsey.stewart@zoominfo.com>
Sent: Wednesday, May 20, 2026 2:08 PM
To: Regulations@CPPA
Cc: Bubba Nunnery
Subject: Preliminary Comment – Notices & Disclosures and Employee Data April 2026
Attachments: ZI CPPA Comments 5.20.26.docx.pdf

This Message Is From an External Sender
WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Good afternoon -

Thank you for the opportunity to submit comments regarding Notice & Disclosure and Employee Data. ZoomInfo's comments are attached. Please don't hesitate to reach out if you have any questions.

Take care -

Lindsey

--
Lindsey Stewart, CIPP/US
Senior Director, Government and Regulatory Affairs
M: [redacted]
E: lindsey.stewart@zoominfo.com

zoominfo

330 W Columbia Way, Floor 8
Vancouver, WA 98660

866.904.9666
zoominfo.com

May 20, 2026

California Privacy Protection Agency
400 R Street, Suite
350 Sacramento, CA 95811

Dear California Privacy Protection Agency,

ZoomInfo is a software and data company that provides information for business-to-business (B2B) sales, recruiting, and marketing. We appreciate the opportunity to submit preliminary comments on the Agency's questions regarding notices and disclosures and employee data, and offer the following recommendations with the goal of building a framework that is both rigorous in protecting consumers and workable in practice.

I. Notices and Disclosures

Question I.2: What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?

One significant source of confusion in privacy policies today is a direct product of the current regulations themselves. The regulations require businesses to describe the categories of personal information they collect using the specific terms set forth in the CCPA's definition of personal information. These are legal terms of art, such as "Internet or other electronic network activity information" and "characteristics of protected classifications under California or federal law," that do not reflect how consumers think about their personal information. The related requirement that businesses identify, for each such statutory category, the third parties to whom information was sold, shared, or disclosed compounds the problem. In practice, these per-category requirements produce dense, repetitive tables in which substantially the same purposes and recipients appear in nearly every row. The result is a privacy policy that is technically complete but functionally uninformative.

CalPrivacy should amend the regulations to allow businesses to describe the personal information they collect in plain, descriptive language that provides consumers a meaningful understanding of the information at issue, rather than mandating use of the statutory enumeration. Similarly, CalPrivacy should allow businesses to disclose purposes, third-party recipients, and retention periods at the level of granularity that most clearly and accurately conveys the business's actual practices, whether organized by data category, by functional context, or at a general level. A privacy policy that explains in straightforward terms what data a business collects, why it collects it, and who receives it will consistently produce a more readable and more

understandable disclosure than a statutory-category matrix. This approach would better align the privacy policy requirements with the regulations' existing mandate that disclosures be "easy to read and understandable to consumers" and would advance the stated purpose of the privacy policy: to provide consumers with a comprehensive and comprehensible description of a business's information practices.

Question II.5: What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights? How can the regulations address this issue?

Before addressing the substance of employee data, ZoomInfo respectfully flags a threshold definitional issue it believes is important context for this rulemaking. The CCPA distinguishes between data sets related to professional context, including business-to-business communications (§ 1798.145(n)(1)) and employment-related contexts (§ 1798.145(m)(1)). These sections are not equivalent.

One covers potentially sensitive employment records — benefits, emergency contacts, and HR files. The other covers professional contact information which is essential to B2B commerce — business email, title, and phone number. This data enables businesses to identify, reach, and transact with one another, and is critical to how commercial markets function.

Regulations designed to protect workers and their data rights should be tailored to the actual risk profile of the data in question. Applying uniform regulatory treatment to data with such different risk profiles and use cases risks over-regulating low-risk, critical commerce data while diverting compliance resources from higher-risk employee data.

Conflict with Federal Law

One of the most significant challenges businesses face when responding to employee rights requests is the direct conflict between CCPA deletion rights and mandatory federal retention obligations. The statute recognizes this conflict — Civil Code § 1798.105(d)(8) exempts retention necessary to "comply with a legal obligation," and Civil Code § 1798.145(a)(1) broadly preserves a business's ability to comply with federal law — but neither the statute nor the regulations provide any practical guidance on how to communicate this to employees.

Cal. Code Regs., tit. 11, § 7022(f)(1) requires businesses to provide a "detailed explanation of the basis for the denial, including any conflict with federal or state law," but offers no standardized language and no guidance on what level of detail satisfies that requirement. The result is inconsistent responses across businesses and unnecessary confusion for employees whose requests are lawfully denied.

CalPrivacy should address this gap by developing standardized response guidance — and ideally model response language — for common scenarios where deletion requests conflict with federal retention obligations, including payroll records under the FLSA, I-9 records under USCIS requirements, and benefits records under ERISA.

Employee Access Requests

A related and significant challenge is the operational burden of responding to employee access requests. In practice, current and former employees rarely limit the scope of their requests to the specific personal information they are seeking. Instead, most submit broad, undifferentiated requests for all personal information the business holds about them. Because employees generate personal information across every system they touch during the course of their employment, responding to these requests requires businesses to search and review potentially hundreds of thousands of internal communications, including emails, instant messages, shared documents, and collaboration platform records, as well as the numerous business applications that employees use or that are used in connection with their employment. The review burden is compounded by the fact that these communications and records frequently contain the personal information of other employees, customers, or third parties, requiring careful redaction before production.

ZoomInfo fully supports the right of employees to understand what personal information their employer holds about them. That right, however, must be balanced against the operational reality of responding to requests that are untethered to any specific informational need. In many cases, the breadth and timing of these requests indicate that the current or former employee is using the CCPA access right as an informal pre-litigation discovery mechanism rather than as a tool for understanding what personal information the business holds. The result is a compliance obligation that is fundamentally different in scale and purpose from a typical consumer access request, and one that the current regulations do not account for. Without reasonable guardrails on scope, the access right risks becoming a tool that imposes disproportionate costs on businesses while producing voluminous disclosures that do not meaningfully advance the employee's understanding of their personal information.

CalPrivacy should address this gap by allowing businesses to require employees to reasonably specify the categories of personal information or the systems and time periods relevant to their request before the business is obligated to conduct a full-scope review. CalPrivacy should also consider establishing distinct processing timelines for employment-related access requests that reflect the volume and complexity involved, and should provide guidance clarifying that the CCPA access right is not intended to serve as a substitute for formal litigation discovery.

Thank you for your consideration. Please feel free to contact me if you have any questions.

Sincerely,

Bubba Nunnery
Vice-President, Government and Regulatory Affairs
ZoomInfo
bubba.nunnery@zoominfo.com

Catbagan, Christian@CPPA

From: Leder, Leslie <leslie.leder@calchamber.com> on behalf of Daylami, Ronak <ronak.daylami@calchamber.com>
Sent: Wednesday, May 20, 2026 2:30 PM
To: Regulations@CPPA
Subject: "Preliminary Comment – Notices & Disclosures and Employee Data April 2026"
Attachments: CalChamber Preliminary Comment Notices Disclosures and Employee Data FINAL 5.20.26.pdf

Importance: High

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To whom it may concern:

Please see comments from the California Chamber of Commerce in response to the Agency's invitation for preliminary comment Notices & Disclosures and Employee Data April 2026, attached.

Best,

Ronak Daylami

Ronak Daylami
Vice President for Advocacy | Privacy, Cybersecurity & Emerging Technologies

CalChamber.
HR Expert & Business Advocate™

California Chamber of Commerce
1215 K Street, 14th Floor
Sacramento, CA 95814
C: [redacted]

Visit calchamber.com for the latest California business legislative news plus products and services to help you do business.

This email and any attachments may contain material that is confidential, privileged and for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient or have reason to believe you are not the intended recipient, please reply to advise the sender of the error and delete the message, attachments and all copies.

CalChamber

May 20, 2026

California Privacy Protection Agency
Attn: Legal Division – Regulations
400 R St., Suite 350
Sacramento, CA 95811

Submitted electronically to: regulations@cppa.ca.gov

SUBJECT: "Preliminary Comment – Notices & Disclosures and Employee Data April 2026"

The California Chamber of Commerce (CalChamber)[1] appreciates the opportunity to comment on the California Privacy Protection Agency's (CalPrivacy) invitation for preliminary comments on Notices and Disclosures and Employee data.

As a general matter, CalChamber supports establishing effective notice and privacy protections that have sufficient flexibility to meet the needs of varying business sizes and industries across California, without creating unnecessary duplication with other laws. That said, CalChamber would respectfully urge CalPrivacy to refrain from initiating new rulemakings at this time. Businesses are currently devoting considerable financial and operational resources to achieving compliance with the most recent set of regulatory updates. The compliance burden is substantial, and organizations need adequate time to implement existing requirements before being asked to adapt to additional changes. Introducing new rules prematurely would strain these efforts, potentially undermining the effectiveness of the current regulatory framework. A measured approach that allows for full implementation of existing rules will ultimately serve both businesses and consumers better than continuous regulatory expansion. That said, we offer the following comments on these two rulemaking processes for your consideration.

I. Notices & Disclosures

1. When reviewing a privacy policy or similar disclosure, what is the most important information to consumers? What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?

The most important information to consumers is likely not additional narrative detail, but disclosures that are easy to find, understand, and compare across businesses. Research suggests that standardized, layered, and concise disclosures improve consumer comprehension more effectively than lengthy or highly legalistic privacy policies. CalPrivacy should therefore prioritize usability, consistency, and implementation flexibility rather than imposing increasingly prescriptive disclosure mandates.[2]

However, before mandating additional changes to notice content, CalPrivacy should allow time to assess the impact of the significant revisions businesses have already made in response to the Agency's recently finalized regulations addressing cybersecurity audits, risk assessments, automated decisionmaking technology, insurance, and related updates to existing CalPrivacy rules (ADMT Regulations). Those regulations took effect only five months ago with phased

[1] CalChamber represents a broad and diverse cross-section of California employers, including many of the covered entities that would be directly affected by the proposed rule package.
[2] Online privacy notices: What works and doesn't, March 2, 2022.

1215 K Street, Suite 1400
Sacramento, CA 95814
916 444 6670
www.calchamber.com

compliance obligations. A more evidence-based approach grounded in further study and consumer surveys after implementation of those changes would better inform whether additional disclosure mandates are necessary and what information consumers still meaningfully lack, if any.

2. What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?

The existing statute and current regulations already contain robust and comprehensive notice provisions that adequately inform consumers of their privacy rights. Consumers are made aware of their rights through multiple channels under the current framework, and these existing mechanisms have proven effective. As a general matter, CalChamber recommends that CalPrivacy take an evidence-based approach to evaluating this issue before making further changes to its regulations.

That said, companies generally have a single privacy notice for all US consumers—which provides a single, clear, and consistent experience for readers. To the extent a statute or regulation mandates state-specific language, those cumulative provisions will increase length and create confusion to the extent they require framing the same point using different formulaic language. We recommend that any proposed rules clarify that businesses do not have an obligation to refer to state-specific rights so long as the notice does not confuse or mislead the California consumer to believe that a right does not apply to them when, in fact, it does.

3. What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this issue?

Privacy policies have become increasingly lengthy in order to satisfy the myriad requirements imposed by various state privacy laws, and consumers may be disinclined to read them in their entirety. This proliferation of disclosures can paradoxically undermine the very transparency that privacy laws, such as the California Consumer Privacy Act (CCPA), seek to achieve. When requiring privacy policy disclosures, CalPrivacy should carefully consider the level of detail that is truly necessary and beneficial for consumers. Rather than adding to this complexity, state regulators should be encouraged to align requirements with existing laws to create a more coherent regulatory landscape. Unique state requirements result in cumbersome, fragmented layouts that do not ultimately benefit consumers. Instead, they create confusion and information overload. Furthermore, definitions of key terms vary significantly across state privacy regimes, sometimes in materially different ways that create genuine compliance challenges. These definitional inconsistencies inevitably result in longer, more cumbersome disclosures as businesses attempt to address each jurisdiction's specific terminology. We strongly urge CalPrivacy, along with all state regulators, to prioritize the alignment of defined terms. Harmonization would reduce unnecessary complexity and produce clearer, more accessible privacy notices that genuinely serve consumer interests.

Businesses also face significant challenges in describing complex and evolving data practices in concise, consumer-friendly language while also maintaining legal accuracy across multiple products, jurisdictions, and operational contexts.[3] As such, it can be difficult to determine the appropriate level of detail for describing data elements and processing purposes in a way that is both accurate and understandable to consumers.

---

[3] See, CalChamber's February 18, 2025 comment's to CalPrivacy's ADMT Regulations discussing the significant operational costs and burdens with compliance.

Another challenge is ambiguity and confusion caused by regulations. For example, broad or novel definitions created through regulation, alongside statutory definitions, create uncertainty about what must be disclosed and how disclosures should be made. Additionally, conflicting frameworks across states and internationally, including different terminology, rights, and disclosures are confusing to customers.

If CalPrivacy intends to impose additional disclosure requirements, it should include examples in the regulations that businesses can use as models. We also recommend that the rules clarify that companies are encouraged to use customer-friendly, easy to understand, and simplified text in their privacy notices, so long as the text used reasonably describes and addresses the disclosure topics required to be in the privacy notice.

4. What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights?

For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?

Effective notice mechanisms are those that provide consumers with timely, contextual, and accessible information in a manner appropriate to the device or interface being used, rather than rigidly tied to a single format. Because different technologies support different user experiences and technical capabilities, regulations must preserve flexibility for businesses to tailor notice mechanisms to the practical limitations and functionality of specific devices and platforms. Privacy-protective practices that build consumer trust require notice mechanisms that are genuinely accessible and understandable — not merely technically compliant.

We recommend that any proposed regulations accommodate the limitations or peculiar characteristics of various interfaces. For example, layered notice is particularly essential for non-traditional interfaces. This can involve short, contextual summaries at the point of interaction, with easy access to comprehensive disclosures through companion apps, web portals, or QR codes. Additionally, the standard for notice should be whether consumers actually receive and understand their rights rather than whether the notice takes a specific form. A well-designed voice prompt on a smart speaker may be more effective than a dense webpage that no one reads. For devices with limited or no screens, clearly and prominently directing consumers to a companion app or web portal should satisfy notice requirements.

We also recommend avoiding overly prescriptive format mandates, which disadvantage entire categories of devices and the consumers that use them. Companies investing in creative, user-friendly notice mechanisms (for instance, icons, dashboards, and contextual prompts) should be encouraged, not penalized for deviating from a rigid template. Additionally, notice mechanisms should account for consumers with disabilities, such as voice-based notices for visually impaired users and visual notices for hearing-impaired users.

Additionally, CalPrivacy should consider businesses' different compliance obligations across multiple jurisdictions.[4]

---

[4] March 27, 2025, Reuter's article titled "The privacy tug-of-war: States grappling with divergent consent standards" has a table showing differing compliance obligations across 16 states. This is just one example of what businesses must resolve as additional rules are set.

5. What challenges do businesses face when providing notices, including opt-out links, across different devices or platforms? How can the regulations address this issue?

As previously noted, CalChamber provided substantial feedback on these issues in its comments on CalPrivacy's ADMT regulations. CalPrivacy should revisit those comments, particularly the discussion of issues the ADMT Regulations' Standardized Regulatory Impact Assessment did not evaluate when assessing compliance costs to industry.

Businesses face substantial operational and technical challenges in providing uniform notices and opt-out mechanisms across the wide variety of modern devices, interfaces, and platforms used by consumers. Many devices, including smartwatches, connected appliances, and gaming systems, have limited, or no, screen size (or user interface) and input capabilities, which constrain how notices and links, such as the "Do Not Sell or Share My Personal Information" link, can be displayed. Smartwatches and wearables have screens too small to display meaningful privacy notices or clickable opt-out links without degrading the user experience; and smart TVs and gaming consoles use remote-control navigation, making hyperlink-based interactions cumbersome and fundamentally different from web browsing.

Attempting to impose uniform notice requirements across fundamentally different device types would be impractical. Accordingly, notice requirements should reflect this technological reality and afford businesses appropriate flexibility in how they provide notice, particularly when the device in question does not contain a traditional user interface. A flexible, outcomes-based approach to notice, rather than rigid prescriptive requirements, would better serve consumer protection goals while accommodating the diverse and evolving landscape of connected devices.

Regulations could also address these challenges by adopting an outcome-based standard, requiring that consumers receive effective notice and have accessible means to exercise their rights without mandating a specific format. The test should be: can a reasonable consumer using this device understand what data is collected and how to opt out? Regulations can explicitly endorse some of the alternative notice mechanisms (for example, layered notice, QR codes, and voice-based notice and opt-outs), while allowing flexibility for innovations and other notice mechanisms. Additionally, avoiding device-specific mandates will avoid outcomes where prescriptive rules tied to specific device categories become quickly outdated as technology evolves.

Ultimately, regulations should support, rather than burden, business efforts that generally effectuate notice to customers with different types of devices, even if not all notice mechanisms perfectly mirror the webpage model.

6. Please provide examples of effective consumer notices and disclosures. If possible, please provide information about specific testing, studies, or data demonstrating their effectiveness.

7. What else should CalPrivacy consider regarding CCPA notice and disclosure requirements?

Some state regulators have suggested that their residents will not know that specific privacy notice text will apply to them unless the disclosure is labeled with the state name. This is the wrong mental model. Privacy notice text should be read to apply unless labeled as for residents of a particular jurisdiction.

II. Employee Data

1. What are your expectations or concerns regarding why businesses collect, use, disclose, or retain your personal information as a job applicant or employee?

2. Have you received a copy of a business's privacy policy, Notice at Collection, or CCPA rights' notices as a job applicant or employee?

a. Identify each notice you have received and describe your experience receiving the notice.

For example, how did you receive the notice(s), at what point in the employment life cycle (hiring, working, offboarding) did you receive the notice(s), and what was the most helpful information in the notices.

b. Do you have any suggestions on how to improve the effectiveness of the notice?

3. What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?

The existing rules already provide employees with a sufficient level of detail to understand and effectively exercise their privacy rights in the employment context. These provisions strike an appropriate balance between transparency and practicality, recognizing the unique nature of the employer-employee relationship. We respectfully urge CalPrivacy not to impose new requirements in this area. Additional mandates would create compliance burdens for employers without meaningfully enhancing employee protections beyond what is already provided. The employment context involves legitimate business needs for data processing that differ significantly from consumer-facing contexts, and the current rules appropriately account for these distinctions. Further regulation would add complexity to employment practices, potentially creating confusion for both employers and employees rather than clarity. We believe the current framework adequately protects employee privacy while allowing employers to maintain necessary business operations.

That said, businesses face unique challenges providing notices to applicants, employees, former employees, independent contractors, officers, directors, dependents, emergency contacts, and beneficiaries because human resources (HR) data is collected across many legally required functions, including recruiting, payroll, benefits, tax, workplace safety, investigations, leave administration, and record retention. Unlike ordinary consumer data, HR data is dynamic, often sensitive, and tied to overlapping employment law obligations. This is compounded by employers' need to provide notice at or before time of collection and employers do not have direct communication with some HR clients (i.e., dependents, beneficiaries, and emergency contacts).

CalPrivacy should coordinate with the Department of Industrial Relations to ensure disclosures are not duplicative and occur at set intervals. For example, providing disclosures at the time of interviews, onboarding, and annually. Creating off-cycle notices, however, would pose challenges to many businesses.

4. Have you exercised your CCPA rights as a job applicant or employee?

a. Describe your experience exercising your rights.

b. Describe any challenges you experienced when exercising your rights.

c. Do you have any suggestions on how to improve the experience?

5. What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights? How can the regulations address this issue?

As stated above, businesses face significant operational and legal challenges when administering privacy rights requests from applicants, employees, former employees, and contractors because workforce data exists across numerous internal systems, vendors, retention environments, and legally regulated processes. As a result, employers must constantly balance privacy rights against mandatory data retention frameworks.

Access requests. Businesses face significant challenges interpreting the CCPA data access right as applied to employees due to the nature of employment data and other regulatory frameworks. When an employee requests "all my personal information," the scope of responsive data in an employment context is enormous and may include payroll records, performance reviews, investigation notes, manager feedback, messages, badge access logs, productivity data/metrics, benefits records, internal communications, and workforce analytics maintained across multiple systems and storage environments, and more.

CalPrivacy in coordination with other agencies should provide clear guidance on what categories of HR data are subject to data access requests, and what categories are excluded. In doing so, CalPrivacy should take into account that certain categories of employment data should not be disclosed to the requesting employee because doing so would compromise legitimate business interests or cause harm to third parties. For example:

- **Investigation records and witness statements, such as employee relations investigative reports:** Disclosure could expose complainants or witnesses to retaliation and chill future reporting of workplace misconduct.
- **Security and loss prevention records:** Disclosure could compromise active investigations or enable circumvention of workplace safety measures.
- **Proprietary workforce analytics:** assessments and workforce planning documents may contain trade secrets, the disclosure of which would harm competitive position.

CalPrivacy should also take into account that California employees already have rights to access their personnel records under Labor Code §§ 1198.5 and 432. CalPrivacy should adopt those statutes as the baseline framework for employee access requests and clarify that data categories beyond personnel records are outside the scope of employee request obligations.

Requests during active investigations or litigation. CalPrivacy should also permit employers to deny data access or correction requests where the responsive data relates to an active complaint, lawsuit, investigation, or other inquiry or action that requires a litigation hold. Employers should be permitted to rely on general legal exceptions in their response without identifying the specific basis for withholding information or disclosing the existence of an investigation consistent with other frameworks that recognize disclosure of investigation-related data can compromise evidence integrity and enable retaliation against complainants (e.g., FOIA exemptions, GDPR Art. 23, and California whistleblower protections).

Data retention clarity. Additional clarity regarding data retention obligations could be helpful. Specifically, clear regulations at the data category level on how long employment related data must be retained. For example, employers often retain HR data for varying periods depending on litigation risk. Without clear regulatory guidance on when to prioritize privacy over litigation-defense retention, businesses are forced to make risk-based decisions, which may vary significantly across organizations. This can also cause confusion for employees as to what they can reasonably expect.

Identity verification for former employees, job applicants, and contingent workers. Verifying the identity of applicants and former employees presents unique operational challenges. Unlike consumer requests where identity can often be verified via existing accounts, former employees no longer have access to employer systems, and employers may possess only limited information for applicants and contractors. Verifying the identity of a former employee who contacts their former employer via personal email requires additional steps. Clear regulatory guidance regarding minimum authentication standards would help businesses avoid additional data collection during verification.

CalPrivacy should toll the 45-day response period during identity verification for former employees who no longer have access to employer systems. The response clock should begin upon successful verification, not upon receipt of the request. Employers should be permitted to require government-issued ID matched against employment records, and should be deemed compliant if the requestor fails to cooperate with reasonable verification attempts within 30 days.

When a contingent worker submits a request, each entity should only be required to produce data for which it is the controller. The worksite employer should not be obligated to collect or produce data held by the staffing agency (or vice versa), even where both entities process data about the same individual in connection with the same work.

Finally, CalPrivacy should account for the practical realities of HR data management when establishing compliance expectations, including that HR data may not sit neatly in a database, and may sit in physical storage (e.g., file cabinets in a storage room), legacy systems, and cloud environments, depending on the age and size of the business. The size of the business and their ability to invest in HR infrastructure should also be taken into account.

6. What steps do businesses take to oversee their service providers' and contractors' CCPA compliance, and what challenges do businesses face when doing so?

For example, do businesses conduct audits of these entities or test the service provider's or contractor's systems? How effective are these audits and tests to assess a service provider's or contractor's CCPA compliance?

Businesses commonly oversee service providers' and contractors' CalPrivacy compliance through contractual requirements, vendor due diligence, security questionnaires, certifications, data processing agreements, incident reporting obligations, and periodic compliance reviews. For example, some companies use a third-party management team to ensure contracts meet CalPrivacy requirements. Businesses also regularly partner with third parties that process or control data on the business's behalf. For example, if a business receives a data access request involving information maintained by a third party, the business may need to coordinate with that third party to identify, retrieve, review, and produce responsive information.

Businesses should retain meaningful flexibility in how they oversee and manage their service providers and contractors with regard to privacy-related contractual commitments. The current contractual framework, which requires service providers and contractors to agree to specific privacy obligations, provides sufficient accountability mechanisms. These contractual provisions, combined with businesses' existing oversight practices, create an effective system of checks and safeguards. We urge CalPrivacy not to mandate burdensome, prescriptive audits and testing requirements that would impose significant costs on businesses without proportionate benefits to consumers. Such mandates would disproportionately affect smaller businesses that lack the resources to conduct extensive audits, potentially creating barriers to market participation. Moreover, a one-size-fits-all approach to oversight fails to account for the varying risk profiles of different relationships. Businesses are best positioned to determine the appropriate level of oversight for their specific circumstances, taking into account factors such as the nature and sensitivity of the data involved, the service provider's track record, and the overall risk profile of the relationship. A flexible approach that allows businesses to tailor their oversight practices to their specific needs will prove more effective than rigid regulatory mandates.

7. What else should CalPrivacy consider regarding CCPA requirements for job applicants and workers in the employment lifecycle (hiring, working, and offboarding)?

CalPrivacy should limit ADMT disclosure and opt-out requirements in the employment context to automated processing that serves as a substantial factor in decisions materially altering the terms of employment (hiring, termination, promotion, demotion). Operational tools used for scheduling, workload distribution, safety monitoring, or productivity measurement should be expressly excluded absent a direct nexus to a consequential employment decision.

There is tremendous opportunity for businesses to gain efficiencies through automation and artificial intelligence (AI) (e.g., AI agents/chatbots that streamline manager/employee self-service). It is challenging to balance process automation using AI and/or ADMT and applicant/worker privacy risks. An opt out requirement is not always operationally feasible or ideal, which prevents large employers from adopting automation in some cases.

Former employee data. CalPrivacy should confirm that privacy notices provided during employment remain effective post-separation. No additional notice or disclosure obligation should arise because the employment relationship has ended.

Employment-adjacent personas. CalPrivacy should exclude from the definition of "consumer" any individual whose personal information is collected solely in connection with an employment relationship, including former employees (alumni) and employee dependents or beneficiaries enrolled in employer-sponsored benefits. Colorado (CPA §6-1-1303(5)) already adopts this approach. These individuals have no direct commercial relationship with the employer, and their data should be governed by employment data rules rather than consumer privacy obligations.

Sensitive data processed for employment administration. The California Privacy Rights Act's (CPRA) "sensitive personal information" category includes SSN, precise geolocation, union membership, and health data, all of which employers routinely process for legitimate employment purposes (payroll, logistics, labor relations, leave administration). CalPrivacy should clarify that the "limit use" right does not apply to sensitive data processed solely for employment administration purposes.

Harmonization with other California employment laws. The CCPA/CPRA sits alongside California Fair Employment and Housing Act (FEHA), Labor Code, California Worker Adjustment and Retraining Notification Act

, and other statutes that create independent data collection and retention obligations. CalPrivacy should ensure its regulations don't conflict with these requirements (e.g., requiring deletion of data that FEHA requires employers to retain for defense of discrimination claims).

III. Conclusion

CalChamber urges CalPrivacy to approach further regulatory developments at this time with extreme caution and from an evidence-based approach that ensures further clarity and protection to consumers. Businesses are continuing to implement CalPrivacy's recent ADMT Regulations and need time before additional requirements are imposed.

CalChamber appreciates CalPrivacy's consideration of these comments, and we look forward to continuing to work with the agency on these important issues.

Sincerely,

Ronak Daylami
Vice President for Advocacy | Privacy, Cybersecurity & Emerging Technologies
California Chamber of Commerce

Catbagan, Christian@CPPA

From: Morgan Stevens <MStevens@actonline.org>
Sent: Wednesday, May 20, 2026 2:35 PM
To: Regulations@CPPA
Cc: Graham Dufault
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: ACT Comment re CalPrivacy Notices and Employee Data.pdf

This Message Is From an External Sender
WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

Please find attached comments from the Association for Competitive Technology in response to CalPrivacy's invitation for preliminary comments on notices & disclosures and employee data.

Thanks very much for the consideration and please let me know if you need any further information.

Sincerely,
Morgan Stevens

--
Morgan Stevens
Policy Associate
ACT | The App Association
(818) 823-8240 | LinkedIn

ACT Association for Competitive Technology

May 20, 2026

California Privacy Protection Agency
Attn: Legal Division—Regulations
400 R St. Suite 350
Sacramento, California 95811

RE: Preliminary Comment – Notices & Disclosures and Employee Data April 2026

The Association for Competitive Technology (ACT) writes to submit comments concerning the California Privacy Protection Agency (CalPrivacy) rulemaking regarding notices & disclosures and employee data.[1]

ACT represents small business innovators and startups in the software development and high-tech space located in California, across the United States, and around the globe.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, the domestic app economy is worth more than $1.8 trillion and provides over 6.1 million American jobs.[3]

As CalPrivacy proceeds with rulemaking, we urge the agency to carefully consider how any proposed rules would affect small and medium-sized developers who provide online services in the state of California. Many small developers do not have the same resources or legal expertise to navigate compliance with new regulatory requirements or interpret statutory obligations as their larger competitors. Any new regulations should protect consumer privacy without unduly burdening small businesses or compromising digital access. To that end, we respectfully urge CalPrivacy to adopt a balanced, flexible approach to regulations governing privacy notices and disclosures and employee data.

I. Notices & Disclosures

2. What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?

Small businesses often lack dedicated privacy counsel and must draft privacy policies using limited internal resources. This is especially true of startups and small businesses with headcounts in the single digits. Without clear regulatory guidance on how to describe common data practices, small businesses may have to rely on generalized language that

[1] https://cppa.ca.gov/regulations/pdf/notices_disclosures_employee_data.pdf
[2] ACT | The App Association, *About*, *available at* http://actonline.org/about.

[3] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

does not accurately reflect their specific operations and create policies that are overly broad, duplicative, or difficult for consumers to follow. CalPrivacy can address this issue by providing additional standardized terminology, plain-language guidance, sample clauses, and adaptable model disclosure templates that businesses can tailor to their own practices. Authoritative resources from CalPrivacy would give small businesses a reliable compliance baseline to build upon and improve the quality and clarity of consumer-facing privacy policies without requiring costly external legal expertise.

3. What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this issue?

Small businesses face several challenges when describing their information practices in privacy policies and other consumer-facing disclosures. Many small businesses rely on third-party tools and services to complement their own products or services. Accurately describing their data practices and other downstream data flows in a consumer-facing disclosure can be burdensome for small businesses, especially in scenarios where they lack the leverage and capacity to obtain and convey detailed data practice information from their vendors. Moreover, the current patchwork of state privacy laws requires small businesses to draft privacy policies and other consumer-facing disclosures to account for several different sets of obligations. As a result, small businesses must anticipate and disclose practices across a range of categories and contexts, which can result in lengthy, complex policies that ultimately undermine the goal of consumer transparency.

CalPrivacy can address these challenges by providing clearer guidance on the level of detail expected in privacy disclosures, particularly for common business scenarios, such as the use of third-party analytics or advertising services. CalPrivacy should also work with regulators in other states with comprehensive privacy laws to harmonize privacy policy and disclosure requirements to the extent possible. By providing guidance and harmonizing expectations, CalPrivacy can help reduce the compliance burdens on small businesses and ensure consumers can access meaningful, accessible information about how their data is collected, used, and shared.

5. What challenges do businesses face when providing notices, including opt-out links, across different devices or platforms? How can the regulations address this issue?

Small businesses increasingly build products and services that operate across a variety of platforms and devices, including mobile apps, web applications, and connected devices. Providing consistent, compliant notices and opt-out mechanisms across these environments presents costly and complex technical and design challenges. In order to ease the associated burdens on small businesses, CalPrivacy should adopt regulations that are technology-neutral and focused on outcomes rather than prescribing specific notice formats or mechanisms. Regulations should provide flexibility for businesses to deliver notices and opt-out mechanisms in a manner appropriate to the device or platform, as long as the notice is clear, accessible, and functional.

II. Employee Data

3. What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?

Providing privacy policies, Notice at Collection, and CCPA rights' notices to job applicants and employees presents operational challenges for small businesses. Unlike consumer-facing privacy disclosures, which can typically be delivered through a business's existing website or app, employment-related notices must be integrated into hiring and onboarding workflows that are often managed through a patchwork of third-party tools, including HR platforms, payroll processors, and benefits administrators. Small businesses that do not have formal HR departments or established onboarding processes may rely on these tools and have limited ability to ensure that notices are delivered at the appropriate point in the employment lifecycle. CalPrivacy can address these challenges by providing tailored guidance and model notices specifically designed for the employment context, including practical examples of how to deliver notices at different stages of the employment lifecycle.

5. What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights? How can the regulations address this issue?

Small businesses must often rely on third-party tools and platforms to perform HR functions. As a result, many small businesses may face challenges in locating and compiling employee data and responding to a rights request comprehensively and within required timeframes. CalPrivacy should consider whether the regulations can provide practical flexibility for small businesses responding to employee rights requests that require coordination across multiple platforms or service providers.

6. What steps do businesses take to oversee their service providers' and contractors' CCPA compliance, and what challenges do businesses face when doing so? For example, do businesses conduct audits of these entities or test the service provider's or contractor's systems? How effective are these audits and tests to assess a service provider's or contractor's CCPA compliance?

Small businesses typically rely on contractual provisions and vendor representations to oversee their service providers' and contractors' CCPA compliance. Unlike larger companies, most small businesses do not have the resources or technical capacity to conduct independent audits or test their vendors' systems and must instead rely on contractual commitments those providers offer.

CalPrivacy should ensure that any service provider and contractor oversight mechanisms in forthcoming regulations are scalable and risk-based, particularly for small businesses. To the extent that regulations include audits, assessments, or technical requirements, they should avoid creating a one-size-fits-all mandate for small businesses to conduct formal audits or technical assessments of their vendors. Instead, CalPrivacy should consider whether reasonable oversight obligations for small businesses can be satisfied

through standardized contractual terms, vendor certifications, or other scalable mechanisms that do not require individual businesses to independently verify providers' compliance.

We appreciate your consideration of the above views and welcome any opportunity to provide additional commentary as the rulemaking process advances.

Morgan Reed
President
Association for Competitive Technology

Catbagan, Christian@CPPA

From: Tony Ficarrotta <tony@networkadvertising.org>
Sent: Wednesday, May 20, 2026 2:39 PM
To: Regulations@CPPA
Cc: Leigh Freund; David LeDuc; Megan Cox; Kate Cox-Nowak
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: NAI_Preliminary_Comments_CalPrivacy_NoticesDisclosures_EmployeeData (May 2026)_formatted.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To the California Privacy Protection Agency,

The NAI is submitting comments in response to the Agency's Invitation for Preliminary Comments on Notices & Disclosures and Employee Data. Please see the attached pdf for our comments. If you have any questions or would like to discuss further, please do not hesitate to reach out.

Thank you,

-Tony Ficarrotta

May 20, 2026

Submitted via electronic mail to: regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Legal Division — Regulations
400 R St., Suite 350, Sacramento, CA 95811

Re: Preliminary Comment — Notices & Disclosures and Employee Data

To the California Privacy Protection Agency ("CalPrivacy"):

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to submit comments in response to CalPrivacy's Invitation for Preliminary Comments on Notices & Disclosures and Employee Data.[1] The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. Since 2000, the NAI has promoted voluntary industry standards for its member companies, which range from small startups to some of the largest companies in digital advertising, including ad exchanges, demand-side platforms, supply-side platforms, and other providers of advertising-technology solutions.

I. Introduction

The California Consumer Privacy Act's ("CCPA") builds consumer rights on a foundation of business disclosures. When those disclosures are clear, consistent, and comprehensible, consumers are better able to exercise their rights. However, due to the complexity of both the CCPA's disclosure requirements and how consumer personal information is used in today's digital economy, businesses face real challenges when balancing fidelity to the CCPA's requirements and their business practices against clarity and comprehensibility for consumers.

The NAI has worked with its member companies to help them achieve that balance for 25 years. Each year, NAI staff reviews, among other things, every member company's privacy notices through the NAI's Privacy Review Program.[2] The NAI's general observations from last year's Privacy Review cycle are documented in the NAI's 2025 Annual Report.[3] That hands-on review work helps the NAI develop a perspective on best practices for consumer-facing disclosures. The recommendations and illustrative examples included in our comments are based in part on the NAI's experience conducting the 2025 Privacy Review cycle.

---

[1] Cal. Priv. Prot. Agency, Invitation for Preliminary Comments: Notices & Disclosures and Employee Data (May 2026), https://cppa.ca.gov/regulations/pdf/notices_disclosures_employee_data.pdf [hereinafter "*CalPrivacy Invitation for Preliminary Comments*"].
[2] *See* NAI's Principles & Self-Regulatory Framework, Appendix A, § 1(a)–(d) (Accountability Requirements for Principle 1 – Transparency), (Mar. 2025), https://www.thenai.org/wp-content/uploads/2025/03/NAI-Framework_March-2025.pdf [hereinafter "*NAI Framework*"]. Member companies are required to undergo an annual review of their transparency disclosures and privacy notices under the NAI Framework.
[3] *See* NAI's 2025 Annual Report, Section III — Privacy Review Program, at 17, https://thenai.org/wp-content/uploads/2026/05/The-NAIs-Annual-Report_2025.pdf [hereinafter "*Annual Report*"].

The NAI believes that today's disclosure environment can be improved, and we hope that in providing these comments we can support regulations that promote disclosures that are both clear, comprehensible, and useful to consumers and easy to implement for businesses.

Below, we list each question posed by CalPrivacy, and provide substantive responses to many of them. In summary, our recommendations are as follows. CalPrivacy should:

1. Issue a voluntary model Notice at Collection as a regulatory safe harbor for the form of the disclosure.
2. Add illustrative examples to the regulations covering disclosure scenarios where the operational gap between principle and disclosure is widest, including (a) categories of third parties in programmatic advertising, (b) retention periods and criteria, and (c) opt-out preference signal display and probabilistic linkage scenarios.
3. Issue an illustrative example on the website / services two-policy disclosure structure common on business-to-business advertising technology websites.
4. Add a nonexclusive regulatory example for notice on interfaces that do not support traditional webpage-based notices, including connected televisions, over-the-top streaming services, and gaming consoles.
5. Clarify in regulation that businesses should not present additional links, referrals, or other disclosures in a manner reasonably likely to confuse or mislead consumers about how to exercise their CCPA rights.
6. Establish a voluntary Alternative Notice Link modeled on the existing Alternative Opt-out Link.
7. Recognize IP-based location estimation as a permissible basis for delivering state-tailored privacy notices at initial notice presentation.
8. Take a risk-based approach on vendor oversight in the employee data context.

II. Notices and Disclosures

Q1. ***When reviewing a privacy policy or similar disclosure, what is the most important information to consumers? What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?***

N/A

Q2. ***What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?***

See our response to Question 3 below, which addresses recurring drafting issues observed across the 2025 Privacy Review cycle and the regulatory tools that may be able to address them.

Q3. ***What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this issue?***

Two structural challenges shape how digital-advertising businesses approach the disclosures the CCPA requires. The first is translating operationally complex practices, including the use of pseudonymous identifiers, data flows involved in cross-context behavioral advertising, and data retention periods that sometimes involves technical elements into: (1) language that is both

technically accurate and accessible to an ordinary consumer; and (2) a format short enough to be useful at the point of collection. The result is wide variance and inconsistent translation of similar practices across notices. This sometimes leads to inefficiency for businesses charged with providing these disclosures, and it may hamper consumer understanding of similar practices across different businesses. Below, the NAI provides recommendations for how CalPrivacy can use regulations to help address these issues.

A. CalPrivacy should issue a voluntary model Notice at Collection that businesses can adopt as a regulatory safe harbor for the form of the disclosure

Among the existing California disclosure obligations, the Notice at Collection is the best-suited candidate for a voluntary model form. Every covered business that collects personal information must provide one at or before each point of collection.[4] The Notice at Collection regulations specify six content elements, and those elements lend themselves to a tabular layout that maps each statutory element to a standardized column.[5]

There is strong precedent for issuing a voluntary model form. Federal regulators have used voluntary model forms with documented results in adjacent privacy contexts. The closest precedent is the Model Privacy Form under the Gramm-Leach-Bliley Act, issued through a joint interagency rulemaking in 2009[6] following formal consumer-comprehension research.[7] The rulemaking record summarizing those studies found that the model form materially outperformed alternative formats on consumer comprehension, the ability to compare practices across institutions, and the ability to make informed choices.[8] However, adoption of the Model Privacy Form is voluntary; a financial institution that uses the model form consistent with the regulators' instructions is in a safe harbor on the form-of-disclosure obligation.[9]

The Notice at Collection presents a similar design opportunity for CalPrivacy. The NAI's 2025 Privacy Review observed variation across different notices at collection with respect to categorization vocabulary, retention formulations, and sale-and-sharing presentation among the businesses we reviewed.[10] To promote normalization of those disclosures, the NAI recommends that CalPrivacy issue a voluntary model Notice at Collection, with safe-harbor treatment for the

---

[4] Cal. Civ. Code § 1798.100(a); Cal. Code Regs. tit. 11, § 7012(a), (d).
[5] Cal. Code Regs. tit. 11, § 7012(e)(1)–(6).
[6] *Final Model Privacy Form Under the Gramm-Leach-Bliley Act*, 74 Fed. Reg. 62890 (Oct. 1, 2009), https://www.federalregister.gov/documents/2009/12/01/E9-27882/final-model-privacy-form-under-the-gramm-leach-bliley-act (joint adoption by the OCC, the Federal Reserve, the FDIC, the Office of Thrift Supervision, the NCUA, the FTC, the CFTC, and the SEC) [*hereinafter "Final Model Privacy Form"*].
[7] Alan Levy & Manoj Hastak, *Consumer Comprehension of Financial Privacy Notices* (2008), https://www.ftc.gov/system/files/documents/reports/quantitative-research-levy-hastak-report/quantitative_research_-_levy-hastak_report.pdf; Kleimann Communication Grp., *Financial Privacy Notice: A Report on Validation Testing Results* (Feb. 12, 2009), https://www.ftc.gov/system/files/documents/reports/financial-privacy-notice-report-validation-testing-results-kleimann-validation-report/financial_privacy_notice_a_report_on_validation_testing_results_kleimann_validation_report.pdf.
[8] *Final Model Privacy Form*, *supra* note 6, at 62894–98.
[9] 17 C.F.R. § 248.2; *Final Model Privacy Form*, *supra* note 6, at 62890.
[10] *Annual Report*, supra note 3, §§ III.a.i–iv, at 20–24.

form and presentation of the notice, conditional on accurate completion of the model fields and on compliance with the CCPA readability standard.[11]

A model form drawn along these lines could be structured substantially as illustrated in Appendix A. Any model form, however, should accommodate a variety of business models, including digital advertising and related services. For example:

- An ad-technology business that processes pseudonymous identifiers. A business that collects information through cookies, mobile advertising IDs, or hashed values rather than direct identifiers can populate the Identifiers row with the operative pseudonymous identifier types and the purposes for which they are used. A sample row for a publisher whose advertising-technology partners process such identifiers is populated in the example form provided in Appendix A.
- A business operating under the third-party-collection rule. Where a first-party publisher allows a third-party ad-tech business to control collection of certain personal information on the publisher's site, both businesses have Notice at Collection obligations, and the regulations permit them to provide a single joint notice describing their collective information practices.[12] Any model form should accommodate this scenario by allowing the publisher to incorporate the relevant practices of third-party businesses into its own notice. In many cases, ad-tech companies have no direct contact with the consumer because the publisher controls the consumer-facing surface entirely. In those scenarios, publisher-delivered Notice at Collection is the only realistic mechanism through which these businesses can satisfy their obligation. CalPrivacy guidance can help reinforce that the publisher's joint notice or equivalent upstream delivery is sufficient. An example illustrating an approach to this type of scenario is provided in Appendix A.

B. CalPrivacy should add illustrative examples in the regulations for digital-advertising disclosure scenarios where the operational gap between principle and disclosure is widest

Beyond the Notice at Collection, the broader privacy-policy disclosure obligations cover a wider range of substantive material that varies across business models. A single model form would likely struggle to capture that breadth. A more apt regulatory tool is the illustrative example, which CalPrivacy already employs extensively in existing regulations. The Notice at Collection regulations already use multiple illustrative examples covering where to make the notice "readily available," how to handle third-party collection, and how to apply the notice in physical-premises contexts.[13] The NAI identifies three candidates from the 2025 Privacy Review where additional illustrative examples would likely help guide businesses in meeting CalPrivacy's expectations and improve efficiency for businesses.

1. Categories of third parties in programmatic advertising anchored to the "meaningful understanding" standard.

The "meaningful understanding" standard for third-party-category disclosures requires within-category granularity that the current regulations do not yet illustrate for the digital-advertising recipient ecosystem. Section 7011(e)(1)(E) requires the privacy policy to describe categories of

[11] Cal. Code Regs. tit. 11, § 7003(a)–(b); *see also id.* § 7012(b).
[12] *Id.* § 7012(g)(1).
[13] *Id.* § 7012(c) (five examples on availability); *id.* § 7012(g)(3) (three examples on third-party collection).

third parties to whom personal information is sold or shared "in a manner that provides consumers a meaningful understanding of the parties to whom the information is sold or shared."[14] The existing definitions in the regulation define "categories of third parties" with generic examples that include "advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."[15] What that definitional baseline does not provide, and what the "meaningful understanding" standard does not yet illustrate, is the level of within-category granularity that the digital-advertising recipient ecosystem requires for the standard to be operative for consumers. Within the regulation's broad category of "advertising networks" alone, several functionally distinct types of recipients operate, and publishers, advertisers, and ad-tech companies face choices of how, or whether, to disaggregate them in their privacy policy disclosures. Their choices in this regard may impact consumer understanding, including disclosures that are too general but also too specific, as industry sub-categories or terms of art may not aid consumer understanding or be material to their decisions about whether to exercise their privacy rights. CalPrivacy can help guide companies and enhance consumer understanding by providing illustrative examples using categories of third parties. An illustrative example could read substantially as follows:

> *A publisher that displays advertising sold through programmatic real-time bidding could describe the categories of third parties to whom it sells or shares identifiers and internet-activity information for advertising as follows, where each category applies: (i)* ***Advertising marketplace and ad-delivery providers*** *— companies that operate the platforms used to request, bid on, select, deliver, and report on ads (industry terms: supply-side platforms, demand-side platforms, and ad exchanges); (ii)* ***Identity and matching providers*** *— companies that maintain advertising identifiers and link consumer activity across browsers and devices for advertising-targeting and measurement purposes; (iii)* ***Measurement, analytics, and attribution providers*** *— companies that measure ad delivery, performance, reach, frequency, and attribution; (iv)* ***Ad verification, fraud-prevention, and brand-safety providers*** *— companies that detect invalid traffic, protect against fraud and security threats, and assess whether ads appear in appropriate contexts; and (v)* ***Audience and data providers*** *— companies that provide, receive, or help create audience segments used for targeting or measurement.*

An example like this (or with another level of granularity that CalPrivacy assesses as appropriate) would tell a consumer in plain language what each category of recipient does, while preserving an opportunity to provide more detailed terminology in parentheticals for precision. It would also resolve the design tension between overly generic disclosures (e.g., "our advertising partners") and overly granular disclosures (an enumeration of every counterparty in a real-time bidding flow).

The example provided above represents one approach to striking a balance that maximes consumer comprehension while providing meaningful guidance to businesses. However, a business may still meet the "meaningful understanding" standard through different categorizations that accurately reflect its specific data flows. The same plain-language discipline applies to how businesses describe the purposes for which they collect and use personal information. A purpose described in concrete operational terms (for example, limiting the number of times an ad is shown (frequency capping), ad performance measurement, or geographically

[14] *Id.* § 7011(e)(1)(E).
[15] *Id.* § 7001(g).

relevant advertising) gives the consumer more usable information than a generic formulation such as "business purposes" or "advertising."

2. Retention periods or criteria.

Retention disclosure is a recurring drafting challenge: general formulations like "as long as necessary for the purposes described" may satisfy the CCPA's approach in form but provide limited information for consumer comprehension. The statute and the implementing regulation require businesses to disclose, for each category of personal information, either the period for which the business intends to retain that category or the criteria the business uses to determine that period.[16] An illustrative example would distinguish three retention patterns commonly used in digital-advertising disclosures:

> *A business may disclose retention for each category of personal information using the pattern that fits the underlying data: (i)* ***Identifier expiry or refresh-based retention*** *— for identifiers such as cookies or session tokens that expire or are refreshed by consumer interaction: "Browser cookies are retained for [defined period] from collection or until the cookie expires or is reset by the consumer's next interaction with the business, whichever occurs first." (ii)* ***Relationship-based retention*** *— for information retained while a consumer maintains an active relationship with the business: "Information tied to an active consumer account is retained for the duration of the account plus a defined period thereafter for routine account-closure processing." (iii)* ***Policy-based retention*** *— for information retained under a defined business-purpose schedule: "Information retained for audit, fraud-prevention, dispute-resolution, or legal-compliance purposes is retained for [defined period] from collection consistent with the business's documented retention schedule, after which the data is deleted, aggregated, or de-identified."*

The three patterns are not mutually exclusive (a single business will commonly use all three), but illustrating them separately could help close the gap between general criterion formulations and consumer-operative disclosure.

3. Opt-out preference signal display, and signal-scope clarification in identity-graph linkage scenarios.

The existing regulations covering opt-out preference signals (OOPS) already provide substantial guidance, including five illustrative examples, descriptions for how a business should display whether it has processed the consumer's OOPS, and how a business should treat an OOPS as a valid request to opt-out of sale/sharing for the consumer's "browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles."[17] However, two adjacent disclosure issues on OOPS are not yet illustrated in the regulations, and the NAI's 2025 Privacy Review surfaced both as areas where guidance would help businesses and consumers.

The first is **the placement and persistence of the opt-out display in preference-center environments**: guidance on where the display should appear, how persistent the display must be across navigation and sessions, and whether the display should describe the scope of processing affected by the signal beyond stating "Opt-Out Request Honored." The existing examples illustrate the general fact of display but not other considerations that will help determine whether

[16] Cal. Civ. Code § 1798.100(a)(3); Cal. Code Regs. tit. 11, § 7012(e)(4).
[17] Cal. Code Regs. tit. 11, § 7025(c)(1), (c)(6), (c)(7)(A)–(E); *id.* § 7026(g).

the display is usefully visible to consumers in practice, or what opt-out requests have been honored, or in what way.

The second is **signal scope in identity-graph linkage scenarios**: a business may maintain linkages associating a browser with other browsers, devices, or pseudonymous profiles in the ordinary course of its business, but those associations are made without relying on an account login. This distinction can be critical, as these linkages are *probabilistic*, whereas account logins are *deterministic*, and thus extending an opt out across probabilistic linkages will often yield imprecise results. The existing examples illustrate scenarios in which such association either exists through a logged-in account or does not exist at all; the intermediate case is left for businesses and consumers to navigate without a guiding example.[18] An additional illustrative example in the regulations would help clarify how the opt-out should apply to probabilistically linked browsers or devices, and how the business should describe the scope to the consumer.[19] Any such example should apply only to linkages a business maintains in the ordinary course and should not require businesses to create or expand identity-graph linkages for the purpose of opt-out propagation.

Currently, the regulations also require businesses to explain how an OOPS will be processed, including whether the signal applies to the device, browser, consumer account, and/or offline sales.[20] Similarly, due to the probabilistic (and imprecise) nature of certain linkages, properly describing how an OOPS will be processed in this context invites risk of describing the scope of the opt out in a way that will be unclear to a consumer. As the requirement to properly disclose and explain how an OOPS will be processed for the consumer has been an enforcement priority for CalPrivacy, the intermediate probabilistic linkage example is precisely where that explanation is hardest to operationalize.[21]

C. CalPrivacy should issue an illustrative example on the website privacy policy / services privacy policy structure that is common in business-to-business ad-tech

California-resident visitors to a business-to-business ad-tech provider's marketing website are consumers under the CCPA, regardless of professional capacity. The CCPA defines a "consumer" as "a natural person who is a California resident … however identified, including by any unique

---

[18] Notably, example D addresses how an OOPS should be processed when a consumer is sharing online browsing habits through the use of a pseudonymous cookie. *See id.* § 7025(c)(7)(D). However, this example does not address whether or how the scope of an OOPS should be extended to an identity graph relying on probabilistic linkages between cookie identifiers.

[19] *Cf.* Network Advertising Initiative, *Guidance for NAI Members: Cross-Device Linking* § II.C, at 5 (May 2017), https://thenai.org/wp-content/uploads/2021/07/NAI_Cross_Device_Guidance.pdf [hereinafter *NAI Cross-Device Guidance*]. When a consumer opts out on one browser or device, the *NAI Cross-Device Guidance* suggests preventing personalized advertising from being served on that browser or device; as well as preventing data collected from that browser or device from being used on other browsers or devices for personalized advertising. The NAI's recommendation here is not that opt-out preference signals automatically propagate across all probabilistic linkages, but that the regulations should provide a guiding example for businesses operating in the intermediate scenario. The *NAI Cross-Device Guidance* provides a proven model for how to do so.

[20] *See* Cal. Code Regs. tit. 11, § 7011(e)(3)(F).

[21] CalPrivacy cited this disclosure requirement in *In re Tractor Supply Co.*, Stipulated Final Order ¶ 43 (Cal. Priv. Prot. Agency Sept. 26, 2025), https://cppa.ca.gov/pdf/20250930_tractor_supply_bd_sfo.pdf; *cf. Complaint*, *People v. Disney DTC, LLC*, No. 26STCV04425 ¶ 15 (Cal. Super. Ct., L.A. Cnty., filed 2026), https://oag.ca.gov/system/files/attachments/press-docs/1%20-%20Complaint%20(Disney).pdf (framing failure to honor opt-out preference signals as a form of deception).

identifier."[22] The former business-to-business exemption, which carved out personal information collected from natural persons acting on behalf of a business in a business-to-business transaction, sunset on January 1, 2023 and is no longer operative.[23] When a covered business collects personal information from a California-resident visitor to its marketing website, the visitor's professional capacity does not exempt the interaction from the CCPA, and the disclosure obligations under the statute and the implementing regulations apply to that collection.

It is common industry practice for business-to-business ad-tech providers to adopt a two-policy structure for marketing-website disclosure: a **website privacy policy** addressed to visitors to the provider's marketing website, and a **services privacy policy** addressed to the end users whose personal information the provider processes through its ad-tech services on other digital properties. The NAI supports this structure because it reflects the fact that the provider operates in two distinct relationships, one with marketing-site visitors and one with end users of the provider's customers' services, each involving different information practices governed by the same CCPA framework.

However, the two-policy structure raises a disclosure-design question that an illustrative example could help resolve. A California-resident visitor to the provider's marketing website is entitled to a comprehensive description of the business's information practices under the privacy-policy regulations. The website privacy policy will ordinarily be the operative disclosure for the consumer's interaction with the marketing website. The services privacy policy describes information practices that may not apply to the marketing-website visitor, but may apply in some scenarios, including where the same provider's advertising technology operates on the marketing website itself. From the consumer's perspective, the question is which policy applies to the marketing-website interaction and how to navigate between them; from the business's perspective, the question is how the two-policy structure satisfies the comprehensive-description requirement for the website-visitor consumer.

The NAI recommends that CalPrivacy issue an illustrative example clarifying how the two-policy structure can give the marketing-website consumer a comprehensible path through the relevant disclosures. An illustrative example could provide that:

> *Business Q is an advertising-technology provider that operates a marketing website for its customers and prospective customers on its own domain; and provides separate services that process personal information in connection with its customers' websites and applications. Business Q maintains two privacy policies: a website privacy policy that applies to the marketing website, and a services privacy policy that applies to Business Q's services as deployed by its customers. On the marketing website, Business Q provides a Notice at Collection at or before the point of collection, including by posting a conspicuous link to the notice on its homepage(s), on webpages where personal information is collected, and in close proximity to webform input fields. The Notice at Collection contains the information required by subsection (e) and includes a link that takes the consumer directly to the relevant section of Business Q's website privacy policy. The website privacy policy describes the information practices applicable to the marketing-website interaction. Where Business Q's services also operate on the marketing website, the website privacy policy either describes those practices*

[22] Cal. Civ. Code § 1798.140(i).
[23] *See id.* § 1798.145(n)(3) ("This subdivision shall become inoperative on January 1, 2023."). Subdivision (n) — the former business-to-business exemption — remains in the statute text but is inoperative by its own terms; the legislature did not extend or replace it.

or provides a conspicuous link that takes the consumer directly to the relevant section of the services privacy policy. This example addresses only Business Q's marketing website and does not determine Business Q's role or notice obligations in any customer's deployment of Business Q's services.

This kind of example would address a recurring drafting question NAI's members have surfaced through the 2025 Privacy Review, while preserving the flexibility for businesses to address two distinct audiences through purpose-appropriate disclosures.

Q4. *What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights? For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?*

The CCPA's notice principles are device-agnostic: disclosures must be easy to read and understandable, and methods for submitting requests and obtaining consent must be easy to understand, symmetric in choice, free of confusing or impairing architecture, and easy to execute.[24] The illustrative examples that accompany those principles, however, address websites, mobile applications, offline forms, telephone, and in-person interactions; the only non-webpage examples in the Notice at Collection regulation concern Wi-Fi captive portals and in-vehicle signage.[25] That leaves real implementation uncertainty on connected televisions ("CTV"), over-the-top ("OTT") streaming services, and gaming consoles. The requirement that a business not operating a website "shall make the privacy policy conspicuously available to consumers"[26] could be clearer as applied to businesses collecting personal information through those platforms.

The NAI recommends that CalPrivacy add a nonexclusive regulatory example confirming that, for interfaces that do not support traditional webpage-based notices, a business may provide notice through a surface-appropriate mechanism (including on-device settings entries, QR codes, short URLs, or paired-application handoffs), provided the mechanism is conspicuous, available at or before the point of collection, routes the consumer directly to the relevant notice or rights mechanism, and complies with the device-agnostic notice principles. The example should not mandate any single user-experience design pattern, should not require long-form notice presentation on constrained interfaces, and should not restrict businesses from offering companion-device handoffs as a primary path where on-surface input mechanisms are cumbersome.

Q5. *What challenges do businesses face when providing notices, including opt-out links, across different devices or platforms? How can the regulations address this issue?*

NAI's substantive positions relevant to this question are developed elsewhere. On cross-device opt-out propagation, including the application of opt-out preference signals to pseudonymous data environments, see NAI's Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals (April 6, 2026).[27] On notice mechanisms for

---

[24] *See generally* Cal. Code Regs. tit. 11, §§ 7003, 7004.
[25] *See id.* § 7012(c)(1)–(5); *id.* § 7012(g)(3)(B)-(C).
[26] *Id.* § 7011(d).
[27] Network Advertising Initiative, *Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals* (Apr. 6, 2026), https://thenai.org/wp-content/uploads/2026/04/NAI-Preliminary-Comments-Reducing-Friction-Opt-Out-Preference-Signals-4.6.2026_layout-version-2.pdf.

interfaces that do not support traditional webpage-based notices, including CTV, OTT, and gaming surfaces, see our response to Question 4 above.

Q6. *Please provide examples of effective consumer notices and disclosures. If possible, please provide information about specific testing, studies, or data demonstrating their effectiveness.*

Each year, NAI's Privacy Review program conducts hands-on review of member companies' privacy notices, choice mechanisms, governance programs, and other items. NAI staff test member implementations through direct website testing, in-product submission of access and deletion requests, privacy-inbox testing, and A/B comparison of browser sessions with and without Global Privacy Control enabled. The 2025 review cycle generated cross-ecosystem observations of design choices that function at the moment of consumer interaction.[28] These observations arise in the context of member adherence to the NAI Self-Regulatory Framework, not controlled consumer-comprehension testing.[29]

The effective practices described below are drawn from that review process and include design patterns NAI staff identified as effective because they provide clarity and ease of use.

A. **Surfacing relevant identifiers in context.** Identifiers that ad-tech companies rely on are not always easy for consumers to locate, particularly when they are accessible only through technical device settings. In some cases, effective rights workflows can address this discoverability problem by reading and displaying the relevant identifier in context, or providing clear, device-specific instructions for locating it. One effective implementation NAI staff observed that addressed this issue starts with a template DSR submission form that cannot natively surface the business's pseudonymous identifier. However, the implementer reads the consumer's device ID from the browser using an iframe, and then displays the relevant identifier and prompts the consumer to copy it into the form.
B. **Jurisdiction-tailored rights presentation.** As state privacy laws have proliferated, effective rights-disclosure architectures present the rights, processes, and statutory language applicable to the consumer's state through clearly indexed state-specific sections or dedicated jurisdiction-tailored pages. The alternative (conditional "you may have rights" or "if your state has a data privacy law" phrasing) has been flagged by privacy enforcement authorities in Delaware, Connecticut, and Oregon as inadequate.[30]
C. **Cookie-consent banners reflecting symmetry-in-choice principles.** Where a banner presents an "Accept All" path for advertising-related cookies or tracking, the most effective implementations we observe provide an equally prominent reject affordance, granular per-purpose toggles that are clearly described, a notice on the banner itself that Global Privacy Control has been detected and honored where applicable, and a clear display of the consumer's current consent state. The statutory footer-link approach remains a separate compliant path;[31] these design choices describe one effective implementation using banners as a primary disclosure surface, not a California requirement to replace the footer-link approach. The combination reflects the symmetry-in-choice principle articulated in CalPrivacy's enforcement action in the *Honda* matter: that the path for a consumer to exercise a more privacy-protective option cannot be longer, more difficult, or more time-consuming than the path to exercise a less privacy-

[28] *See Annual Report*, *supra* note 3, §§ III, III.b.i, at 17, 25.
[29] *See NAI Framework*, *supra* note 2.
[30] *See Annual Report*, *supra* note 3, § III.a.ii — Declarative Rights, at 20.
[31] *See generally* Cal. Civ. Code § 1798.135.

protective option.[32] The on-banner GPC notice in particular closes a longstanding consumer-comprehension gap, since consumers using GPC otherwise have no contemporaneous confirmation that their preference signal was received.

D. **Privacy policies with dedicated authorized-agent and appeals sections.** State-by-state fragmentation has produced procedural complexity in two specific areas, authorized-agent intake and (where applicable) consumer appeals, that consumers otherwise must navigate by emailing generic privacy contact addresses. Effective privacy policies surface these procedures directly: a dedicated authorized-agent section setting out who may submit, what documentation is required (and not required) for verification, where to direct the submission, the applicable timeline, and the expected response; and, where applicable, a dedicated appeals section setting out the appeal process and decision points. This pattern converts opaque downstream processes into foreseeable consumer-facing ones, reducing the response-time and effort burdens that otherwise fall on consumers.

E. **Device- and platform-specific opt-out guidance in CTV contexts.** In the CTV context, effective consumer-facing disclosures provide device- and platform-specific opt-out instructions rather than relying on browser-centric privacy language. Such disclosures may appropriately link to supplementary resources, including NAI's device-specific consumer guidance updated in late 2025 to span web browsers, mobile devices, CTV, and streaming devices,[33] where those resources function as a supplement to the business's own statutory choice mechanisms rather than a substitute. CTV consumers otherwise face a notice environment built for browsers, with limited access to choice resources tailored to the device they are using.

F. **Privacy policy navigability**. Effective privacy notices are mindful of the consumer's path through the privacy policy itself, where the 2025 Privacy Review surfaced practical navigability factors that materially affect whether a consumer reaches the disclosure that applies: descriptive section headings, a functioning table of contents, a current "last updated" date, working in-policy hyperlinks, and content organization that does not require the consumer to scroll past extensive content that may be less relevant to reach, *e.g.*, rights and choice mechanisms.

These examples are illustrative rather than exhaustive. NAI's 2025 Privacy Review cycle has surfaced additional implementations across the ecosystem, and the NAI would welcome the opportunity to share further detail at the agency's request.

Q7. ***What else should CalPrivacy consider regarding CCPA notice and disclosure requirements?***

Consumer notice fatigue can arise from too many notices, particularly when they are presented or linked to in the same place. This is a risk when companies present many disclosure links in the website footnote even where each individual disclosure link is compliant. This is challenging because businesses today face a growing array of those obligations: the CCPA, the consumer-privacy laws of many other states, industry opt-out tool referrals, cookie-consent notices, sensitive-data-use disclosures, and state-specific consumer-rights content within the privacy policy itself. The corresponding links and sections often serve similar purposes under different

---

[32] *In re Am. Honda Motor Co.*, Stipulated Final Order ¶ 60 (Cal. Priv. Prot. Agency Mar. 7, 2025), https://cppa.ca.gov/regulations/pdf/20250307_hmc_order.pdf; *see also* Annual Report, *supra note 3*, § III.b.ii — Symmetry in Choice & Design, at 26.

[33] *See* Network Advertising Initiative, *How to Opt Out*, https://thenai.org/how-to-opt-out/ (last visited May 20, 2026) (providing device-specific opt-out instructions spanning web browsers, mobile devices, and TVs & streaming devices).

headings: "Your Privacy Choices" and "Your Ad Choices"; "Notice at Collection" and "Privacy Notice"; "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information"; California-rights language alongside parallel content for other states. NAI has previously urged CalPrivacy to apply a streamlining principle to overlapping notice architectures in adjacent CalPrivacy rulemaking, including in NAI's 2025 comments on the Automated Decisionmaking Technology (ADMT) regulations;[34] the same principle remains relevant for the notice-architecture concerns considered here.

The NAI offers three recommendations to reduce the risk notice fatigue without weakening any substantive disclosure obligation, each explained in more detail below:

- Clarify that businesses should not present additional links, referrals, or other disclosures likely to mislead or confuse consumers about how to exercise their CCPA rights.
- Establish a voluntary "Alternative Notice Link" modeled on the existing Alternative Opt-out Link, consolidating the Notice at Collection and the privacy-policy access path at the point of collection.
- Recognize IP-based location as a permissible basis for delivering state-tailored privacy notices at initial notice presentation, without prescribing detailed implementation rules.

A. CalPrivacy should clarify that businesses should not present additional links, referrals, or other disclosures likely to mislead or confuse consumers about how to exercise their CCPA rights

The CCPA's prominence requirements for homepage links set a standard for the consumer's initial routing to disclosures at the moment at which the consumer decides which link to click to begin exercising a CCPA right.[35]

However, the prominence of CCPA-required links may be degraded when the homepage footer (or other consumer-facing surface) presents too many additional links, referrals, or disclosures alongside the operative CCPA links in ways that may confuse consumers about which link delivers the CCPA-required functionality. The consumer may select a link that does not deliver the desired

[34] *See* Network Advertising Initiative, *Comments on CCPA Updates* (June 2, 2025), at 2, https://thenai.org/wp-content/uploads/2025/06/NAI-Comment-on-CCPA-Updates-6.2.2025.docx.pdf [hereinafter *NAI ADMT Comments*].
[35] *See* Cal. Civ. Code § 1798.135(a); Cal. Code Regs. tit. 11, § 7011(d); *id.* § 7013(c).

result and walk away believing the right has been exercised when it has not. Recent CalPrivacy and California Attorney General enforcement reflects the risk.[36] [37]

To address this risk, the NAI recommends that CalPrivacy adopt the following standard directly in regulation:

> *A business shall not present additional links, referrals, or other disclosures in a manner reasonably likely to confuse or mislead consumers into believing they have exercised a CCPA right or have been provided with a CCPA-required disclosure when they have not been.*

Adopting this language in regulation would clarify a principle articulated through enforcement and promote a more uniform standard businesses can implement, reducing reliance on case-by-case enforcement to address the same recurring design risk. It would also benefit consumers by requiring businesses to consider whether too many additional links may confuse or mislead consumers.

B. CalPrivacy should establish a voluntary "Alternative Notice Link" modeled on the existing Alternative Opt-out Link

The CCPA already recognizes that closely related disclosure links can be consolidated into a single, clearly-labeled link or mechanism. The existing Alternative Opt-out Link implements this for choice: a business may, in lieu of posting separate Notice of Right to Opt-out and Notice of Right to Limit links, post a single Alternative Opt-out Link titled "Your Privacy Choices" or "Your California Privacy Choices," paired with a standardized icon.[38] The Alternative Opt-out Link is voluntary; adopting businesses gain an approved form of consolidated link presentation, and consumers gain a consistent, recognizable point of entry. CalPrivacy has applied the same consolidation principle in the Automated Decisionmaking Technology ("ADMT") context, accepting that the ADMT pre-use notice may be presented as part of the existing Notice at Collection.[39] The same concept can be applied to the disclosures consumers encounter at the point of collection.

---

[36] *In re 2080 Media, Inc. d/b/a PlayOn Sports*, Stipulated Final Order ¶ 47 (Cal. Priv. Prot. Agency Feb. 27, 2026), https://privacy.ca.gov/wp-content/uploads/sites/357/2026/03/Order-of-Decision_PlayOn_Enforcement.pdf (concluding that a business "failed in its responsibility to provide a method for opting out of the Sale/Sharing of Personal Information by certain Tracking Technologies and instead stated in its privacy policy that Consumers should opt-out directly with third parties via the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA)"). The NAI publicly recognized the principle the *PlayOn* order applies shortly after the order was announced, *see* NAI, *Statement from NAI President & CEO Leigh Freund on the CalPrivacy Settlement with PlayOn Sports* (Mar. 3, 2026), https://thenai.org/press/statement-from-nai-president-ceo-leigh-freund-on-the-calprivacy-settlement-with-playon-sports-decision/. Well before *PlayOn* was announced in September 2025, the NAI had sunset its legacy industry opt-out infrastructure to align its consumer-facing resources with the CCPA's business-level opt-out architecture.

[37] *People v. The Walt Disney Co.*, Final Judgment and Permanent Injunction ¶¶ 26(e), 29 (Cal. Super. Ct., L.A. Cnty., Feb. 11, 2026), https://oag.ca.gov/system/files/attachments/press-docs/CA_SUP_LAX_26STCV04425__Final_Judgment_and_Permanent_Injunction.pdf (¶ 29 enjoining "language and choice architecture likely to confuse or deceive CONSUMERS"; ¶ 26(e) requiring opt-out notices not require consumers to "unnecessarily search or scroll through text" or use "hard-to-find-links, unlabeled carets, arrows, or other hidden menu icons").

[38] Cal. Code Regs. tit. 11, § 7015(a)–(b).

[39] *Id.* § 7220(a); *NAI ADMT Comments*, *supra* note 34.

The existing Notice at Collection regulations already permit a business to satisfy the obligation by linking directly to the section of the privacy policy that contains the required content.[40] In practice, businesses using that deep-link approach often still present a second, adjacent privacy-policy link at the same collection interface, because the existing regulations do not address the relationship between using deep-linking to present the notice at collection and the general privacy-policy accessibility requirement.[41] The result in those cases is a consumer being presented with two links to reach the same disclosure: the same structural concern the Alternative Opt-out Link already addresses on the choice side.

To address this issue, the NAI recommends that CalPrivacy establish a voluntary Alternative Notice Link, modeled on the existing Alternative Opt-out Link, as follows:

> *A business may, in lieu of posting separate links to a Notice at Collection and to the business's privacy policy, post a single, clearlylabeled link that directs the consumer to the section of the business's privacy policy containing the required Notice at Collection content. The linked section must include a conspicuous same-page control, persistent navigation element, or immediately adjacent link allowing the consumer to access the full privacy policy. The single link shall use a standardized title (for example, "Notice at Collection & Privacy Policy") and may be paired with a standardized icon, in a form CalPrivacy may specify. Where a business uses the Alternative Notice Link consistent with this section, no separate general privacy-policy link is required.*

The recommendation does not reduce the substantive content of CCPA disclosures; the required Notice at Collection content elements all remain. It addresses only the link architecture by which the consumer reaches those elements.

C. CalPrivacy should recognize IP-based location for delivering state-tailored privacy notices at initial notice presentation

State-tailored notice presentation can streamline a consumer's path to the operative rights without changing the substantive disclosures. In many cases, privacy policies have grown into long, structurally complex documents that combine general descriptions of a business's information practices with discrete sections tailored to the California consumer-privacy regime and, increasingly, to those of other states. A consumer reaching the policy through a single conspicuous link encounters substantial content that may not apply to the consumer's actual state of residence, lengthening the document and increasing the cognitive load of identifying the operative rights. Some businesses, in response, deliver state-tailored privacy notices keyed to the state associated with the consumer's current connection, a positive streamlining response to a real consumer burden observed across the NAI's 2025 Privacy Review.

However, state-tailored delivery or privacy disclosures requires a workable way to estimate the state associated with the consumer's current location. One practical mechanism is reference to the state associated with the site visitor's current IP address. While imperfect, use of IP address to estimate general location is an accepted industry practice, and has also been recognized as a valid approach in some circumstances by Minnesota. Minnesota's Consumer Data Privacy Act provides

[40] Cal. Code Regs. tit. 11, § 7012(f).
[41] *See id.* § 7011(d).

that "use of an Internet protocol address to estimate the consumer's location is sufficient to determine the consumer's residence."[42]

The NAI recommends that CalPrivacy establish a presumption (or a comparable form of recognition) that a business may use IP-based location estimation to estimate the state associated with the consumer's current connection for the purpose of selecting which state-tailored privacy notice to present at initial notice presentation. This presumption should anticipate and account for businesses accommodating consumers whose IP location does not correspond to their actual state of residence (for example, VPN users or consumers traveling), so long as those businesses make routing to other state disclosures available to the consumer as needed.

III. Employee Data

Scoping note: The NAI's Privacy Review Program focuses on consumer-facing practices in the digital advertising ecosystem. The NAI does not review member companies' HR practices. The NAI provides a response to Q6 (service-provider and contractor oversight) below because that question has broader applicability and draws directly on NAI's adtech-vendor-oversight experience.

Q1. ***Expectations or concerns about why businesses collect, use, disclose, or retain personal information as a job applicant or employee?***

N/A

Q2. ***Have you received a copy of a business's privacy policy, Notice at Collection, or CCPA rights' notices as a job applicant or employee?***

N/A

Q3. ***What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?***

N/A

Q4. ***Have you exercised your CCPA rights as a job applicant or employee?***

N/A

Q5. ***What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights?***

N/A

Q6. ***What steps do businesses take to oversee their service providers' and contractors' CCPA compliance, and what challenges do businesses face when doing so? For example, do businesses conduct audits of these entities or test the service provider's or contractor's systems? How effective are these audits and tests to assess a service provider's or contractor's CCPA compliance?***

NAI's Privacy Review program does not examine member companies' HR practices, and we leave most of this question to commenters with HR-vendor administration expertise. We offer two observations.

[42] Minn. Stat. § 325M.14, subd. 3(a)(5) (2025).

A. **Vendor oversight under the CCPA is risk-based by design.**

The CCPA service-provider regulation requires the contract to grant the business the right to take "reasonable and appropriate steps" to ensure CCPA-consistent use of personal information, and identifies a permissive, non-exhaustive menu (manual reviews, automated scans, internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months) among the steps those rights "may include."[43] What is reasonable and appropriate depends on the sensitivity of the data, the processing role, the controls already in place at the vendor, and the scalability of testing across different kinds of vendors.

B. **The employee-data context is particularly sensitive and is not representative.**

Employee-data processing implicates workplace power asymmetries and decisions affecting employment opportunities, compensation, benefits, discipline, and termination. Vendor-oversight calibration appropriate to that context may not reflect what "reasonable and appropriate" oversight requires across other CCPA contexts, including the ad-tech ecosystem, where processing roles, data sensitivity, contractual controls, and technical access points differ materially.

The NAI encourages CalPrivacy to consider these distinctions when considering regulations applicable to the employee data context and address vendor-oversight standards of general application separately.

Q7. ***What else should CalPrivacy consider regarding CCPA requirements for job applicants and workers in the employment lifecycle?***

N/A

IV. Conclusion

The NAI appreciates the opportunity to engage with CalPrivacy on these questions. Our recommendations are offered in service of notices and disclosures that are clear, comprehensible, and useful to consumers, supported by clear and reasonable expectations of businesses delivered through regulation, model notices, and examples in the regulations. The NAI stands ready to provide additional information and to continue engaging with CalPrivacy on the regulatory landscape under the CCPA.

Respectfully submitted,

Tony Ficarrotta

Vice President, General Counsel

The NAI

tony@networkadvertising.org

[43] Cal. Code Regs. tit. 11, § 7051(a)(6).

Appendix A: Sample Form Notice at Collection*

NOTICE AT COLLECTION · CALIFORNIA CONSUMER PRIVACY ACT

Notice at Collection of Personal Information

[Business Name] · Effective [date] · 11 Cal. Code Regs. § 7012

California law requires us to tell you, **at or before we collect your personal information**, what we collect, why, whether we sell or share it, and how long we keep it. The table below covers each category of personal information we collect about California consumers.

§ 7012(G) This notice describes collection by **[Business Name]** and, where applicable, by third parties that control collection on this site or app. Where provided jointly with another business, it describes their collective practices.

Look across each row to see what we collect, why we use it, whether we sell or share it, and how long we keep it.

Categories of Personal Information *types we collect about you* § 7012(e)(1)	**Purposes of Use** *why we collect & how we use it* § 7012(e)(2)	**Do we sell this category?** *for money or other valuable consideration* § 7012(e)(3)	**Do we share this category for cross-context behavioral advertising?** *shared for ads*	**Retention** *how long we keep it* § 7012(e)(4)
Identifiers Browser cookies; mobile advertising IDs (IDFA / AAID); hashed user identifiers.	• Ad delivery • Performance measurement • Cross-context behavioral advertising • Fraud prevention & security • Legal compliance	[Yes / No]	[Yes / No]	**Cookies:** [period] or until reset by consumer **IDFA/AAID:** [period] or until reset by consumer **Hashed IDs:** [period] from collection
Internet or other electronic network activity URLs visited; ad interactions; device signals.	• [Purposes specific to this category]	[Yes / No]	[Yes / No]	[Period or criteria]
Sensitive personal information *(if collected)* List each SPI category collected — e.g., precise geolocation; account log-in credentials; contents of communications; government identifiers; racial or ethnic origin; health information; biometric information.	• [Business's actual purposes for collecting and using this SPI]	[Yes / No]	[Yes / No]	[Period or criteria]

Your choices under the CCPA		
Opt out of sale and sharing § 1798.120 / § 1798.135	*Include if any category is sold or shared*	[Link to Notice of Right to Opt-Out]
Limit use of sensitive personal information § 7027 Applies only when our purposes for SPI go beyond those permitted by § 7027(m).	*Include if SPI is used or disclosed beyond § 7027(m)*	[Link to Notice of Right to Limit]
Read our full privacy policy § 7011	**Always include**	[Link to Privacy Policy]
Questions? Contact us at [email] or [postal address].		

[Business Name] Notice at Collection 11 Cal. Code Regs. § 7012(e), (g) Page 1 of 1

* Produced with assistance from generative AI tools.

CCPA is great but it has no impact at all because of loop holes same as AB5 law commerce/online people to do cross marketing. It is mainly used by recruiters, T To steal way more personal information.

Based on internet regarding how to solve issues,
1. All companies must be covered as part of this initiatives, not just bigger firms smaller firms to do dirty games or ask smaller firms to use AI and do dirty game

2. Recruiters must have license number same as loan officers and all the details r of job posting itself. Accuracy of any job posting on any platform must be recru on recruiter only not job applicant. Recruiter must make sure if they post job for and all other mandatory details for CA not generalized remote and entire USA. E application then they must post details with CA privacy requirement not just rem location saying USA. Recruiter must share all the details upfront or take permiss applicant's data including but not limited to system, location. Who has access to when and what data accessed must be shared with the applicant by default not afl

3. By Default every user's data must be deleted within 15 days of last conversati working with recruiter, so recruiter must delete user's data within 15 days (all th vendors/ sub vendors - no exception at all). If user wants, user can ask for extens or assume that user wants data to be stored. Data storage approval must not exce default rule must apply to all industry / all employers.

4. There is no easy anonymous tips submission mechanism at all. Simple online breaching company's' detail. Enforcement must be done within 15 days, not lifel

5. Penalties must be meaningful not just fig leaf type like $10 each violation. It n bigger firms and smaller firms must pay heavy fine or license terminated.

6. Any company not maintaining 1 to 5 ration in IT department, must face manda them. Meaning 5 US citizens only 1 Temp worker allowed. Offshore and all tem considered as part to 5 to 1 ratio. Most game of Privacy breach happen using thes offshore. AI must not be excuse for privacy breach and must not replace 5 to 1 ra

8. Privacy breached using AI tools, must have 10 times more penalty then norma term.

Loop holes like AB5 which purposely exclude engineers and doctors from indep even janitor is considered as cleaning engineer by design. This is just game. Fix t otherwise it will have no impact.

California Privacy Protecti

MAY 2 0 20

Received
Sac Mailroom

CCPA is great but it has no impact at all because of loop holes same as AB5 law. Privacy is breached not only by e-commerce/online people to do cross marketing. It is mainly used by recruiters, Tax preparer, Mortgage firms etc... To steal way more personal information.

Based on internet regarding how to solve issues,
1. All companies must be covered as part of this initiatives, not just bigger firms as these days bigger firms uses smaller firms to do dirty games or ask smaller firms to use AI and do dirty games.

2. Recruiters must have license number same as loan officers and all the details must be posted up front at the time of job posting itself. Accuracy of any job posting on any platform must be recruiter responsibility. Burden of proof on recruiter only not job applicant. Recruiter must make sure if they post job for CA, they must include wage range and all other mandatory details for CA not generalized remote and entire USA. Basically if CA person is eligible for application then they must post details with CA privacy requirement not just remote and no privacy based on location saying USA. Recruiter must share all the details upfront or rake permission with whom they share applicant's data including but not limited to system, location. Who has access to those systems, who accessed data, when and what data accessed must be shared with the applicant by default not after request made.

3. By Default every user's data must be deleted within 15 days of last conversation of intent. Let's say you are working with recruiter, so recruiter must delete user's data within 15 days (all the systems including offshore vendors/ sub vendors - no exception at all). If user wants, user can ask for extension but company must not initiate or assume that user wants data to be stored. Data storage approval must not exceed more than 15 days. This 15 days default rule must apply to all industry / all employers.

4. There is no easy anonymous tips submission mechanism at all. Simple online form must be available to submit breaching company's' detail. Enforcement must be done within 15 days, not lifelong.

5. Penalties must be meaningful not just fig leaf type like $10 each violation. It must be criminal or jail term for bigger firms and smaller firms must pay heavy fine or license terminated.

6. Any company not maintaining 1 to 5 ration in IT department, must face mandatory twice a year audit paid by them. Meaning 5 US citizens only 1 Temp worker allowed. Offshore and all temp work visa (any non US citizen) considered as part to 5 to 1 ratio. Most game of Privacy breach happen using these temp work visa folks and offshore. AI must not be excuse for privacy breach and must not replace 5 to 1 ratio.

8. Privacy breached using AI tools, must have 10 times more penalty then normal ones, including executives jail term.

Loop holes like AB5 which purposely exclude engineers and doctors from independent contractor rule. These days even janitor is considered as cleaning engineer by design. This is just game. Fix the system without any exceptions otherwise it will have no impact.

California Privacy Protection Agency
MAY 2 0 2026
Received
Sac Mailroom

Catbagan, Christian@CPPA

From: Curtis, Laura E <laura.curtis@apci.org>
Sent: Wednesday, May 20, 2026 3:14 PM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: APCIA - CalPrivacy Comment Letter_May 2026 (5.20.26).pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

On behalf of the American Property Casualty Insurance Association ("APCIA") and our members, thank you for the opportunity to provide these comments in response to the California Privacy Protection Agency's Preliminary Comment - Notices & Disclosures and Employee Data April 2026. We look forward to engaging with you and your staff. We would appreciate it if you could kindly confirm receipt at your convenience.

Thank you!
Laura

Laura Curtis
Assistant Vice President, State Government Relations (AZ & CA)
American Property Casualty Insurance Association (APCIA)
[redacted] (cell)
laura.curtis@apci.org

May 20, 2026

Sent via email to the California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
400 R St., Suite 350
Sacramento, CA 95811
regulations@cppa.ca.gov

RE: Preliminary Comment - Notices & Disclosures and Employee Data April 2026

On behalf of the American Property Casualty Insurance Association ("APCIA")[1] and our members, thank you for the opportunity to provide comments in response to the California Consumer Privacy Agency's ("CalPrivacy" or "Agency") regulations addressing notices and disclosures and employee data.

APCIA respectfully offers several guiding principles for the Agency's consideration. Effective regulation should: (1) prioritize consumer comprehension over the volume or granularity of disclosures, (2) preserve flexibility across a wide range of business models and technological contexts, and (3) promote regulatory stability so that companies can focus on enhancing user experience rather than continually reengineering compliance frameworks. Our comments are intended to help CalPrivacy further these principles as you move forward in this proceeding.

Notices and Disclosures

APCIA encourages CalPrivacy to prioritize simplicity, brevity, and usability in notices and disclosures. Consumers consistently struggle to read lengthy and complex privacy policies, and a "less is more" approach better serves their needs. Disclosure requirements should focus on key, decision-relevant information, including general categories of personal information collected, categories of third parties receiving the data, core uses of the data, and whether business may sell the personal information to third parties. Overly detailed or prescriptive requirements can undermine comprehension by leading to increasingly complex disclosures, discouraging consumer understanding and engagement. To that end, CalPrivacy should consider a concise, standardized safe harbor disclosure that businesses may elect to use, similar to the CFPB's Model Privacy Form.

The Agency should also avoid requiring statutory terminology in consumer-facing disclosures. Legalistic or technical terms often confuse consumers and reduce clarity. Allowing plain-language

[1] APCIA is the primary national trade association for home, auto, and business insurers.

descriptions, and revisiting requirements to use specific statutory category labels, would improve usability without diminishing transparency.

Regulatory stability is equally important. Repeated changes to disclosure requirements have forced businesses to frequently revise notices, diverting resources from improving clarity and the consumer experience to focus more on mere compliance. More stable requirements focused on providing consumers information they need rather than whether a company uses specific terminology would enable better-designed, more consistent disclosures over time.

CalPrivacy should also adopt a flexible, technology-neutral approach to notice delivery. Consumers engage across a wide range of platforms, including mobile applications and connected devices that may not support traditional web-based notices. Regulations should support contextual, layered, and just-in-time notices, while allowing businesses to tailor delivery to the relevant interface. Similarly, requirements for opt-out links and related disclosures should emphasize functional equivalence rather than identical presentation across platforms, recognizing differing technical capabilities and different ways that consumers interact with technology.

Finally, both research and experience demonstrate that lengthy, granular privacy policies are ineffective, and additional summaries do not necessarily improve comprehension. Short, clear, and focused disclosures are more likely to be read and understood. The Agency should ensure its rules do not incentivize over-disclosure at the expense of usability.

Employee Data

The same principles of clarity, brevity, and usability should guide requirements in the employment context. Notices to job applicants, employees, and contractors are most effective when they are concise, easy to understand, and delivered at appropriate stages of the employment lifecycle.

Employers face distinct operational and legal challenges, including managing multiple HR systems, coordinating with service providers, and complying with legal obligations that require collecting and retaining employee and job applicant data. Simplifying and streamlining notice requirements would improve both compliance and employee understanding.

The exercise of CCPA's privacy rights in the employment context also presents novel complexities that are not always present in traditional consumer interactions. Employers must balance these rights with other legal obligations, as well as the need to preserve investigations, fraud prevention efforts, and workplace safety. Regulations should recognize these realities and provide appropriate flexibility.

APCIA also urges the Agency to avoid overly prescriptive compliance requirements, particularly with respect to oversight of service providers and contractors. APCIA members employ risk-based approaches that prioritize higher-risk activities and allocate resources efficiently. One-size-fits-all audit or testing mandates could undermine these approaches and limit effective risk management.

With respect to data retention, regulations should clearly permit employers to retain personal information for the full duration necessary to meet legal obligations, including applicable statutes of limitation. Employers must maintain records for employment, tax, benefits, and potential claims purposes, and clarity in this area is essential.

Finally, CalPrivacy should consider the broader impact of burdensome requirements. Excessively prescriptive rules may create disincentives to hire in California or expand operations involving California workers. Aligning requirements with practical business realities is particularly important for employers operating across multiple jurisdictions.

Conclusion

APCIA appreciates the Agency's consideration of these issues. Across both notices and employee data, CalPrivacy should prioritize clarity over comprehensiveness, flexibility over prescriptiveness, and stability over continual regulatory change. APCIA welcomes further engagement as the Agency's work progresses.

Respectfully submitted,

Laura Curtis
Vice President, State Government Relations

Catbagan, Christian@CPPA

From: Price, Aliyah N. <aliyah.price@faegredrinker.com>
Sent: Wednesday, May 20, 2026 4:03 PM
To: Regulations@CPPA
Cc: Abrahamson, Reed
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: FINAL IPMPC Response to CalPrivacy Disclosures and Employee Data Rulemaking [05202026].pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

Attached, please find comments from the International Pharmaceutical & Medical Device Privacy Consortium (IPMPC) in response to the invitation for preliminary comments on notices and disclosures and employee data.

Thank you for considering our comments and recommendations. If you have any questions, you may contact us at www.ipmpc.org.

Sincerely,

Aliyah N. Price
Associate
Pronouns: she/her/hers
aliyah.price@faegredrinker.com
Connect: vCard

+1 202 230 5138 direct

Faegre Drinker Biddle & Reath LLP
1500 K Street, N.W., Ste. 1100
Washington, DC 20005, USA

IPMPC
International Pharmaceutical & Medical Device Privacy Consortium

May 20, 2026

By electronic submission:
California Privacy Protection Agency
Attn: Legal Division – Regulations
400 R St., Suite 350
Sacramento, California 95811

Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026

The International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC") welcomes the opportunity to provide comments in response to the request from the California Privacy Protection Agency (the "Agency") for comment on potential regulatory changes related to notices and disclosures and employee data.

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical and medical-device manufacturers. The IPMPC is the leading voice in the global pharmaceutical and medical device industry to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[1]

We thank the Agency for the opportunity to comment and provide recommendations on whether changes to the California Consumer Privacy Act ("CCPA") regulations related to notices and disclosures and employee data are needed.

Our specific comments follow.

I. Notices and Disclosures

4. What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights? For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?

Effective mechanisms for providing notice to consumers of their CCPA rights and how to exercise them should be contextual, timely, and actionable. This means that notices should be delivered where a consumer is making a choice and provide a simple way for the consumer to exercise their rights. Effective approaches for interfaces that do not support traditional webpage-based notices include:

- Layered notices, where a short summary with key information about a business's privacy practices is provided alongside a link or QR code to full details;

[1] More information about the IPMPC is available at https://www.ipmpc.org. These comments reflect the position of the IPMPC as an organization and should not be construed as the positions of any individual member.

- Just-in-time pop-ups at the point of personal information collection, such as when enabling analytics, location services, or creating an account;
- Standardized privacy icons or labels that highlight key uses like sale or sharing of personal information or the collection of sensitive personal information; and
- Persistent entry points, such as footer links, or in-app settings, which allow users ongoing access and control.

5. What challenges do businesses face when providing notices, including opt-out links, across different devices or platforms? How can the regulations address this issue?

The regulations should take into account the challenges businesses face when providing notices, including opt out links, across devices and platforms other than traditional web-based platforms. Specifically, we ask the Agency to allow the use of "equivalent alternatives" in situations where a direct clickable link is not technically feasible, such as providing a settings path, QR code, or companion app to facilitate notice and opt-outs.

Life sciences companies interact with consumers and patients in a number of ways that are specific to the industry. For example, the primary interaction that some life sciences companies may have with patients is through a medical or other connected device. These devices may not be developed in a way that privacy notices or opt-out links can be easily provided to the consumer (for example, they may lack screens sized to support large amounts of text or may not have features to support user input). Thus, to comply with the current CCPA regulations, life science companies must find alternative means of providing the required notices and disclosures to consumers that are not always efficient or cost effective. This results in an increased cost for the business which in turn results in an increased cost for the consumer. It also requires some businesses to collect more personal information than they ordinarily would (for example, mailing addresses to provide a notice by mail) to be able to deliver notices to consumers.

Moreover, we ask the Agency to consider revising the regulations to (i) clarify what it means to "honor" an opt-out across different identifiers, distinguishing between device or browser, and account-level choices, and specify when account-level prompts are permissible and (ii) allow flexibility for multi-step paths as long as such paths are clear and not burdensome. There are a variety of identifiers, such as browser cookies, mobile advertising IDs, device IDs, or account credentials that do not map cleanly to one person which makes providing appropriate notice or tracking opt-out preferences difficult. Signals like the Global Privacy Control (GPC) can be difficult to detect or honor consistently in mobile apps and connected devices.

Finally, the regulations could include reasonable grace periods for remediation when third-party technologies change to help businesses maintain compliance.

6. Please provide examples of effective consumer notices and disclosures. If possible, please provide information about specific testing, studies, or data demonstrating their effectiveness.

Notices and disclosures for consumers are most effective when they are provided in plain language. Thus, to assist businesses in providing consumers with effective notices and disclosures, the regulations could provide examples of what constitutes acceptable plain language.

In addition, layered privacy notices, drafted to present a short summary with key information, along with links to more detailed disclosures, have been shown to improve consumer comprehension compared to traditional long-form privacy policies. Just-in-time disclosures delivered at the point of personal information collection, such as when enabling cookies, turning on location services, submitting forms, enrolling in patient programs, or creating accounts, help ensure that consumers are provided adequate notice. Centralized "Privacy Centers" are also effective, as they provide a consolidated location where consumers can access all relevant notices and FAQs and submit rights requests. Additionally, user interfaces that offer consent choices through plain-language toggles and purpose-based categories (e.g., "Analytics" or "Personalized Advertising") along with clear explanations of the impact of each choice tend to be effective for providing notice and disclosure.

7. What else should CalPrivacy consider regarding CCPA notice and disclosure requirements?

We ask the Agency to consider the four following principles when considering if changes are necessary to the notice and disclosure requirements in the regulations.

Harmonization

Aligning CCPA notice obligations and requirements with other state and global privacy frameworks is important to reduce consumer confusion and compliance friction.

Practicality and Safe Harbors

The Agency should consider offering model language (such as appropriate plain language), optional standard tables, and safe harbors or grace periods for good-faith compliance, especially where practices are complex and rapidly evolving.

Accessibility

Accessibility expectations should be reinforced (e.g., readability on small screens, accessibility for consumers with disabilities), while still allowing flexibility for interfaces with technical constraints.

Change Management

The Agency should consider clarifying when and how consumers should be notified of material privacy policy changes (e.g., change logs, effective dates, or prominent notice for material changes) while avoiding policies that might lead to "notice fatigue" among consumers.

II. Employee Data

3. What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?

We ask the Agency to consider revising the regulations to expressly permit lifecycle-based, layered notices and privacy policies tailored to specific roles, such as applicant, employee, or alumni/offboarding instead of a single comprehensive privacy policy. Revisions to the regulations to clarify how detailed businesses must be when processing purposes are contingent (e.g., "as needed for investigations, compliance, and security") and examples for notices and disclosures related to monitoring, analytics, and workplace technologies would help businesses communicate more effectively with employees and job applicants and support compliance.

These changes to the regulations would address challenges businesses experience with respect to job applicants and employees. The volume and diversity of HR data sources (which include systems for HR information, payroll, benefits, learning management, security and badge access, IT monitoring, internal investigations, travel and expense tracking, diversity and inclusion initiatives, and health and safety programs) make providing a single clear and plain language privacy policy difficult. Moreover, the purposes for collecting and using this personal information also change throughout the employment lifecycle, making it hard to keep privacy policies accurate, relevant, and straightforward, despite businesses updating the policies annually. Many businesses also have global workforces and need notices and privacy policies that apply and comply with legal requirements across jurisdictions while remaining clear for California applicants and employees.

5. What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights? How can the regulations address this issue?

We ask the Agency to establish clearer, risk-based standards for verifying employee and applicant requests and to provide more explicit guidance on common exemptions and limitations of rights requests in the employment context (such as those related to investigations, security, or legal holds) and how to communicate those exemptions and limitations to employees and job applicants. These changes would address issues businesses encounter when providing job applicants and employees with the ability to exercise their privacy rights, as businesses encounter conflicts with other legal obligations, such as record retention requirements, tax and payroll regulations, litigation holds, and regulated industry requirements, as well as privileged workplace investigations which can make it difficult to know how and to what extent the business must comply with the request.

In addition, we ask the Agency to consider revising the regulations to allow partial fulfillment of job applicant and employee rights requests, with follow-up as more information becomes available. This would allow businesses to respond to rights requests in a more efficient and cost-effective manner, as businesses must search for responsive information across numerous HR and IT systems, as well as from multiple affiliates, service providers, and contractors.

6. What steps do businesses take to oversee their service providers' and contractors' CCPA compliance, and what challenges do businesses face when doing so? For example, do businesses conduct audits of these entities or test the service provider's or contractor's systems? How effective are these audits and tests to assess a service provider's or contractor's CCPA compliance?

We ask the Agency to clarify what constitutes "reasonable" oversight of vendors and service providers based on risk level. Specifically, the regulations should allow the use of group audits, independent audit reports, and standardized frameworks for compliant service provider and contractor oversite. Moreover, we ask the Agency to consider providing safe harbors when businesses implement appropriate contractual controls and monitoring, even if a service provider or contractor later fails to comply despite those measures.

One common method that businesses use to oversee service provider and contractor compliance is contractual controls; conducting due diligence on service providers' and contractors' privacy and security practices via the use of questionnaires and security and privacy assessments; and ongoing monitoring of service providers' and contractors' compliance through, for example, periodic attestations, and, where appropriate, targeted audits (such as SOC 2 reports, independent assessments, or penetration test summaries).

However, businesses face several key challenges in this oversight process. Scaling oversight across large vendor ecosystems can cause audit fatigue. Large vendors may have hundreds or thousands of customers. If regulations require businesses to audit their service providers and contractors, those large vendors will have to dedicate a significant amount of time and employee hours to conducting the audits for each of their customers. This increases expenses for the vendor, which in turn raises the cost of the products and services they provide to their customers, and ultimately results in increased costs for consumers.

Moreover, it is not always feasible for businesses to conduct audits of the service providers and contractors directly. For example, many businesses, particularly smaller businesses, may lack the expertise to be able to conduct audits of their service providers and contractors in a meaningful way. Thus, relying on independent audit reports (such as SOC 2 or ISO), contractual attestations, and targeted validation or testing for higher-risk vendors is a much more effective and efficient way for many businesses to oversee service provider and contractor compliance.

Conclusion and Contact Information

Thank you for considering our comments and recommendations. If you have any questions, you may contact us at http://www.ipmpc.org.

Catbagan, Christian@CPPA

From: Jennifer King PhD <kingjen@stanford.edu>
Sent: Wednesday, May 20, 2026 4:42 PM
To: Regulations@CPPA
Subject: Preliminary Comment - Notices & Disclosures and Employee Data April 2026
Attachments: JKing CPPA May 2026 comments.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Attached please find my submission to the notices and disclosures rule making.
Thanks,
Jen King

--

Jennifer King, Ph.D (she/her)
Privacy and Data Policy Fellow
Stanford Institute for Human-Centered Artificial Intelligence
hai.stanford.edu

https://hai.stanford.edu/people/jennifer-king
www.jenking.net/publications
Google Scholar profile: https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en

Stanford University
Human-Centered
Artificial Intelligence

To: CALIFORNIA PRIVACY PROTECTION AGENCY
400 R ST. SUITE 350
SACRAMENTO, CA 95811
Via email: regulations@ccpa.gov

May 20, 2026

To whom it may concern:

Thank you for the opportunity to submit comments on the topic of notices and disclosures to CalPrivacy. I submit the comments below on behalf of myself; they do not represent the views of HAI or Stanford University. These comments are based upon my twenty years of experience researching consumer data privacy issues, specifically the design of user interfaces and notices, including privacy policies.

I. Notices and Disclosures

1. When reviewing a privacy policy or similar disclosure, what is the most important information to consumers? What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?

Consumers are often comfortable disclosing personal information to a first party, particularly if the disclosure is contextually appropriate and appears necessary for the functioning of a digital service.[1] However, where consumer concern grows is when personal data is shared or

[1] King, J. (2018). Privacy, Disclosure, and Social Exchange Theory. UC Berkeley. ProQuest ID: King_berkeley_0028E_17901. Merritt ID: ark:/13030/m5t77dzd. Retrieved from https://escholarship.org/uc/item/5hw5w5c1

sold to third parties.[2] This is especially true when such practices are unclear or poorly disclosed to consumers. For example, Apple's decision to move its third party advertising tracking opt-outs from within the iPhone's settings to a top-level dialog window that users had to engage with upon installing and opening an app, adoption soared.[3]

While the CCPA did help improve how CCPA-related compliance information is presented within privacy policies, to the extent that companies now often present such information in a tabular format, the reality is few consumers will actually find that section of a privacy policy, let alone read it. Further, these disclosures are typically still buried within a much larger document, and in many cases consumers must scroll to find this information—assuming they know what they are looking for. In short, the "notice at collection" requirement is not tied to a consumer's actual experience of collection, as such notices are buried in privacy policies and not required reading.

It is certainly true that all of this could be improved. Apple's adoption of nutrition labels in their App Store makes it easier for consumers to scan an app's label to glean what data its developer collects.[4] The nutrition label style of presentation could potentially help outside the app store context if it were standardized, uniform, and easy to find on any website, similar to the food product nutrition labels that inspired this approach.[5] In short, if not left to choice. However, the labels would need to be unsparing in their approach and not minimize what companies are actually doing with consumers' data, which undoubtedly companies will resist.

Even with standardized labeling that accurately captures a company's data collection and processing practices, there remains no guarantee that such an approach will either change the behavior of companies or provide consumers with an actionable means to protect themselves. A core challenge is that consumers cannot negotiate with businesses over these practices; their options are to take it or leave it, and in many cases, they cannot opt out of

---

[2] Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park. "How Americans View Data Privacy." Pew Research Center, Oct. 18, 2023. Available at: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[3] Apple Inc. 2025. If an app asks to track your activity. https://support.apple.com/en-us/102420

[4] Gian Luca Scoccia, Marco Autili, Giovanni Stilo, and Paola Inverardi. 2022. An empirical study of privacy labels on the Apple iOS mobile app store. In Proceedings of the 9th IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft '22). Association for Computing Machinery, New York, NY, USA, 114–124.

[5] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10). Association for Computing Machinery, New York, NY, USA, 1573–1582.

using digital services, even if they find a business' practices objectionable. Without regulation curbing the most extreme forms of data collection (e.g., third party data collection without explicit consent), consumers may want to vote with their feet but may not find competitive options given a lack of regulatory pressure to prohibit the most exploitative data collection and use practices.

To that end, while improving the state of privacy disclosures through standardization and uniform design would be an improvement, it is likely to be marginal. Better, as I discuss in more depth below, would be to also require machine readable versions of privacy policies and CCPA-specific compliance data in order to allow third party developers to build tools to process and present this information to consumers in ways that they can more clearly understand and take action upon.

2. What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?

A one sized-fits all approach to privacy disclosures does not work for the public, due to significant variances in education levels, English fluency, technical fluency, age (including teens and children), to name a few variables. Multiple studies have documented the significant barriers presented by privacy policies written in legal language.[6]

Here are a few suggestions for CalPrivacy to consider to address this ongoing problem:

1. **Consumer-friendly version of CCPA policy**: require that companies produce a separate, consumer friendly version of their CCPA compliance information in a simple, easy to read format with multiple language versions available to meet the needs of the California public. Obviously more detail is needed than I provide here to define "simple" and "easy to read," but at minimum this would require a visual design that is easier to read than the large blocks of densely worded text common in the majority of privacy policies; written at a grade level that maps closely to the average reading level of the California public (e.g., high school); and is accessible for those with visual

[6] See generally: Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-scale readability analysis of privacy policies. In Proceedings of the International Conference on Web Intelligence (WI '17). Association for Computing Machinery, New York, NY, USA, 18–25.; Wagner, Isabel. "Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996--2021." arXiv preprint arXiv:2201.08739 (2022); Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., ... & Schaub, F. (2015). DISAGREEABLE PRIVACY POLICIES: MISMATCHES BETWEEN MEANING AND USERS'UNDERSTANDING. BERKELEY TECHNOLOGY LAW JOURNAL, 30, 1.

disabilities. Standardization remains important here as consumers should not be forced to navigate endless variations of policies, even if they are more consumer friendly.

2. **Machine-readable version of CCPA policy:** similar to the above, but in a machine readable format that can be customized by consumers using software that could translate it into appropriate languages, age-based or educational level-based reading formats. Machine-readable policies may also provide the infrastructure for consumer-focused AI powered tools, such as agents, to aid consumers with purchasing and disclosure choices by delegating one's policy preferences to an agentic tool.

It is important to note that while both of these approaches will improve transparency into businesses' data practices, they cannot be the singular basis by which consumers are provided more information. Meaning, that without educational supports and public outreach, only the most curious or better educated consumers may benefit from them. Finally, without actionable choices that can result from this knowledge, the result is likely to be *privacy resignation*[7]: a dislike or dissatisfaction with one's data privacy options but the sense that nothing can be changed. While there may be some product choices consumers can make based on their dislike of a business' data practices, there are unfortunately many others contexts where monopolistic practices, product lock-in, scaling effects, or simply a lack of businesses competing on privacy practices makes it difficult to impossible for consumers to choose a product or service that reflects their true preferences.

3. What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this Issue?

From a consumer and researcher perspective, businesses struggle to be transparent about their data practices because they don't want consumers to factor them into their decisionmaking. In the absence of a regulatory floor limiting or prohibiting certain practices, businesses engage in a race to the bottom, adopting practices such as third party data sales both to bolster income and because competitors are also engaged in the same. Similarly, businesses also maximize the data they collect from consumers because they do not want to lose a competitive advantage; this is especially true in this new era of artificial intelligence. Generally, consumers dislike these practices, and if clearly disclosed may seek alternatives or alter their disclosure behavior.

[7] Draper, Nora A., and Joseph Turow. "The corporate cultivation of digital resignation." *New media & society* 21, no. 8 (2019): 1824-1839.

Businesses also do not communicate longer term, downstream risks to consumers from the collection, processing, and sharing or selling of personal data. Case in point: in 2019, I published a portion of my dissertation research examining disclosure choices by early adopters of 23andMe, the genetic information service which has since suffered from a data breach as well as gone bankrupt.[8] The 23andMe customers I spoke with were generally unable to anticipate the future uses and risks of their genetic data after sharing it with the company. Instead, they were focused on the short-term benefits and the potential contributions their data made to the company's research projects. While a few customers evinced mild concern that a data break or hacking event could happen, most believed the company's promises in their security practices. In their sign-up process, the company did not fully disclose the possible risks in a way that consumers could concretely weigh and understand; to the extent that this was addressed at all, it was as fine print in their privacy policy and terms of service agreements. In sum, consumers are far more likely to engage in temporal discounting at the point of disclosure and are unable to anticipate future uses of their data. In particular, the companies that engage in more risky data practices, such as allowing third party collection and sharing or selling consumer data should be obligated to prominently highlight the future downstream risks from such activities.

4. What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights? For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?

Requiring businesses to provide machine readable privacy policies is one potential way to address this issue. Consumers could access a device's policy through a variety of means (e.g., QR codes, email, others), including prior to purchase, and use a purpose-built app to evaluate the data practices associated with the device. A combination of advocacy groups, foundations, and academic researchers could collaborate in building the infrastructure to support such an effort.

7. What else should CalPrivacy consider regarding CCPA notice and disclosure Requirements?

[8] Jennifer King. "*Becoming Part of Something Bigger": Direct to Consumer Genetic Testing, Privacy, and Personal Disclosure*. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 158 (November 2019), 33 pages.

It is important to acknowledge the large body of research over the past two decades that has focused on improving privacy policies and disclosures.[9] Much digital ink has already been spilled in this effort, and largely these recommendations have not been widely adopted. Meaning, there is still much that can still be tried that researchers have already developed and tested; reinventing the wheel is unnecessary. The solution I advocate for above—standardized machine readable privacy policies—is not novel and was first introduced in its basic form in 2000![10] I am advocating for this solution because with the advent of artificial intelligence, the internet is on the cusp of the most significant technological change in over thirty years. Specifically, the infrastructures that have powered the web until now are finally at the cusp of major change and the momentum and necessity to make fundamental transformations is here. But importantly, much of this research demonstrates, repeatedly, that static privacy policies posted on websites as a solution for consumer knowledge and consent are inherently flawed. CalPrivacy has an opportunity to push this space forward by requiring open technological solutions that support universal access and allow for the presentation of information, as well as the delegation of consent, using tools that can enforce consumers' own preferences and, perhaps eventually, negotiate the disclosure of personal data and the specific terms on their behalf.

Thank you for your time and consideration.

Sincerely,

Dr. Jennifer King
Privacy & Data Policy Fellow,
Stanford Institute for Human-Centered Artificial Intelligence

[9] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15). USENIX Association, USA, 1–17.
[10] https://www.w3.org/P3P/introduction.html