

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://coppa.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.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is written in a cursive style with a large, stylized 'M' and 'R'.

Morgan Reed
President
Association for Competitive Technology