WHAT BUSINESSES SHOULD DO RIGHT NOW AS CALIFORNIA FINALLY BEGINS TO ENFORCE CCPA

Greenberg Glusker

2049 Century Park East, Suite 2600
Los Angeles, CA 90067
GreenbergGlusker.com | 310-553-3610

What businesses should do right now as California finally begins to enforce CCPA

"Realistic painting of a California brown bear with fangs in Yosemite, standing in profile on red sand." Image generated through open-source packages.

Written by: Peter K. Jackson, CIPP/US, Counsel in Greenberg Glusker's Intellectual Property Group

Greenberg Glusker

California's privacy watchdog finally has fangs. So where will it clamp down?

Years of court challenges prevented California's privacy agency from enforcing its own regulations. That's over.[1] So where will the agency bite down first?

Here's what we think businesses should focus on immediately.[2] You can read about why we think these steps are crucial below.

To avoid acronym soup, this article uses shorthand defined in the glossary. These general recommendations assume some familiarity with CCPA[3] and don't reflect all the nuances and exceptions that may apply to a particular business. Consult a certified attorney or privacy professional to understand whether and how they map to your business. Onto the recommendations.

Eliminate barriers to opt-out and delete requests

- Just delete it. If a consumer asks your business to delete their information, do it. That includes requests routed through services like DeleteMe, which can absolutely serve as "authorized agents" under California law.

  » Yes, California law allows a business to verify a consumer's identity and an agent's authority to act on a consumer's behalf. But the watchdog's first enforcement bulletin targets unnecessarily burdensome verification practices.

  » For most businesses, it's simpler and easier to presume deletion is appropriate whenever a request can be matched to information the business maintains. Resort to verification only when there's real doubt.

- Few barriers are allowed.

  ✗ Remember, it's never okay to ask a consumer to create an account in order to exercise privacy rights—whether to delete their info or opt-out of targeted advertising.

---

[1] As of April 24, 2024, no uncertainty remains about whether the watchdog's regulations are currently enforceable. The tick-tock: A California trial court decision delayed the agency's enforcement of its regulations. An appellate court reversed, allowing enforcement of the watchdog's existing regulations as of April 1, 2024. A last-ditch appeal to the California Supreme Court foundered. After prolonging its period to decide whether to hear the appeal, the California Supreme Court denied the petition for review on April 24, 2024.

[2] This article is about CCPA, the consumer privacy law enacted and amended by California voters in recent elections—not the 1950s-era wiretapping statute known as CIPA. We described CIPA mitigation strategies here.

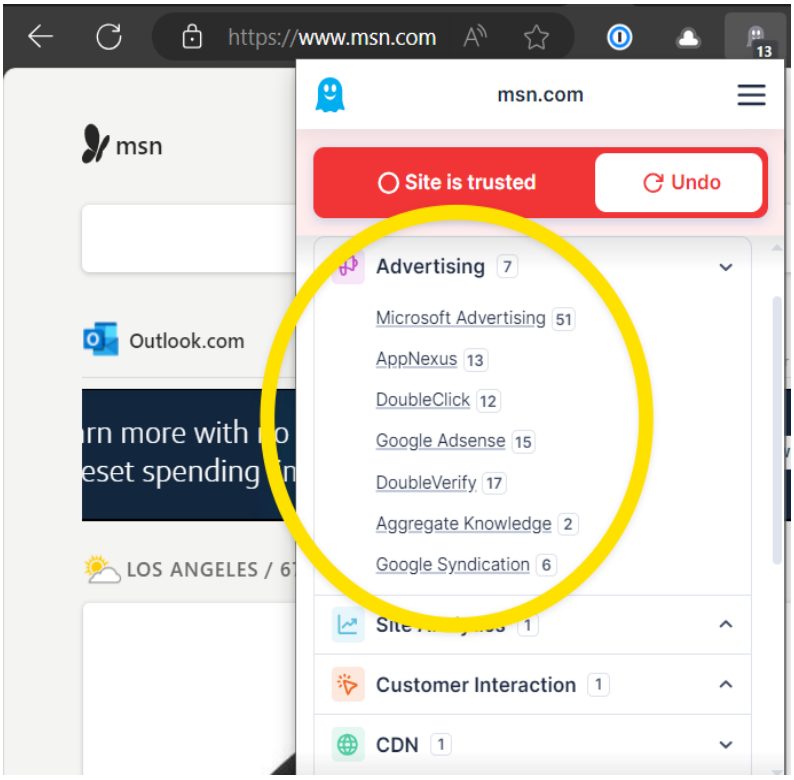
[3] As a reminder: California privacy law grants consumers rights they can exercise against any business which maintains their information. There are two main buckets. One is opt-out rights. These are forward-looking, and can easily be honored through across-the-userbase settings. The second bucket is control rights. These are backward-looking and involve information collected previously: the right to know (obligating you to disclose what you *know* about the consumer and, in general terms, how you've used that info), the right to correct (requiring you to update your records to *correct* any inaccuracies specified by the requesting consumer): the right to delete (requiring you to *delete* any information you maintain about the consumer)

✗ For requests to opt out of any 'sharing' or 'sale' or 'limit' the disclosure of sensitive info[4], asking for additional info is prohibited[5]. Making those requests one-click at most is a core purpose of California privacy law.

Make sure your tech supports—and honors—consumer preferences

Note: This step is only relevant if your business allows information collected through your online service[6] to flow to others for targeted-ad purposes. The ad industry, and now the law, call that "sharing".

» *Unsure if your business shares?* Browser extensions like Ghostery make it easy for anyone to know if a website employs common advertising tools. Beware false negatives—extensions may miscategorize some tools and don't examine actual data flows that may constitute sharing.



Screen capture of the Ghostery extension's scan of msn.com.

Implement GPC tech & an opt-out homepage link. To reiterate, these steps are required if your business allows information collected through your online service to flow to others for targeted-ad purposes. The ad industry, and now the law, call that "**sharing**".

[4] The right to 'limit' is only relevant if you collect sensitive info, like precise (GPS) locations, and disclose it for any purpose that is not necessary to provide what the goods or services the user requests, such as 'sharing' or selling.

[5] After honoring the opt-out request, a business may inform the consumer that opting-out affected preexisting individual settings and display an option to opt back in.

[6] California privacy law puts obligations on the "business" that controls the collection of information on a website or app. Those obligations attach regardless of whether information is collected by that business itself, or is collected by a third-party cookie or tool that business authorizes.

» Affected businesses must provide (1) opt-out responsiveness to Global Privacy Control (GPC) signals and (2) implement at least one other opt-out method. Turn off all sharing for users sending global opt-out signals.[7]

✗ *Your cookie banner or popup?*[8] *Probably not an acceptable method*. In fact, no U.S. laws require those. Most out-of-the-box solutions were designed with European privacy law[9] in mind. California's regulations, which came later, frame cookie banners as unacceptable[10] wherever they lack the verbiage and functionality required of opt-out methods by California privacy law.

The Guardian's CCPA-compliant cookie modal for California visitors at theguardian.com/us.

---

[7] Technically, CCPA requires businesses to honor any "global opt-out preference signal", not just GPC signals. However, GPC is the only signal that California regulators have specifically focused on for enforcement purposes. It's also the principal signal readily available to consumers through browser extensions and settings.

[8] A *banner* covers part of a website but doesn't prevent the user from navigating to other pages. A *modal* must be actioned by the user before the page behind it will be accessible. Many websites must use modals to comply with GDPR.

[9] The European GDPR regime requires user consent prior to *any* data collection that is not necessary to provide the requested service (i.e., a website). Users don't *need* ad trackers or benign tools like Google Analytics, Adobe Fonts and Zendesk. Allowing technologies like those to collect data from Europeans—even an IP address—is prohibited until the user gives opt-in consent. Thus the birth of the cookie modal industry. (GDPR principles are in effect across the EU, with specifics and priorities set by national regulators, such as France's CNIL and the Irish Data Protection Authority).

[10] Specifically:

> "A notification or tool regarding cookies, such as *a cookie banner or cookie controls, is not by itself an acceptable method* for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An *acceptable* method for submitting requests to opt-out of sale/sharing *must address the sale and sharing* of personal information." Cal. Code of Reg. § 7026(a)(4).

In other words, cookie controls tend to obfuscate the simple opt-out choices California requires. California privacy law focuses on whether your business shares user info with ad trackers—and specifies required methods you *must* use to allow opt-outs—and

- If you already deploy a banner or modal, tailor it[11]. Add prominent “do not sell or share” language favored by California privacy law to its cover screen. Make that link a one-click affair. You don’t need to ditch any out-of-the-box features, like a “manage perferences” link to toggles for specific categories of embedded technologies.

- While you’re customizing, add language and links to inform visitors that your user agreement (often ‘Terms of Service’ or ‘Terms of Use’) and privacy policy apply. Increased visibility can help defeat claims that hinge on visitors being unaware of your legal terms or privacy disclosures.[12]

» *Add a homepage ‘Do Not Share’ or ‘Your Privacy Choices’ link.* Online services need two opt-out methods. Processing GPC signals is always required, so that’s one. For the second, a homepage footer link is the smart choice.[13] Unless your business needs a sensitive data opt-out, we recommend the standard ‘Do No Sell or Share My” info link, which visually signals to consumers and regulators that your business has taken steps to comply with California privacy law.[14] Clicking the link should turn off all ‘sharing’ of data from the visitor for targeted-ad purposes, and notify the user that has happened. Here’s an example:

---

says that you must disclose what you collect. Realistically, a banner can’t communicate all of the disclosures required by California privacy law without linking to a separate document (like your privacy policy).

[11] Most businesses buy cookie banners from big vendors (like OneTrust), and many don’t use the right language out of the box. In most cases, the disclosure’s text and links can be customized for different jurisdictions, shown as applicable based on the user’s location.

[12] Always obtain actual *acceptance* when a visitor first establishes an ongoing relationship with your business, such as by creating an account or ordering products. You want to be able to show each user took an action to accept the legal terms and privacy disclosures, such as ticking

- *Sensitive data opt-outs*. This is less common. But, if you ever disclose "sensitive" information to outsiders who don't need it to provide the services users request, add a 'Your Privacy Choices' link (which must include the blue-toggle icon) instead. It should opt consumers out of both sale/sharing and unnecessary disclosure of sensitive info. Otherwise, you'll need both the 'Do Not Share' and a separate 'Limit the Use of Sensitive Info' link.[15]

- An example is allowing third-party video-players to receive users' precise (GPS) locations. The GPS coordinates, unlike a physical address, are "sensitive". Your business may need your customer's coordinates to route a courier to their location. Disclosing them to the courier is necessary; no opt-out required. But the website video player doesn't need GPS coordinates; at most, a general location would probably suffice.

Update stale privacy policies

If your privacy policy hasn't been updated in the last 18 months, it's probably out of date.

- Consumer privacy laws in other states have gone into effect in the last few years. If your policy doesn't extend privacy rights to residents in those states, it's stale. In the words of Connecticut's enforcement chief in April 2024, "companies that haven't updated their policies since our law passed can't be complying. It just is what it is."[16]

  - No other state gives consumers all the rights California does. All states extend most of them. For most business, treating all U.S. users as California residents is the easiest, most efficient approach. (Our DMs are open if you have questions.)

- Read your policy, even if it's relatively recent. Does it accurately describe the types of info you collect, how you use that data and what you disclose to outside businesses? More importantly, would a consumer understand those descriptions? If you can't, a consumer probably can't either. The watchdog's regulations see vague and jargon-heavy descriptions as problematic.

Gauge your risk profile

Expect targeted ads to remain in the crosshairs:

- California's first big enforcement push in 2022 focused on whether online businesses were honoring those global signals, namely Global Privacy Control. We expect the watchdog to pursue them just as much.

[15] For clarity, an independent 'Limit the Disclosure of my Sensitive Personal Information' link is not required where one link has both effects. Cal. Civ. Code § 1798.135(a)(3) ("the business [has] discretion [to] utilize a single, clearly labeled link on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that link easily allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information").

[16] Remarks of Michele Lucan, Connecticut Deputy Associate Attorney General/ Chief of the Privacy and Data Security Section, at IAPP Global Summit 2024 panel "Direct Insights from U.S. State Privacy Enforcers."

- *Why?* Global signals shift the opt-out burden from the consumer to businesses, in a move praised by privacy advocates. Instead of manually clicking the 'Do Not Share' option on every single website, a user with a global setting sends that opt-out request automatically just by visiting a webpage.

- In 2022, Sephora became the poster child for global-signal noncompliance.[17] Other e-commerce websites were targeted too, but escaped public fines by curing their noncompliance within 30 days. That grace period no longer exists; it was excised by the same amendment that created California's privacy watchdog.

Industry focuses:

- The *watchdog* has also publicly stated that it's focused on car companies and data collection from vehicles, just like many other regulatory bodies. Make compliance a high priority if your business obtains data collected by consumer vehicles or other sensors (like security cameras and other 'smart' devices).

Why take these steps?

Our hunches are grounded in the agency's guidance and public statements, as well as California privacy law in general. They reflect:

- The agency's April 2024 Enforcement Advisory, described in depth below.[18]

- Remarks by the agency's executive director and enforcement chief at separate sessions during the 2024 IAPP global summit in early April 2024.

- Discussions at the watchdog's public meetings.

- Enforcement proceedings, both those in the public record and otherwise.

Our recommendations also reflect the entirety of California's privacy law. California's privacy law weighs in at more than 50,000 words.[19] Much of its heft is devoted to allowing Californians to opt-out of targeted advertising, the practice of sharing user data with ad companies (Google and Facebook being the largest) so ads can pinpoint individual eyeballs.

April 2024 Enforcement Advisory

Our recommendations also reflect the watchdog's guidance "Applying Data Minimization to Consumer Requests" published April 2, 2024. Despite the title, the guidance (1) emphasizes certain concrete focuses in addition to (2) restates general, abstract principles without new commentary. Here's what its 2,400 words boil down to:

Concrete actions:

[17] See this PDF of the settlement or the California attorney general's press release.

[18] See this PDF (also available from the agency itself) and the discussion below

[19] The regulations expend approximately 26,222 words. The text of CCPA, as amended, clocks in at approximately 23,986.

- *Actioning consumer requests*:
  - Regulation section 7060(d) outlines that businesses should generally avoid requesting additional information for verification purposes unless necessary, and must delete any new information collected for verification as soon as practicable after processing the consumer's request.
  - Regulation section 7025(c)(2) stipulates that businesses should not require additional information beyond what is necessary to send an opt-out preference signal.
  - Under regulation section 7026(c), businesses must not require consumers to create an account or provide unnecessary information for requests to opt out of sale/sharing.
  - According to regulation section 7027(d), businesses must not ask for extra information when a consumer submits a request to limit the use or disclosure of sensitive information.
- *Preventative measures*:
  - Businesses are reminded to specifically address possible negative impacts on consumers through additional safeguards such as encryption or automatic deletion.

General principles:

- The foundational principle of data minimization in the CCPA that businesses collect information only to the extent necessary for the purposes for which it is collected. Businesses must apply the data minimization principle for each purpose they collect, use, retain, and share information.
- Use of a consumer's information must be reasonably necessary and proportionate to the purposes described at collection.

Glossary

- "**agency**" and "**watchdog**" both refer to the California Privacy Protection Agency, often referred to as CPPA.
- "**California privacy law**" is the California Consumer Privacy Act (or CCPA), as amended by the California Privacy Rights Act, and the regulations promulgated pursuant to CCPA. It doesn't include the 1950s-era wiretapping law known as the California Invasion of Privacy Act (CIPA).
- "**information**" and "**info**" refers to *personal information*, as defined in California privacy law.
- "**regulations**" refers to the regulations promulgated by the agency under California's privacy law. They form part of California's privacy law.

Greenberg Glusker

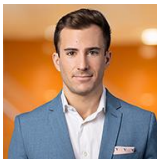
Cybersecurity and Privacy

Data is crucial for modern business, but legal regulations struggle to keep up with technological advances. We help clients navigate complex regulations, focusing on compliance, accountability, and risk control. Working with technology and IP experts, we offer practical, business-oriented solutions tailored to clients' objectives and priorities, emphasizing problem-solving and anticipation.

- We counsel clients on, among other topics, the European Union's GDPR law, as well as the California Consumer Privacy Act (CCPA).
- We also advise on more narrowly targeted sectoral statutes, such as the Children's Online Privacy and Protection Act, the Gramm–Leach–Bliley Act and Federal Trade Commission decisions. Depending on a client's situation and industry, more than one of these may be applicable.
- Our clients also receive guidance in best practices and government standards that may fall short of being legal requirements, but significantly affect potential liability.
- We are frequently called upon to review internal practices and data security requirements, in order to manage risk relating to vendors and customers.
- We draft both external and internal policies to ensure statutory compliance.
- We regularly conduct internal and forensic investigations in the event of a security breach. Working closely with technology partners, we can follow data almost anywhere and reconstruct what happened and why.
- We provide training to employees in privacy and data security procedures.
- We counsel clients on the purchase of cyber-insurance policies.
- Our clients operate across all forms of digital technologies such as cloud Software as a Service ("SaaS"), streaming entertainment, restaurants and hospitality, and e-commerce. We also counsel many professional services clients, including accounting firms, consultancies, and other law firms.

Greenberg Glusker Team

Tim Toohey



Peter Jackson

Alexis Anderson