Privacy Enforcement 2026

Where Regulators are Focusing — and Where Companies are Getting Caught

Frankfurt Kurnit Tech Law Summit

May 12, 2026

Daniel Goldberg

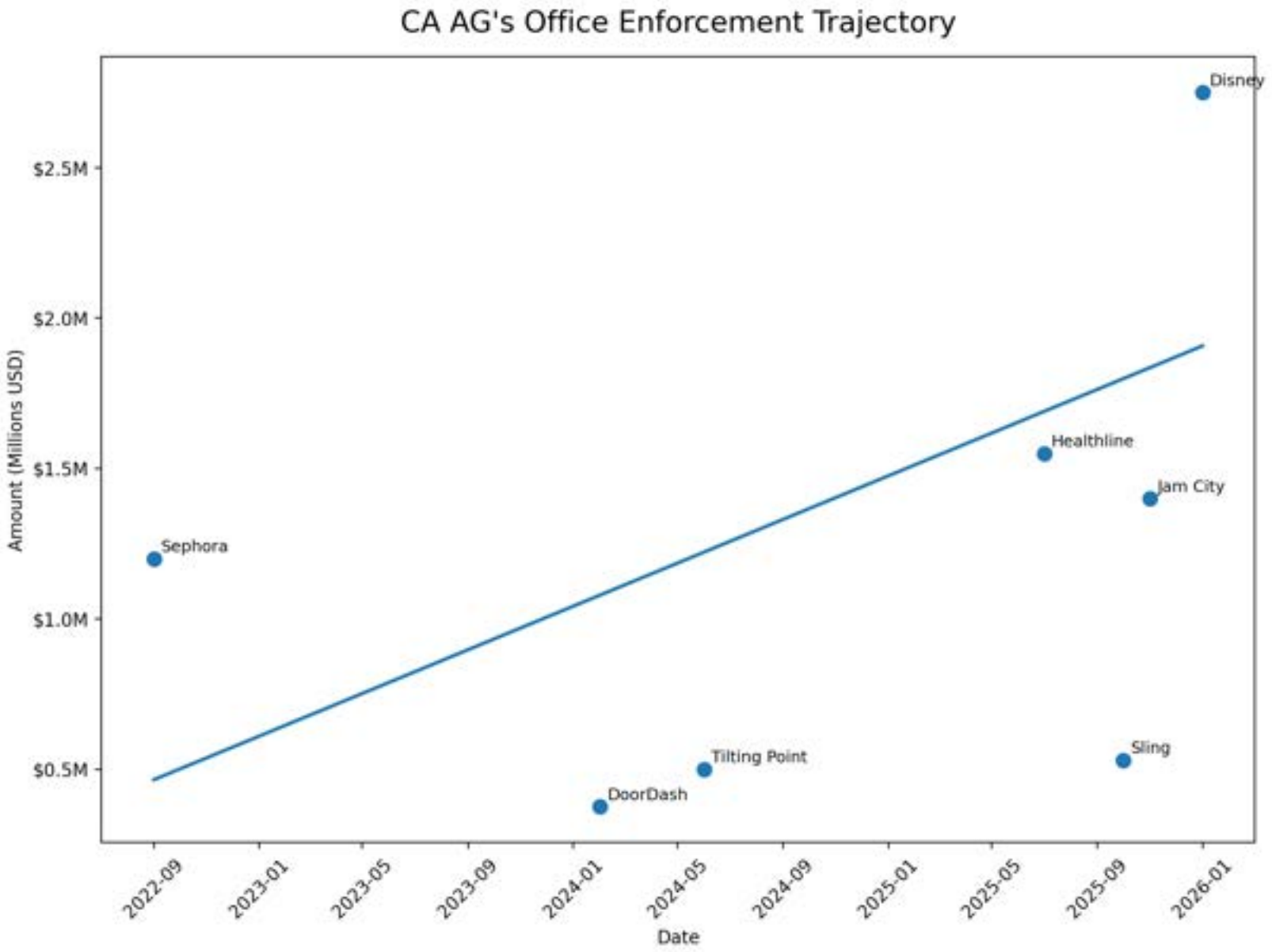
Frankfurt Kurnit Klein + Selz PC

Enforcement Today

- Privacy enforcement is no longer theoretical
  - 9 public CCPA enforcement actions in the past year
  - 9 public CA data broker enforcement actions
  - Public enforcement by Texas AG, Connecticut AG, and more
  - Many more investigations are not public
  - Enforcement activity is broader than what is announced
- Exposure is increasing
  - Most enforcement is driven by operational failures, not intentional misconduct
  - Regulators have moved beyond what disclosures say to whether systems work (do your opt-outs actually work?)
  - Settlement amounts are increasing for the same underlying allegations.

California Enforcement Landscape

- Who is Enforcing
  - California Attorney General (AG)
  - California Privacy Protection Agency (CalPrivacy)
  - District Attorneys
- What Laws are Being Enforced
  - CCPA, UCL, Delete Act, COPPA
- Penalties / Exposure (per-consumer exposure scales rapidly)
  - CCPA – $2,500 per violation, $7,500 intentional
  - Delete Act –$200 per day for registration failure + $200 per deletion request failure
  - UCL – up to $2,500 per violation
  - COPPA - up to $50,120 per violation



Sephora (Sept 2022) – $1.2 million

DoorDash (Feb 2024) – $375,000

Tilting Point (June 2024) – $500,000

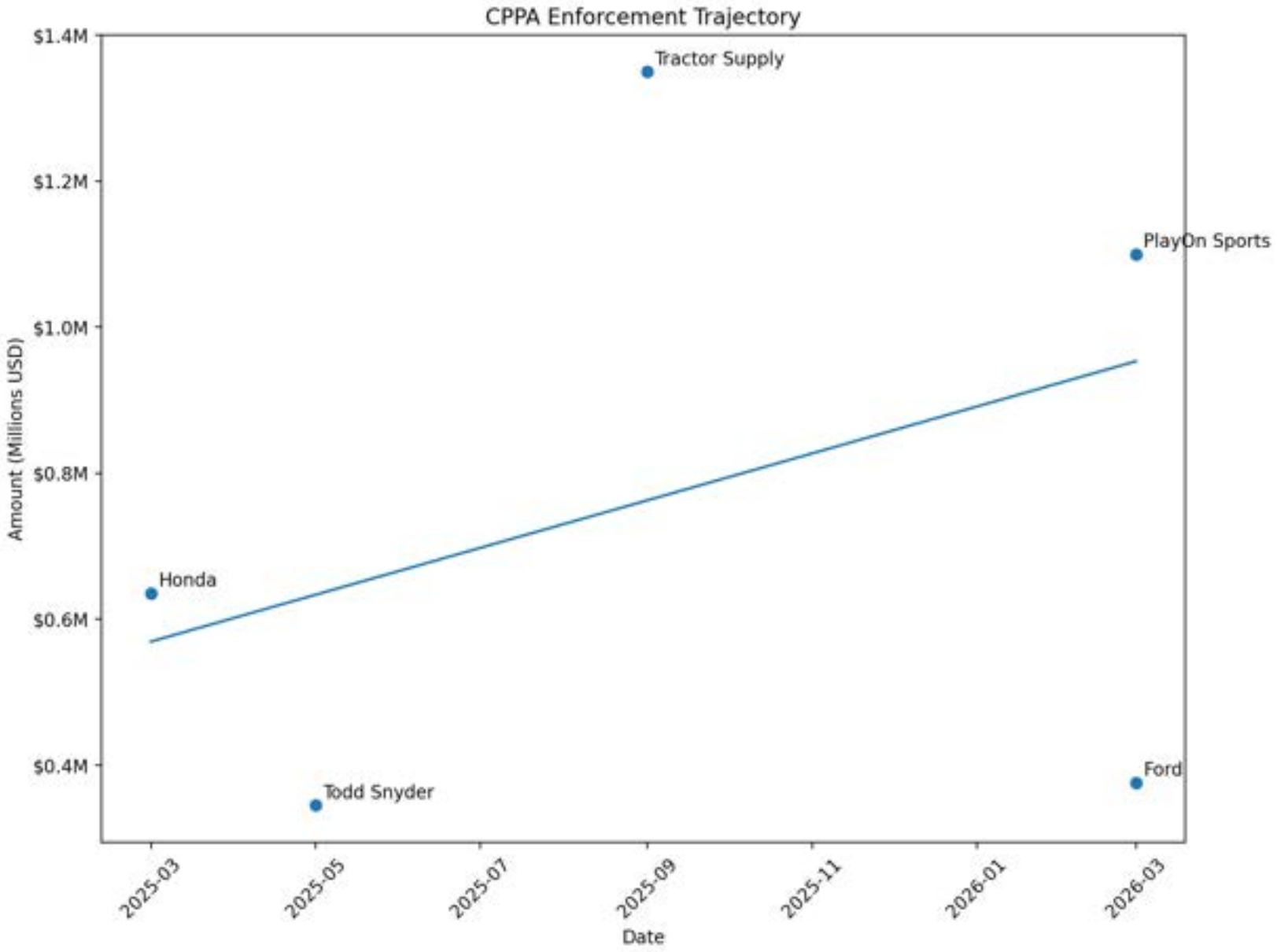
Healthline (July 2025) – $1.55 million

Sling (Oct 2025) – $530,000

Jam City (Nov 2025) – $1.4 million

Disney (Jan 2026) – $2.75 million

Frankfurt Kurnit Klein + Selz PC



Honda (March 2025) - $635,500

Todd Snyder (May 2025) $345,178

Tractor Supply (Sept 2025) - $1.35 million

Ford (March 2026) - $375,703

PlayOn Sports (March 2026) - $1.1 million

Frankfurt Kurnit Klein + Selz PC

Attorney General Bonta, Partners Secure $12.75 Million General Motors Privacy Settlement

Press Release / *When It Comes to Data Privacy, Consumers Must Be in the Driv...*

Friday, May 8, 2026

Contact: (916) 210-6000, agpressoffice@doj.ca.gov

Largest CCPA penalty in California history to date and first data minimization case

How Companies Get on the Radar

- Most investigations start the same way
  - Consumer complaints (especially around their rights)
  - Regulator sweeps (sector-based or issue-based)
  - Testing of websites and apps by regulators
  - Public reporting, lawsuits, or media coverage
  - Data broker registry gaps or mismatches
  - Vendor or downstream misuse
  - Speaking with other regulators

Investigations: How They Actually Unfold

- Initial Contact
- Investigation and Remediation
- Resolution
  - Quiet close, public settlement, litigation
- Post Settlement
  - Audits, reporting

Where Regulators are Focusing

1. Sale and Sharing Opt-Outs
2. Contracts and Records
3. Purpose Limitation and Data Minimization
4. Minors
5. Data Brokers
6. Employment

Sale and Sharing Opt-Outs

- What Regulators Expect
  - Single easy to use mechanism where consumers can opt-out of all sales or shares by a business
  - Technology agnostic (cookies + non-cookies)
  - Applies across all systems and services
- The Reality
  - Operationally complex — requires coordination across vendors, systems, and platforms
  - Limited vendor solutions — no single tool handles end-to-end compliance
  - Easy to break — misconfigurations, updates, and vendor changes create gaps
  - Confusion with CIPA and GDPR obligations
- What We See in Practice
  - Fragmented, layered opt-out experiences that don’t fully work

Common Opt-Out Deficiencies

a. Transparency Failures
b. Improper Opt-Out Mechanism
c. Friction and Dark Patterns
d. Technical and Operational Failures
e. Scope Failures

a. Transparency Failures

- Privacy policy
  - Did not inform consumers of their right to opt-out, including through preference signals (PlayOn)
  - Mispresented that generally no selling or sharing (PlayOn)
  - Misrepresented that no selling or sharing for specific type of data (driving data) (GM)

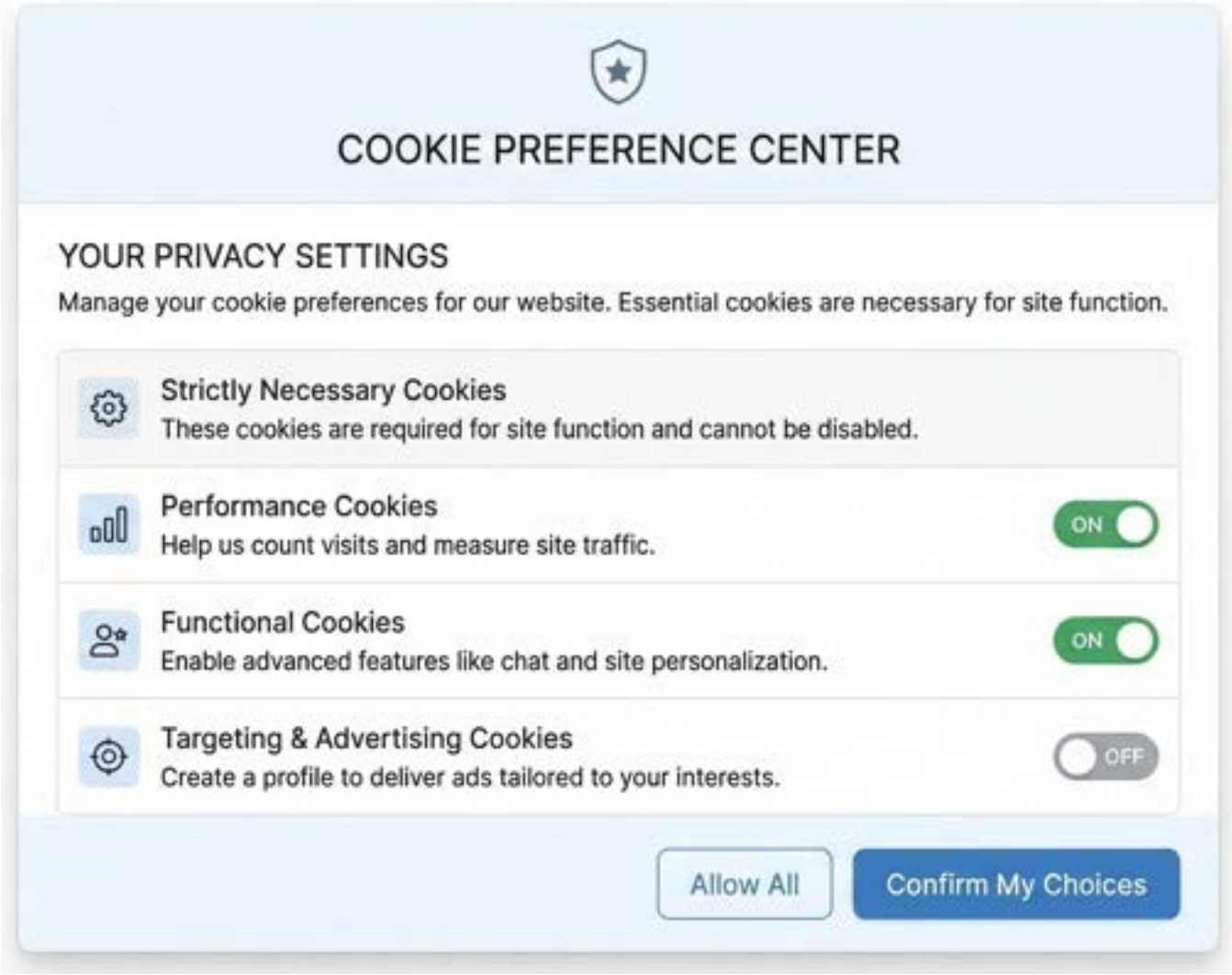
- No “Do Not Sell” or “Your Privacy Choices” link (PlayOn)

b. Improper Opt-Out Mechanism

- Used a cookie mechanism for opt-outs
- Used a webform for opt-outs
- Relied on third party industry opt-out tools

Used a Cookie Mechanism for Opt-Outs

- "[C]ookie preferences are not the same as a CCPA opt-out of the sale and sharing of a consumer's personal information. Cookie choices typically include options to allow, limit, or refuse cookies placed in a browser or to manage similar tracking technologies on an internet website. But the CCPA opt-out right is broader: it permits a consumer to direct the business to stop all cookie-based and non-cookie-based selling and sharing of the consumer's personal information across browsers, devices, and offline." (Sling)



AI generated example

Used a Webform for Opt-Outs

- "Tractor Supply's webform had no effect upon how the company shared consumers' personal information through third party tracking technologies used for advertising purposes, leaving consumers with the false impression that Tractor Supply had stopped selling and sharing their personal information." (Tractor Supply)
- No GPC Signal (Tractor Supply)
- Only offers email address and toll-free number (PlayOn)

Frankfurt Kurnit Klein + Selz PC

Relied on Third Party Industry Tools

- "[Improperly] directed students and other users to opt-out through the Network Advertising Initiative and the Digital Advertising Alliance, violating the company's responsibility to provide its own method for consumers to opt-out." (PlayOn)

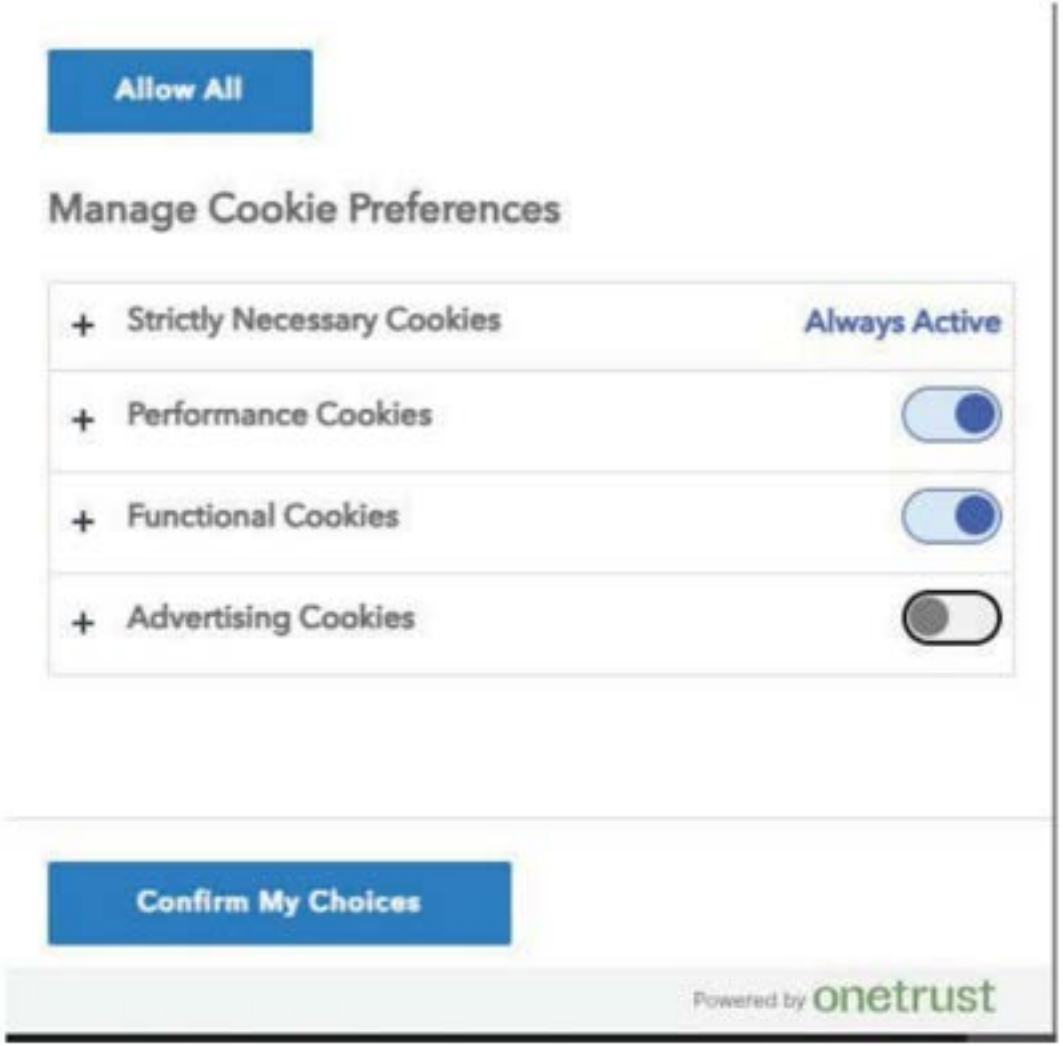
We and our third-party advertising partners may use cookies and similar technologies for interest-based advertising. You may have the ability to opt-out of certain of these data collection practices used by our third-party advertising partners for interest-based advertising. To learn more about interest-based advertising and how you may opt-out of certain uses of information by some of our third-party advertising partners, please visit: Digital Advertising Alliance (DAA): http://www.aboutads.info/choices or Network Advertising Initiative (NAI): http:www.networkadvertising.org/choices.

c. Friction and Dark Patterns

- Opt-out is harder than opt-in
- Buried or misleading flows
- Over-collection of data and improper verification

Opt-Out is Harder than Opt-In

- "Accept All" with no equivalent "Reject All" (Honda)
- Extra clicks (Honda)
- Additional steps to opt out ("Are you sure?") (Sling TV)



Buried or Misleading Flows

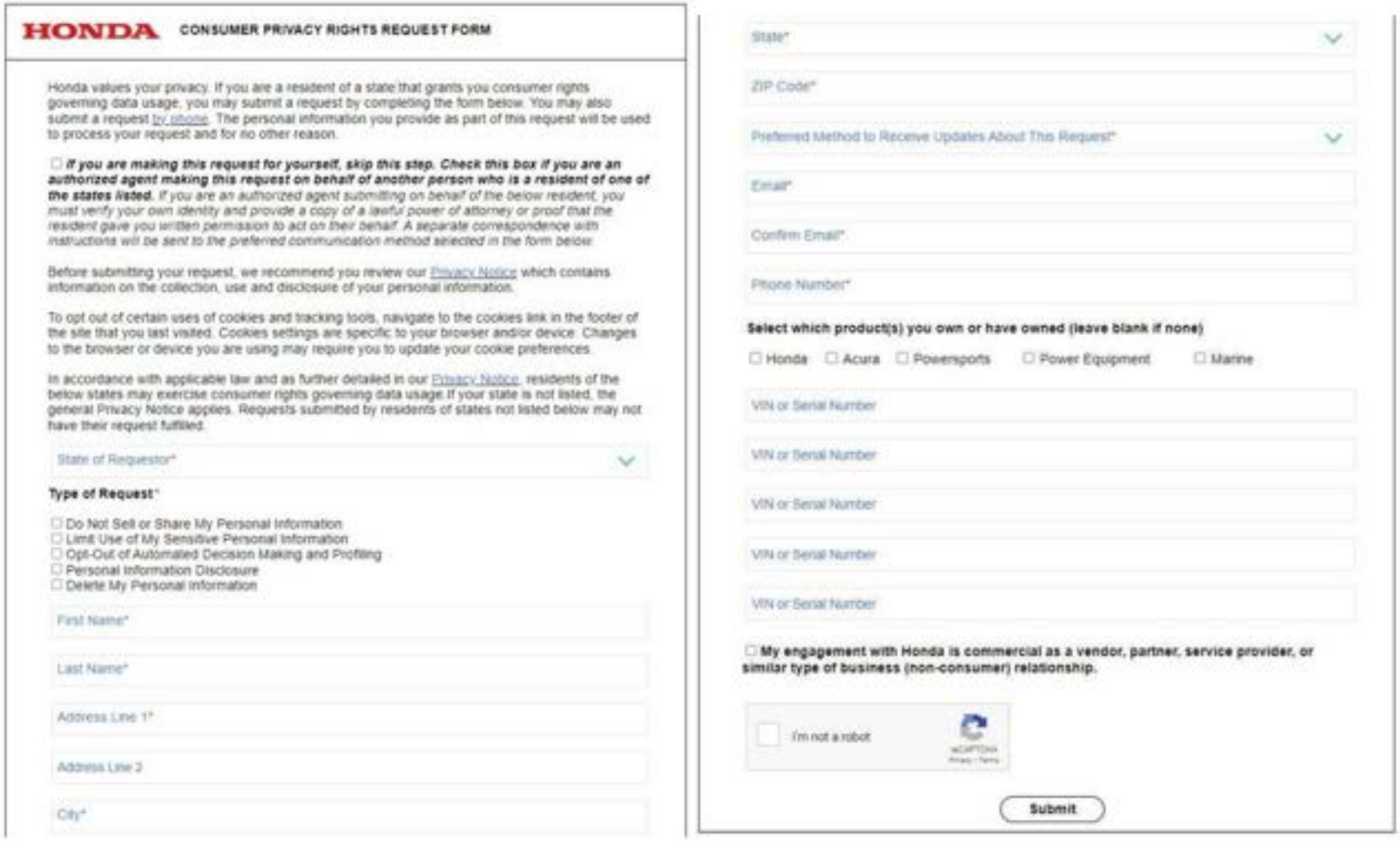
- Opt-out paths buried within cookie manager (below the fold or behind expandable menus) (Sling)
- Users directed to mechanism that has no effect (app links to web cookie controls that do not affect in-app tracking) (Sling)

AI generated example

Over-Collection and Improper Verification

- Requiring sensitive data
  - Photo of consumer holding identity document (Todd Snyder)
- Requiring excessive data
  - First, last, address, city, state, zip, email, phone, VIN (Honda)
- Requiring identity verification (Ford)
- Requiring consumers to verify authorized agents directly (Honda)

Excessive Data



HONDA CONSUMER PRIVACY RIGHTS REQUEST FORM

Honda values your privacy. If you are a resident of a state that grants you consumer rights governing data usage, you may submit a request by completing the form below. You may also submit a request by phone. The personal information you provide as part of this request will be used to process your request and for no other reason.

☐ ***If you are making this request for yourself, skip this step. Check this box if you are an authorized agent making this request on behalf of another person who is a resident of one of the states listed.*** *If you are an authorized agent submitting on behalf of the below resident, you must verify your own identity and provide a copy of a lawful power of attorney or proof that the resident gave you written permission to act on their behalf. A separate correspondence with instructions will be sent to the preferred communication method selected in the form below.*

Before submitting your request, we recommend you review our Privacy Notice which contains information on the collection, use and disclosure of your personal information.

To opt out of certain uses of cookies and tracking tools, navigate to the cookies link in the footer of the site that you last visited. Cookies settings are specific to your browser and/or device. Changes to the browser or device you are using may require you to update your cookie preferences.

In accordance with applicable law and as further detailed in our Privacy Notice, residents of the below states may exercise consumer rights governing data usage. If your state is not listed, the general Privacy Notice applies. Requests submitted by residents of states not listed below may not have their request fulfilled.

State of Requestor*

Type of Request*

☐ Do Not Sell or Share My Personal Information
☐ Limit Use of My Sensitive Personal Information
☐ Opt-Out of Automated Decision Making and Profiling
☐ Personal Information Disclosure
☐ Delete My Personal Information

First Name*

Last Name*

Address Line 1*

Address Line 2

City*

State*

ZIP Code*

Preferred Method to Receive Updates About This Request*

Email*

Confirm Email*

Phone Number*

Select which product(s) you own or have owned (leave blank if none)

☐ Honda ☐ Acura ☐ Powersports ☐ Power Equipment ☐ Marine

VIN or Serial Number

VIN or Serial Number

VIN or Serial Number

VIN or Serial Number

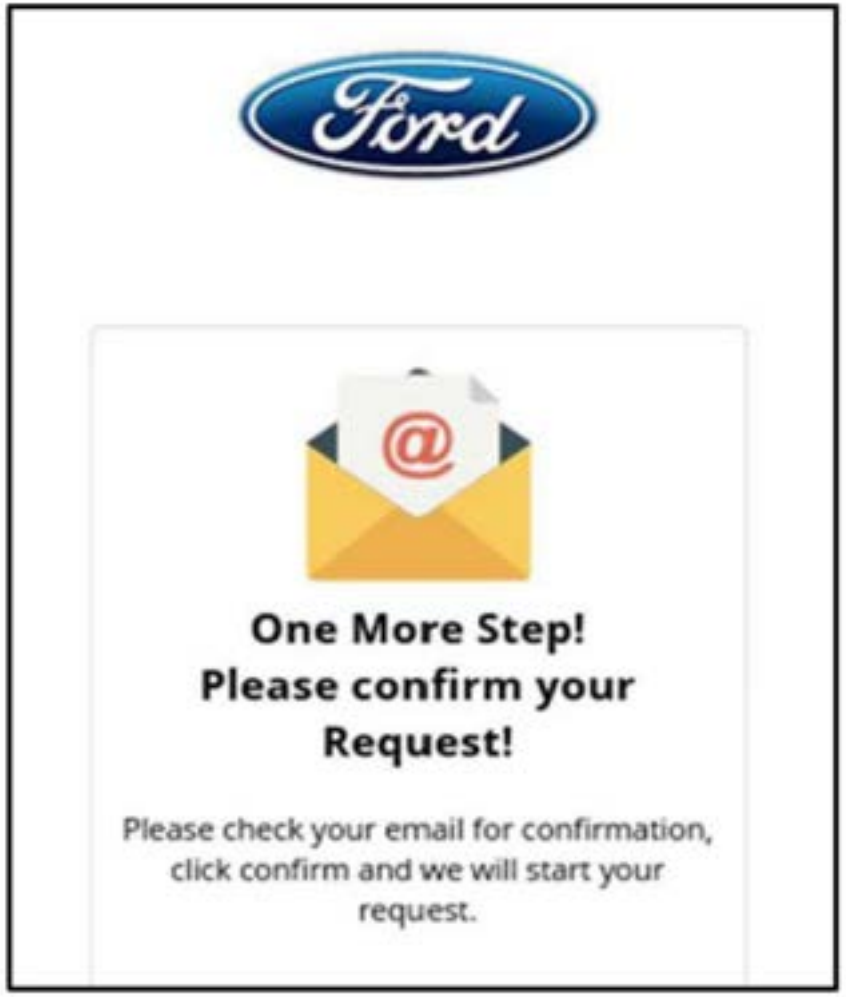
VIN or Serial Number

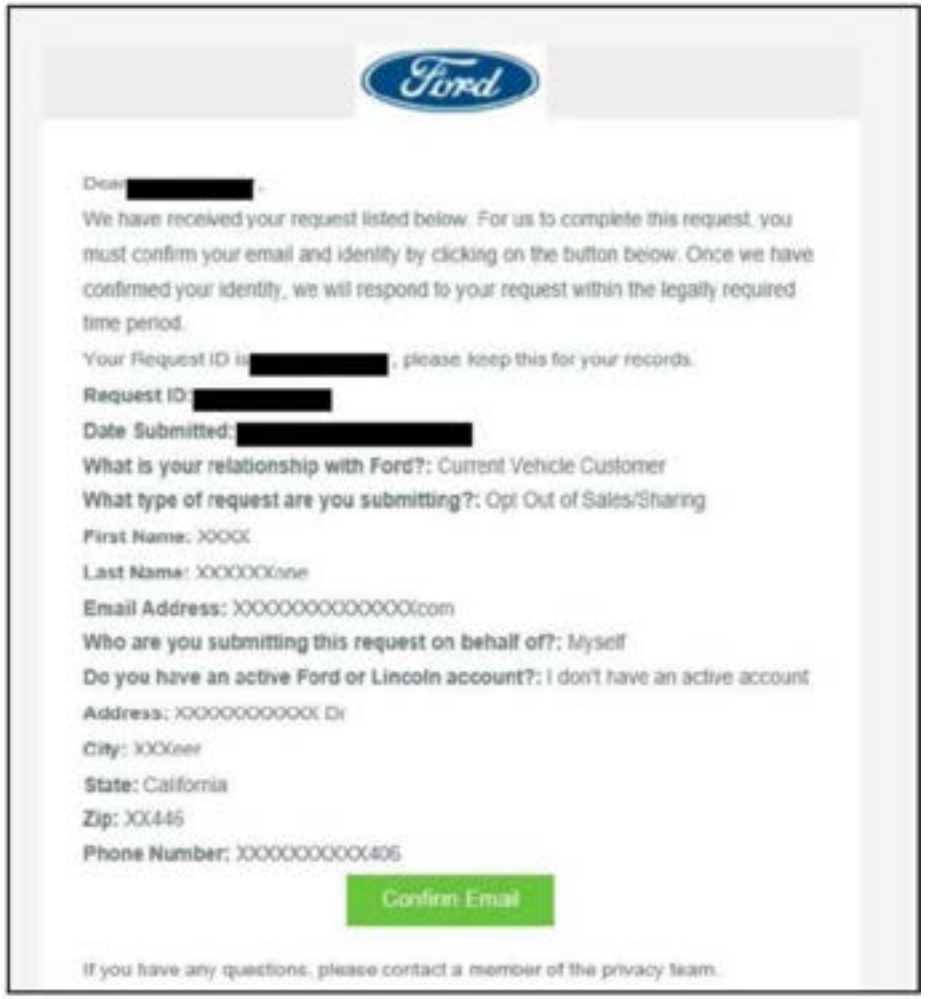
☐ **My engagement with Honda is commercial as a vendor, partner, service provider, or similar type of business (non-consumer) relationship.**

I'm not a robot

Submit

Identity Verification





Frankfurt Kurnit Klein + Selz PC

Verification for Authorized Agents

HONDA CONSUMER PRIVACY RIGHTS REQUEST FORM

Honda values your privacy. If you are a resident of a state that grants you consumer rights governing data usage, you may submit a request by completing the form below. You may also submit a request by phone. The personal information you provide as part of this request will be used to process your request and for no other reason.

☐ ***If you are making this request for yourself, skip this step. Check this box if you are an authorized agent making this request on behalf of another person who is a resident of one of the states listed.*** *If you are an authorized agent submitting on behalf of the below resident, you must verify your own identity and provide a copy of a lawful power of attorney or proof that the resident gave you written permission to act on their behalf. A separate correspondence with instructions will be sent to the preferred communication method selected in the form below.*

d. Technical and Operational Failures

- Consent banner fails or disappears (Todd Snyder)
- Opt-out does not actually disable tracking (Healthline)
- Vendors tools misconfigured or not functioning as intended (most actions)
  - "Businesses should scrutinize their privacy management solutions to ensure they comply with the law and work as intended, because the buck stops with the businesses that use them . . . Using a consent management platform doesn't get you off the hook for compliance." (Todd Snyder)

e. Scope Failures

- Web-only opt-out for multi-platform business (Sling, GM)
- Failure to apply opt-out across apps, CTV, or vehicles (Sling, Disney, GM)
- Failure to apply across logged-in environments, pseudonymous profiles, or advertising linked systems (Disney)
  - "Effective opt-out is one of the bare necessities of complying with CCPA. The investigation found that Disney's opt-out processes did not allow a consumer — even when logged into their account — to completely opt-out of and stop all sale or sharing of their data, in violation of the CCPA. Specifically, the investigation found that each of the methods Disney provided had key gaps that allowed Disney to continue to sell and share consumers' data."
  - "While Disney diligently linked consumer devices and data for purposes of targeting consumers with ads, it failed to link those same devices and data when it came to complying with consumers' exercise of their statutory right to opt out of targeted advertising. If a business can associate a consumer's devices with the consumer for advertising purposes, it can and must associate those devices with the consumer for purposes of honoring the consumer's opt-out rights."

Counsel Checklist

- User Interface (What to Evaluate)
  - Confirm the company offers a single, mechanism that covers all sale and sharing, not just cookies
  - Ensure symmetry and low friction (opt-out is no harder than opt-in)
  - Validate that the opt-out path is clear, conspicuous, and not misleading (no false or ineffective choices)
  - Watch for conflating legal regimes: CCPA opt-out ≠ GDPR consent ≠ CIPA consent
- Engineering (What Must Actually Work)
  - Confirm that an opt-out actually stops sale/sharing data flows and triggers required technical signals
  - Ensure the business honors opt-out preference signals (e.g., GPC) as valid opt-outs
  - Pressure-test scope of application:
    - Logged-in users: opt-out applies across the entire account ecosystem
    - Logged-out users: opt-out applies at the browser/device and associated profile level
  - Assume systems will fail: expect and plan for breakage, not perfect compliance
- Audit and Defensibility (What Regulators Will Ask to See)
  - Require ongoing testing after releases, tag changes, SDK updates, A/B tests, and vendor changes
  - Do not accept assurances that CMPs, tag managers, or ad tech partners are configured correctly
  - Ensure the company can document and clearly explain how opt-outs work in practice, how failures are detected, and how and when fixes are implemented

Where Regulators are Focusing

1. Sale and Sharing Opt-Outs
2. Contracts and Records
3. Purpose Limitation and Data Minimization
4. Minors
5. Data Brokers
6. Employment

Contracts and Records

- What Regulators Expect
  - All contracts include CCPA-required language
  - Company has conducted robust due diligence when executing contracts
  - Company has internal records of processing operations ready to provide to regulators
- The Reality
  - Many contracts address GDPR, but not CCPA. Contractual obligations do not align.
  - There is no universally adopted form (industry templates often miss CCPA requirements)
  - Pressure on teams to quickly execute contracts and asymmetrical negotiation leverage
  - Tough to keep internal policies updated and accurate
- What We See in Practice
  - Contracts do not meet CCPA requirements
  - Company fails to conduct adequate due diligence
  - Company does not have internal policies or fails to abide by them

Contracts Don’t Meet CCPA Requirements

- Could not produce contracts (Honda)
- Contracts did not include CCPA required language (Todd Synder)
- Contracts did not specify purpose limitation (Healthline)
  - Any business purpose
  - Any internal use inuring to the recipient’s direct benefit
  - For the purposes contemplated in the agreement or as otherwise agreed to by the parties
- Contracts did not address treatment of opt-out signals (Healthline)

Company Fails to Conduct Due Diligence

- Participated in advertising contractual framework (IAB MSPA) to supplement existing contracts with CCPA provisions, but failed to ensure downstream recipients were signatories to the framework. (Healthline)

Digital Advertising Activity	Permitted Activities
Ad Delivery and Targeting	
First-Party Advertising	Y
Targeted Advertising	N
Third-Party Segment Creation	N
Frequency Capping Activities	Y
Negative Targeting	Y
Ad Reporting	
Measure Ad Performance	Y
Apply Market Research to Generate Campaign Insights	Y
Ad Fraud Detection	Y
Ad Viewability	Y

No Internal Policies or Failure to Abide

- Had a formal internal privacy program since at least 2019, but failed to comply with it (GM)

- Could not produce risk assessments when requested (GM)

Counsel Checklist

- Require CCPA-compliant contract language in every agreement involving personal information (GDPR terms alone are insufficient)
- Correctly classify counterparties (service provider vs. third party) based on actual data use
- Limit use to specific, defined business purposes — prohibit open-ended or "any business purpose" language
- Prohibit selling or sharing where required and require compliance with opt-out requests and signals
- Flow CCPA obligations downstream to subprocessors and other recipients
- Conduct and document due diligence — do not rely on templates, representations, or industry frameworks alone
- Ensure contracts reflect reality and can be produced to regulators on demand
- Regularly evaluate and test internal policies and programs

Where Regulators are Focusing

1. Sale and Sharing Opt-Outs
2. Contracts and Records
3. Purpose Limitation and Data Minimization
4. Minors
5. Data Brokers
6. Employment

Purpose Limitation and Data Minimization

- What regulators expect
  - All data is collected for limited and specific purposes
  - All data is deleted where no longer necessary and proportionate
  - Sensitive data is subject to heightened restrictions
- The Reality
  - Businesses don't know or can't anticipate purposes for which they might use data (e.g., AI training)
  - Pressure from marketing and business teams to leverage data
  - Regulatory views on sensitive data do not align with historical industry practices
- What We See in Practice
  - Data sold in violation of purpose limitation
  - Data retained and disclosed in violation of data minimization
  - Sensitive data and high-risk processing remain a major compliance gap

Data Sold in Violation of Purpose Limitation

- Sold device identifiers along with titles/URLs of diagnosed medical condition articles visited to ad networks without expressly informing consumer or obtaining consent (Healthline)

- Sold driving data (including precise geolocation, hard braking, hard acceleration, speed threshold crossings, seat belt usage, late-night driving, and trip time and duration) to data brokers without expressly informing consumers or obtaining consent (GM)

    - Even if disclosed, selling driving data for insurance rating purpose likely would not have been compatible with purpose to provide requested services (GM)

    - Disclosing driving data to set premiums is an unlawful purpose and an unlawful purpose likely can never satisfy purpose limitation (GM)

    - Under the GM settlement, where consent required, GM must obtain consent for each separate, unrelated service or feature that collects, uses, or discloses the driving data (GM)

Data Retained and Disclosed in Violation of Data Minimization

- Began collecting geolocation data in 2016 but did not start selling it until 2020, years after it was necessary to operate the requested service (GM)
- Sold geolocation data to a data broker when the data broker did not need that data for its driving-rating product (GM)
  - "When asked why GM sold geolocation data to Lexis, but not Verisk, GM simply said that's what the contracts required" (GM)
  - Contractual permission to sell does not equal legality

Sensitive Data and High-Risk Processing Remain a Major Compliance Gap

- Sold consumers' sensitive data (precise geolocation data) to third parties without limit the use and disclosure and/or consent (GM)

- Failed to comply with its own internal privacy program regarding sensitive data in the context of purpose limitation, data minimization, and risk assessments (GM)
  - Could not produce risk assessment covering its decision to sell driving data to data brokers (GM)

Risk Assessments

- We've now seen two cases, PlayOn and GM, that expressly reference and impose requirements on companies to conduct CCPA risk assessments
- The CCPA Regs require risk assessments for processing that presents significant risk to a consumer's privacy, including:
  - Selling or sharing personal information
  - Processing sensitive personal information
  - Using automated decision-making technology (ADMT) for a significant decision concerning a consumer
  - Profiling or inferring characteristics about applicants, students, or employees
  - Profiling or inferring characteristics based on a consumer's sensitive location
  - Processing personal information with intent to train an ADMT for a significant decision concerning a consumer or identify verification
- Risk-assessment requirement effective January 1, 2026; first executive attestation and summary submission due April 1, 2028.

Deidentification

- One of the more significant aspects of the GM settlement is the role deidentification plays in the injunctive terms
- GM is not required to obtain consent, and is not required to delete data, where it uses deidentified data for research or product improvement, provided that only deidentified data is disclosed to third parties for that purpose and marketing is excluded

Counsel Checklist

- Treat purpose limitation and data minimization as substantive constraints on use
- Evaluate data uses in context and ensure disclosures are specific and sufficient for the actual use cases
- Apply the consumer-reasonableness test: put yourself in the consumer's shoes — would this use reasonably be expected in this context?
- Reassess purpose compatibility when data uses expand (e.g., analytics, targeting, AI training)
- Apply heightened scrutiny to sensitive data and context-specific signals that elevate risk
- Conduct and document risk assessments where high-risk processing
- Ensure contracts clearly limit purposes and align with how data is actually used
- Evaluate deidentification options to address purpose limitation and data minimization

Where Regulators are Focusing

1. Sale and Sharing Opt-Outs
2. Contracts and Records
3. Purpose Limitation and Data Minimization
4. Minors
5. Data Brokers
6. Employment

Minors

- What Regulators Expect
  - Affirmative authorization for ages 13-15 before selling or sharing
  - Systems configured to identify and treat minors differently
  - Protections applied across all products, services, and data uses
- The Reality
  - Systems built for under 13 (COPPA), not 13-15 (CCPA) or 15-17
  - Vendors offer limited minor-specific controls
  - SDKs and data flows difficult to understand or audit
- What We See in Practice
  - Age gates set incorrectly or inconsistently (13 instead of 16)
  - Companies ignore indicators of minors

Age Gates Set Incorrectly or Inconsistently

(Jam City)

AI generated example

Ignoring Indicators of Minors

- No protections for minors' data despite child-directed content and parental content controls / ad restrictions (Sling)
- Targeted households with children, indicating aware of child users (Sling)

Counsel Checklist

- Evaluate whether the product, service, or feature is directed to children under COPPA, including mixed-audience or child-appealing content
- Ensure age gates and age signals are correctly implemented, and that any resulting actual knowledge of a minor leads to proper application of age-based requirements (including affirmative authorization for ages 13–15)
- Do not ignore indicators of minors, such as content type, audience targeting, parental controls, student or youth contexts, or household-level signals
- Ensure systems are configured to treat minors differently, not just under-13 users, across products, services, SDKs, and data uses
- Review vendors, SDKs, and ad tech to confirm they support minor-specific controls and honor age-based restrictions in practice
- Consider the impact of emerging laws that extend protections to users under 18, including heightened default settings, profiling limits, and design-based obligations
- Account for platform and ecosystem changes (e.g., age-verification obligations or platform APIs that transmit age signals and create actual knowledge)

Where Regulators are Focusing

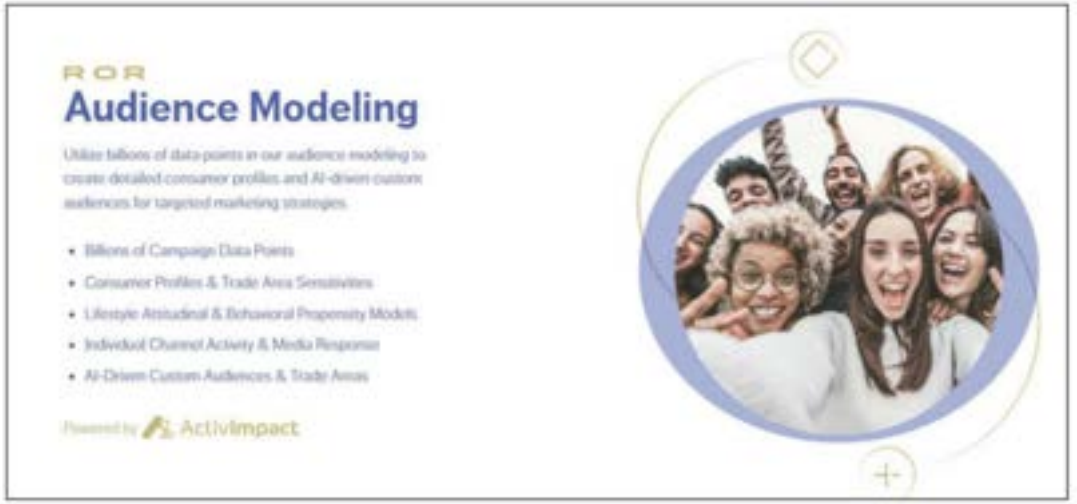
1. Sale and Sharing Opt-Outs
2. Contracts and Records
3. Purpose Limitation and Data Minimization
4. Minors
5. Data Brokers
6. Employment

Data Brokers

- This is a sleeper risk
  - Many companies may qualify as data brokers without realizing it
  - Also, if you work with a data broker, there may be associated exposure
- A “data broker” under California law is any business that that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.
- “Direct relationship” means that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business’s products or services.
  - A consumer does not have a “direct relationship” with a business:
    - if the purpose of their engagement is to exercise their consumer rights or for the business to verify their identity
    - if the consumer does not intend to interact with the business (simply collecting personal information directly from the consumer is not enough)
    - as to personal information it sells about the consumer that it collected outside of a “first party” interaction with the consumer (it can be a data broker in some contexts)

Where Companies are Getting Caught

- All actions based on failure to register
- $200/day + unpaid fees + enforcement costs
- To date, 9 cases by CalPrivacy (from sweeps)
  - GrowBots (Nov 24) - $35.4k;
  - UpLead (Nov 24) - 34.4k
  - Infillion (Dec 24) - $54.2k;
  - The Data Group (Dec 24) - $46.6k;
  - Key Marketing Advantage (Jan 25) - $55.8k
  - Background Alert (Feb 25) - $50k / shutdown;
  - National Public Data (May 25) - $46k / defaulted
  - Accurate Append (July 25) - $55.4k;
  - ROR Partners (Dec 25) - $56k
- Data Broker Enforcement Strike Force



Frankfurt Kurnit Klein + Selz PC

Exposure is About to Change Drastically

- By Jan 1, 2026:
  - Create an account, complete registration, including payment ($6,600 per year)
  - Select identifiers collected (first name, last name, DOB, zip, email, phone, MAID, CTV ID, VIN)
  - Each data broker must register separately, including subsidiaries
  - Must list all websites, trade names, or DBAs
- Starting Aug 1, 2026:
  - Access account every 45 days to pull list of consumer deletion requests (in hashed form)
  - Normalize and hash internal identifiers, match those against the deletion requests, and delete matching records and maintain a suppression list
  - Direct service providers to do the same.
  - Report status online.
  - Failure to delete is $200/day/consumer + enforcement costs
- Starting Jan 1, 2028, must:
  - Undergo independent audit every 3 years to assess compliance

Risks to Non-Data Brokers Where Selling to or Receiving Data from Data Brokers

- Sold data to data brokers in violation of CCPA (GM)
- Obtained data from third parties (like data brokers) to build advertising models (Disney)
  - Under the settlement Disney was required to:
  - Provide clear and conspicuous notice that it conducts cross-context behavioral advertising using personal information obtained from third parties.
  - For any consumer who opt-outs, stop selling and sharing the consumer's personal information and stop conducting cross-context behavioral advertising for that consumer.

Counsel Checklist

- Assess whether the company qualifies as a data broker in any context, including where personal information is collected and sold without a direct consumer relationship
- Do not assume first-party status applies universally — a company can be a data broker for some data uses but not others
- Register where required and maintain ongoing compliance with applicable data-broker regimes (e.g., California, Texas, Vermont, Oregon), including reporting and renewal obligations
- Prepare for Delete Act obligations, including participation in DROP and downstream deletion instructions to service providers
- If selling to or receiving data from a third party (including a data broker), evaluate downstream obligations, including notice, opt-out, deletion, and role classification
- Ensure contracts align with data-broker obligations, including restrictions on downstream use and clear role allocation
- Treat data-broker activity as high-risk processing, with appropriate governance, documentation, and readiness for regulator sweeps or inquiries

Where Regulators are Focusing

1. Sale and Sharing Opt-Outs
2. Contracts and Records
3. Purpose Limitation and Data Minimization
4. Minors
5. Data Brokers
6. Employment

Employment

- What regulators expect
  - California consumer privacy protections apply to personal information of California employees and job applicants, not just consumers
- The Reality
  - Companies are focused on employment and labor laws, not privacy laws, when handling employee and applicant data
  - The U.S. has historically provided limited privacy protections for employee and job-applicant data
- What We See in Practice
  - Insufficient privacy disclosures for employees and job applicants
  - Employment data treated as “out of scope” for consumer-privacy compliance programs

Insufficient Privacy Disclosures

- Tractor Supply had a job-applicant privacy policy, but allegedly failed to provide applicants with notice of their CCPA rights or any explanation of how to exercise those rights
- The company was required to update both its job-applicant privacy policy and employee privacy policy to address these gaps

STATE OF CALIFORNIA

CALIFORNIA PRIVACY PROTECTION AGENCY
400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov

INVITATION FOR PRELIMINARY COMMENTS

NOTICES & DISCLOSURES AND EMPLOYEE DATA

The California Privacy Protection Agency (CalPrivacy) is exploring whether regulatory changes related to notices and disclosures, or employee data are necessary. (*See* Gov. Code §§ 11346(b), 11346.45.) CalPrivacy seeks input from stakeholders on both of these topics and is accepting preliminary comments through May 20, 2026.

Invitation for Preliminary Comments

The California Consumer Privacy Act (CCPA) and CalPrivacy's implementing regulations require businesses to provide consumers with notices explaining their privacy practices, including a privacy policy, Notice at Collection, and notices about consumers' privacy rights. (Civ. Code §§ 1798.100-135; Cal. Code Regs., tit. 11 §§ 7002, 7003, 7004, 7010-7016, 7020-7028, 7220.) These and other CCPA requirements also apply to businesses' processing of employees' personal information. (Civ. Code §§ 1798.140(i), 1798.145(m); Cal. Code Regs., tit. 11 §§ 7002, 7003, 7004, 7011, 7012, 7020-7028, 7050-7053, 7060-7063, 7080-7081.) CalPrivacy is exploring whether these regulations should be amended, and whether new regulations addressing these topics should be adopted.

Counsel Checklist

- Treat employees and job applicants as covered individuals under CCPA
- Ensure privacy notices are provided to employees and job applicants, including notice of rights and how to exercise them
- Review HR, recruiting, and applicant-tracking workflows to confirm disclosures align with actual data collection and use
- Scrutinize biometrics and workplace monitoring tools (e.g., fingerprints, facial recognition, keystroke or productivity monitoring) for heightened privacy obligations and risk
- Evaluate AI-driven or automated screening tools used in hiring, promotion, or workforce management for ADMT, profiling, and risk-assessment implicatons
- Ensure contracts with HR vendors, recruiters, background-check providers, and assessment platforms include CCPA-required provisions, correct role classification, and purpose limitations
- Integrate employment data into broader privacy governance, including documentation, escalation paths, and regulator-readiness

Final Takeaways

- Make clear to ownership: this is real risk, not theoretical
  - Enforcement is active and testing how your systems actually operate
- Own operational readiness
  - Know who owns data, tracking, vendors, and consumer rights and ensure teams are aligned and reachable
- Document and be able to explain your practices
  - What data you collect, how it's used, and how rights function in practice
- Be ready to respond immediately
  - Triage complaints and inquiries; escalate quickly; assume preservation obligations
- Have support in place
  - Experienced outside counsel and internal teams ready to engage on short notice

Thank you!

Daniel Goldberg
Chair, Data Strategy Group
Frankfurt Kurnit
dgoldberg@fkks.com