A Comprehensive Legal Analysis of the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Policies, Rules, and Compliance Obligations

1. Introduction: The Evolution of California Privacy Law

The California Consumer Privacy Act (CCPA), effective in 2018, established the first comprehensive data privacy framework in the United States. However, this initial legislation was quickly and substantially augmented by the California Privacy Rights Act (CPRA). The CPRA, a ballot initiative (Proposition 24) passed by California voters in November 2020, did not create a separate law; rather, it significantly amended and expanded the CCPA.[1] The currently enforceable statute is therefore correctly understood as the "CCPA, as amended".[1]

This evolutionary path, from legislation to a strengthening voter initiative, demonstrates that California's privacy framework is not static. The passage of Prop 24 to close perceived loopholes in the original CCPA indicates a dynamic legal ecosystem where privacy protections are progressively "ratcheted up," and businesses must anticipate this ongoing evolution in their compliance strategies.

The Central Role of the California Privacy Protection Agency (CPPA)

A cornerstone of the CPRA was the establishment of the California Privacy Protection Agency (CPPA), the first dedicated data privacy enforcement agency in the nation.[2] This agency assumed the rulemaking authority from the California Attorney General and is now the primary entity responsible for implementing and enforcing the law.[6]

The CPPA's mandate is broad and includes [2]:

- Adopting and amending regulations to implement the CCPA.
- Enforcing the law and assessing penalties for non-compliance.
- Promoting public awareness of consumer rights and business responsibilities.
- Providing technical assistance and advice to the Legislature on privacy-related legislation.

The creation of the CPPA signals a fundamental shift in the enforcement landscape. While the Attorney General continues to have co-enforcement authority [10], the original enforcement was managed by an office with myriad other priorities. The CPPA, by contrast, is a specialized, well-funded agency with a singular focus on privacy.[9] This move from sporadic, AG-led actions to proactive and specialized regulatory oversight exponentially increases the enforcement risk for non-compliant organizations.

2. Applicability: Determining CCPA/CPRA Jurisdiction

The CCPA applies to any for-profit entity that "does business in California" and meets *at least one* of the following three thresholds.[1]

The Three-Prong Test

1. **Revenue Threshold:** Has annual gross revenues in excess of $25 million.[1] This threshold is based on the business's *global* gross revenue, not just revenue generated in California, and is calculated based on the preceding calendar year.[4]
2. **Data Volume/Activity Threshold:** Annually buys, sells, or *shares* the personal information of 100,000 or more California residents or households.[1]
3. **Business Model Threshold:** Derives 50% or more of its annual revenue from *selling* or *sharing* California residents' personal information.[1]

The CPRA's modifications to these thresholds were strategic. The original CCPA's data volume test was 50,000 "consumers, households, or *devices*".[4] This low bar, which included "devices," meant many small websites with modest traffic could be inadvertently swept into the law's scope simply by using common analytics. The CPRA raised the number to 100,000 and, critically, removed "devices" and the passive "receives" from the test, focusing instead on active commercialization: "buying, selling, or sharing".[13]

This change likely de-scoped some smaller businesses that only passively collect data. However, the CPRA *simultaneously* expanded the 50% revenue threshold to include revenue from *sharing*.[14] This was a targeted maneuver to ensnare data brokers and ad-tech companies of *any* size, even those under the $25 million revenue threshold, whose primary business model relies on sharing data for advertising.

Valuable Table: Applicability Thresholds (CCPA vs. CPRA)

Criterion	CCPA (2018) Threshold	CPRA (Current Law) Threshold
Revenue	> $25 million annual gross revenue [4]	> $25 million annual gross revenue (clarified as global) [1]
Data Volume / Activity	Annually buys, receives, sells, or shares the PI of **50,000** or more consumers, households, or **devices**.[4]	Annually buys, sells, or **shares** the PI of **100,000** or more residents or households.[1]
Business Model	Derives 50% or more of annual revenue from **selling** consumers' PI.[4]	Derives 50% or more of annual revenue from **selling or sharing** consumers' PI.[1]

Application to Affiliated Entities

The law's reach extends to entities beyond those that directly meet the thresholds. An entity that controls or is controlled by a covered "business," and that *shares common branding* (such as a shared name, servicemark, or trademark that an average consumer would recognize), is also subject to the CCPA.[11] This provision has significant implications for corporate families, subsidiaries, and joint ventures.

3. Foundational Definitions: The Language of CCPA Compliance

Understanding the CCPA's specific terminology is essential for compliance.

"Personal Information" (PI)

The law uses a broad definition of "Personal Information," which includes any data that "identifies, relates to, or could reasonably be linked, directly or indirectly, with a particular consumer or household".[15] This explicitly includes identifiers such as names, aliases, and IP addresses, as well as commercial data like purchase histories, internet activity like browsing histories, geolocation data, employment-related data, and, significantly, *profiles* or *inferences* drawn about a consumer.[15]

"Sensitive Personal Information" (SPI)

The CPRA introduced a new subset of PI called "Sensitive Personal Information" (SPI).[15] This distinction is critical because it triggers a new, specific consumer right: the Right to Limit its use and disclosure. Identifying and mapping SPI is a foundational step for compliance.

Valuable Table: Statutory Categories of Sensitive Personal Information (SPI)

Category	Description	Source(s)

Government IDs	Social Security, driver's license, state ID, or passport number.	[15]
Financial/Account	Account log-in, financial account, debit/credit card number *in combination with* any required security code, password, or credentials.	[15]
Geolocation	Precise geolocation data.	[15]
Protected Classes	Racial or ethnic origin, religious or philosophical beliefs, union membership.	[15]
Communications	Contents of a consumer's mail, email, and text messages (unless the business is the intended recipient).	[15]
Biometric/Genetic	Genetic data; Biometric information used for unique identification.	[15]
Health/Sex	Information concerning a consumer's health, sex life, or sexual orientation.	[15]
Other	Citizenship or immigration status [15]; Neural data.[15]	[15]

"Business Purpose" vs. "Commercial Purpose"

The CCPA distinguishes between *why* data is used:

- **Business Purpose:** The use of PI for the business's operational needs. This use must be "reasonably necessary and proportionate" to achieve the intended operational purpose.[21] The CCPA lists seven categories of business purposes: (1) Auditing, (2) Security, (3) Debugging/Repair, (4) Certain Short-term Uses, (5) Performing Services, (6) Internal Research, and (7) Quality/Safety Maintenance.[21]
- **Commercial Purpose:** The use of PI to advance a company's economic interests.[23] This includes activities like monetizing data, targeted advertising, or generating product recommendations.[23]

Decoding "Sale," "Sharing," and "Cross-Context Behavioral Advertising" (CCBA)

These definitions are central to the CCPA's opt-out rights.

- **Sale:** The exchange of PI for "monetary or other valuable consideration".[24] The "valuable consideration" clause is extremely broad and was the linchpin of the *Sephora* settlement.[25]
- **Sharing:** A new term introduced by the CPRA to definitively close a perceived loophole in the definition of "sale".[26] "Sharing" is *specifically* defined as disclosing or making PI available to a third party for **cross-context behavioral advertising**.[1]
- **Cross-Context Behavioral Advertising (CCBA):** Defined as targeting advertising to a consumer based on their PI obtained from activity *across* different, unrelated "businesses, distinctly-branded websites, applications, or services".[27]

The creation of the term "sharing" was a direct legislative response to the industry's argument that exchanging consumer data with ad-tech partners for *services*—like analytics or ad targeting—was not a "sale" because no money changed hands.[24] This argument created a loophole where the very activity the CCPA was designed to regulate (tracking users across the web for targeted ads) was arguably permissible.[29]

While the California AG's enforcement action against Sephora successfully argued that these services *did* constitute "valuable consideration" and were therefore a "sale" [25], the CPRA simultaneously rendered the argument moot. By creating "sharing" [1], the law made it clear that any transfer of PI to a third party for CCBA [27] is, at a minimum, "sharing," which triggers the consumer's "Right to Opt-Out." The debate is over; the ad-tech ecosystem is explicitly regulated.

4. The Consumer Rights Framework: A Detailed Analysis

The CCPA, as amended, grants California residents a robust suite of privacy rights.

The Right to Know/Access

Consumers have the right to request that a business disclose both the *categories* and the *specific pieces* of PI it has collected about them.[1] This disclosure must cover:

- The categories of PI collected.[4]
- The categories of *sources* from which the PI was collected.[4]
- The business or commercial purpose for collecting, selling, or sharing the PI.[4]
- The categories of third parties to whom the PI is disclosed.[4]

The default lookback period for a "Right to Know" request is the 12-month period preceding the request.[32] However, new regulations have significantly altered this limitation. Businesses are now required to respond to requests for information *beyond* the 12-month period, unless "doing so proves impossible or would involve disproportionate effort".[34] A business cannot merely claim this; it must provide the consumer with a "detailed explanation" justifying the impossibility or effort.[34]

This change creates a new data governance challenge. It directly conflicts with the new transparency rule requiring businesses to *disclose* their data retention periods in the Notice at Collection.[36] If a business discloses that it retains employee data for seven years to comply with legal obligations [38], it cannot reasonably claim "disproportionate effort" [34] when an employee requests seven years of their PI. This development effectively forces businesses to either *truly* delete all data not subject to legal holds or invest in data management systems capable of retrieving *all* retained PI, regardless of age, thereby weakening the "disproportionate effort" defense.

The Right to Delete

Consumers can request that a business delete PI it has collected *from* them.[1] This obligation "flows down," meaning the business must also direct its service providers to delete the information.[6]

This right is *not* absolute. The law provides several key exceptions.[1] A business may deny a deletion request if the information is necessary to:

- Complete the transaction for which the PI was collected.
- Detect security incidents or protect against malicious activity.
- Debug and repair errors in functionality.
- Exercise free speech or ensure the right of another consumer to exercise free speech.
- Comply with a legal obligation.
- Engage in public interest research.
- For internal uses "reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."

The Right to Opt-Out of Sale/Sharing

Consumers have the right to direct a business *not* to "sell" or "share" their PI.[1] Businesses must provide a clear and conspicuous link on their website (e.g., "Do Not Sell or Share My Personal Information") and must also recognize and honor user-enabled opt-out preference signals, such as the Global Privacy Control (GPC).[1] The *Sephora* settlement made failure to honor GPC a clear enforcement priority.[42]

Once a consumer has opted out, the business must wait at least 12 months before asking them to opt back in to the sale or sharing of their PI.[1]

The Right to Correct

A new right introduced by the CPRA, this allows consumers to request the correction of inaccurate PI a business holds about them.[1] The business must use "commercially reasonable efforts" to correct the information as directed by the consumer.[30]

The Right to Non-Discrimination

A business is prohibited from discriminating or retaliating against a consumer for exercising any of their CCPA rights.[1] This includes:

- Denying goods or services.[45]
- Charging different prices or rates (including by denying discounts).[45]
- Providing a different level or quality of goods or services.[45]

A business *is* permitted to offer financial incentives, such as a discount in exchange for the collection or sale of PI, but the incentive program must be fair, clearly disclosed, and require the consumer to opt-in.[47]

Valuable Table: Summary of Consumer Rights (CCPA vs. CPRA)

Consumer Right	**Origin**	**Brief Description**
Right to Know / Access	CCPA	Right to know what PI is collected, its sources, purposes, and third-party disclosures.[1]
Right to Delete	CCPA	Right to request deletion of PI collected *from* the consumer, subject to exceptions.[1]
Right to Opt-Out	CCPA	Right to opt-out of the *sale* of personal information.[1]
Right to Non-Discrimination	CCPA	Right not to be penalized for exercising CCPA rights.[1]
Right to Correct	CPRA	**New Right.** To request correction of inaccurate PI.[1]
Right to Limit SPI	CPRA	**New Right.** To limit the *use and disclosure* of Sensitive

		PI to specific permitted purposes.[1]
Right to Opt-Out of Sharing	CPRA	**Expanded Right.** Extends opt-out to "sharing" for cross-context behavioral advertising.[1]
Right to Access ADMT	CPRA / Regs	**New Right.** To access information about a business's use of Automated Decision-Making Technology.[45]

5. Special Focus: The Right to Limit Sensitive Personal Information (SPI)

The "Right to Limit" is one of the most operationally complex new rights introduced by the CPRA.[30] It allows a consumer to direct a business to *only* use their SPI for a set of specific, permitted purposes.[1]

Permitted Uses (The "Exceptions" to the Right)

A business is *not* required to offer the "Right to Limit" if it *only* uses SPI for purposes defined in the regulations.[44] These permitted uses include:

- Performing the services or providing the goods "reasonably expected by an average consumer" who requests them.[18]
- Performing services on behalf of the business, such as servicing accounts, processing payments, providing customer service, or providing storage.[18]
- Detecting security incidents, resisting fraudulent activity, and ensuring physical safety.[18]
- **Crucially:** Collecting or processing SPI *where such collection or processing is not used for the purpose of inferring characteristics about a consumer*.[18]

This last exception reveals the true nature of the right. It is not a right to block the *collection* of SPI; it is a right to block *secondary, inferential uses* of that data. This provision is the law's primary tool against invasive profiling.

For example, a consumer must provide SPI (e.g., a credit card number and security code) to complete a purchase. This is a "permitted use".[18] However, that business might also want to use the consumer's *precise geolocation* (also SPI) to *infer* characteristics about them, such as "frequent visitor to high-end stores," and then use that profile for targeted advertising. The "Right to Limit" [6] and the exception in [18] directly target this secondary, inferential step. The consumer can effectively state, "You may use my geolocation to provide me with map services, but you may *not* use it to infer characteristics about my lifestyle."

This creates an enormous technical and data governance challenge. Businesses must map *all* uses of SPI and tag them as "Permitted" or "Inferential." If *any* "Inferential" use exists, the "Limit" link must be offered. When a consumer clicks it, the business must have a technical mechanism to *sever the data flow* of that consumer's SPI to the inferential/profiling models, while *still allowing* it to flow to the "Permitted" operational systems, such as payment processing.

Implementation Mechanics

- **The "Limit" Link:** Businesses that use SPI for any purpose *other* than the permitted uses must provide a "clear and conspicuous link" on their website labeled "Limit the Use of My Sensitive Personal Information".[6]
- **Combined Link:** The regulations permit a single, combined link, such as "Your Privacy Choices" or "Your California Privacy Choices," that allows a consumer to exercise *both* the Right to Opt-Out of Sale/Sharing and the Right to Limit SPI.[6]
- **Procedural Rules:** The method for submitting the request must be easy for consumers to execute, require minimal steps [44], and must *not* require the consumer to create an account.[44]
- **Flow-Down:** Upon receiving a request, the business must notify all its service providers or contractors that use the SPI and instruct them to comply with the consumer's request within 15 business days.[44]

6. Operationalizing Compliance: Business Obligations and Processes

The CCPA mandates specific policies and procedures for businesses to operationalize these consumer rights.

Notice and Transparency

- **Notice at Collection (NaC):** A business must provide a notice *at or before* the point of PI collection.[1] This notice must be easy to understand [36] and must include:
    - The categories of PI and SPI to be collected.[36]
    - The purposes for which the PI/SPI is collected or used.[36]
    - Whether the PI/SPI is *sold or shared*.[36]
    - **Data Retention:** The length of time the business intends to retain *each category* of PI/SPI.[36] This is a critical new requirement, and vague statements like "as long as reasonably necessary" are non-compliant.[38]
    - A link to the business's privacy policy and, if applicable, the Notice of Right to Opt-out.[36]
- **Privacy Policy:** A business must maintain a comprehensive, online privacy policy that is updated at least every 12 months.[53] This policy must:
    - Provide a detailed description of all consumer rights (Know, Delete, Correct, Opt-Out, Limit) and *how* to exercise them.[14]
    - Explain the process for submitting a "verifiable consumer request".[14]
    - List the categories of PI the business has collected, sold, shared, and/or disclosed for a business purpose in the *preceding 12 months*.[14]
    - Identify the *sources* from which PI is collected.[14]
    - State the *purposes* for collection and use.[14]
    - Include links to "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" (or a combined "Your Privacy Choices" link).[53]
    - Be accessible, using plain language, a format readable on small screens, and be available in any language in which the business provides contracts or other key information to consumers.[53]

Responding to Consumer Requests: Timelines and Verification

Businesses must have a process to verify the identity of the consumer making a request to

Know, Delete, or Correct.[55] This process cannot require the consumer to create an account [44] and must first attempt to match the information provided by the consumer with data the business already maintains.[55]

The timelines for responding are strict and differ by request type.

Valuable Table: Mandated Timelines for Responding to Consumer Requests

Request Type	**Acknowledge Receipt**	**Substantive Response**	**Extension Period**
Know	10 *business* days [6]	45 *calendar* days [6]	+45 calendar days (90 total) with notice [6]
Delete	10 *business* days [6]	45 *calendar* days [6]	+45 calendar days (90 total) with notice [6]
Correct	10 *business* days [6]	45 *calendar* days [6]	+45 calendar days (90 total) with notice [6]
Opt-Out (Sale/Sharing)	Not specified; must act.	**15 *business* days** to comply [6]	N/A
Limit SPI	Not specified; must act.	**15 *business* days** to comply [6]	N/A
Access ADMT	10 *business* days [55]	45 *calendar* days [55]	+45 calendar days (90 total) with notice

Data Security: The "Reasonable Security" Standard

The CCPA mandates that businesses "implement and maintain reasonable security procedures and practices" to protect PI.[58] This requirement is the sole basis for the law's private right of action.

Critically, the statute itself *does not* define "reasonable security".[61] However, authoritative guidance exists. The 2016 California Attorney General's Data Breach Report *endorsed* the **CIS Critical Security Controls (CIS 20)** as establishing a "minimum level of information security".[61] The report explicitly stated that the "failure to implement all the Controls that apply... constitutes a lack of reasonable security".[62] Other frameworks, such as the NIST Cybersecurity Framework, are also considered reliable guidance.[61]

This endorsement effectively establishes a *de facto* legal standard. In a class-action lawsuit following a data breach, the plaintiff's argument will hinge on proving the business's "failure to implement... reasonable security".[60] The most direct way to do this is to hire an expert to audit the breached company against the CIS 20 controls. Therefore, a business's single best *defensive* measure against data breach liability is to have *already* conducted an audit against the CIS 20 (or NIST) and to have *documented* its implementation. This documentation becomes the core of the legal defense.

7. The New Frontier: ADMT, Risk Assessments, and Cybersecurity Audits

In September 2025, the CPPA's new regulations for Automated Decision-Making Technology (ADMT), Risk Assessments, and Cybersecurity Audits were approved.[35] These rules, effective January 1, 2026, with phased-in compliance dates, shift the CCPA from a purely consumer-rights law to a comprehensive corporate governance and accountability framework.[2]

Automated Decision-Making Technology (ADMT)

- **Scope:** These rules apply to a business's use of ADMT to make "significant decisions" about consumers, such as those affecting their employment, housing, credit, education, or healthcare.[48] The final rules narrowed the definition to ADMT that "replaces or substantially replaces human decision-making," thereby excluding routine automation tools.[65]

- **Consumer Rights:** Consumers are granted new rights regarding ADMT:
  1. **Pre-Use Notice:** Businesses must provide a clear notice *before* using ADMT for a significant decision.[48]
  2. **Right to Opt-Out:** Businesses must provide an option to opt-out of the use of ADMT, subject to certain exceptions.[35]
  3. **Right to Access:** Consumers can request information about the ADMT, which must include a "plain language" description of the ADMT's *logic*, how it processed their PI, and how the business used the output in making its decision.[45]

Mandatory Risk Assessments

- **Scope:** Businesses are required to conduct and document risk assessments for "high-risk processing activities," which includes the use of ADMT for significant decisions and the processing of SPI.[35]
- **Obligations:** The assessment must be reviewed and approved by a senior executive or other individual with authority.[49] Businesses must then submit an *attestation* and a *summary* of their completed assessments to the CPPA.[35]

Annual Cybersecurity Audits

- **Scope:** Businesses meeting specified revenue or data processing thresholds will be required to conduct an annual cybersecurity audit.[35]
- **Obligations:** Businesses must submit certifications of their completed audits to the CPPA on a phased-in schedule.[66]

This new regulatory regime, particularly the requirements for *executive attestation* [49] and *submissions to the CPPA* [66], fundamentally changes the nature of compliance. This "SOX-ification" of privacy mirrors the Sarbanes-Oxley Act's model for financial reporting. Privacy ceases to be merely an internal policy matter for legal and IT; it becomes a formal, auditable, C-suite-level responsibility. A senior executive will now be *personally accountable* to regulators for the company's data privacy risk posture, elevating privacy to a core element of corporate governance and risk.

Valuable Table: Compliance Deadlines for New Regulations

Compliance Obligation	Requirement	Compliance Date	Source(s)
New Regulations Effective	New rules for Audits, Risk Assessments, ADMT	**January 1, 2026**	[2]
Risk Assessments	Businesses must *begin* conducting risk assessments.	**January 1, 2026**	[66]
ADMT Regulations	Businesses must comply with ADMT requirements.	**January 1, 2027**	[65]
ADMT Access Requests	Businesses must be ready to respond to access requests.	**April 1, 2027**	[35]
Risk Assessment Submissions	Submit first attestation & summary to CPPA.	**April 1, 2028**	[35]
Cybersecurity Audit (Tier 1)	Submission due (Biz > $100M revenue).	**April 1, 2028**	[66]
Cybersecurity Audit (Tier 2)	Submission due (Biz $50M-$100M revenue).	**April 1, 2029**	[66]
Cybersecurity Audit (Tier 3)	Submission due (Biz < $50M revenue).	**April 1, 2030**	[66]

8. Enforcement, Penalties, and Key Precedents

The CCPA has significant enforcement "teeth," wielded by two bodies.

Dual Enforcement and Penalties

The CCPA is enforced by both the California Attorney General [10] and the CPPA.[2] These agencies can levy significant civil penalties:

- Up to **$2,500** per *non-intentional* violation.[9]
- Up to **$7,500** per *intentional* violation.[9]
- Up to **$7,500** for *any* violation involving the personal information of minors under 16.[9]

These penalties are "per-capita," meaning they can be assessed *per consumer* whose right was violated, which can lead to catastrophic fines in large-scale non-compliance cases.[68] Critically, the CPRA *removed* the mandatory 30-day "right to cure" for businesses in AG or CPPA enforcement actions.[69] Enforcement can now be immediate and without warning.

Case Study: The *Sephora* Settlement (August 2022)

The first major public CCPA settlement was against Sephora, which agreed to pay a $1.2 million fine.[42] The AG's allegations centered on three key failures [42]:

1. Failing to disclose to consumers that it "sells" their PI.
2. Failing to post a "Do Not Sell My Personal Information" link.
3. Failing to honor GPC (Global Privacy Control) opt-out signals.

The most critical legal interpretation from this case was the AG's successful argument that Sephora's *exchange* of customer PI with third-party analytics and advertising partners (via website cookies and pixels) in return for *services* constituted a "sale" under the CCPA's "other valuable consideration" clause.[24]

The settlement also highlighted a failed defense. The AG noted that such a transfer *would not* have been a "sale" if Sephora had valid, CCPA-compliant "service provider" contracts in place with these third parties.[73] Sephora did not, and its privacy policy explicitly stated it did not sell data, which the AG found to be false.[42] The actionable lesson from *Sephora* is that a properly-drafted, CCPA-compliant "Service Provider" contract (or Data Processing Addendum) is the primary legal shield that prevents a data transfer to an analytics or marketing vendor from being classified as a "sale" or "sharing."

The Private Right of Action (PRA)

The CCPA also grants a limited private right of action to consumers, but *only* for data breaches.[60] It does *not* apply to violations of other rights (e.g., a failure to delete data).

- **Legal Standard:** The PRA is triggered when a consumer's *nonencrypted and nonredacted* personal information is subject to unauthorized access, exfiltration, theft, or disclosure *caused by* the business's failure to "implement and maintain reasonable security".[60]
- **Damages:** Consumers can sue for statutory damages of **$100 to $750 per consumer, per incident,** or their actual damages, whichever is greater.[60]
- **Right to Cure:** For the PRA *only*, the 30-day "right to cure" remains. A consumer must give the business 30-day notice before suing for statutory damages.[1] The "violation" is the *failure* to maintain reasonable security, not the breach itself. Therefore, the "cure" is for the business to implement reasonable security (e.g., the missing CIS 20 controls) within that 30-day window and provide a written statement that no further violations will occur.[1] This makes rapid, post-breach remediation a critical legal strategy to stop a class-action lawsuit.

9. Nuanced Applications and Evolving Scope

The End of the Exemptions: Full Applicability to HR and B2B Data

As of January 1, 2023, the temporary and partial exemptions for employee/applicant (HR) data and business-to-business (B2B) data *expired*.[1]

This is a monumental shift. Employees, job applicants, independent contractors [76], and B2B contacts are now "consumers" under the law and are entitled to the *full* suite of CCPA rights, including the rights to Know, Delete, Correct, Limit SPI, and Opt-Out of Sale/Sharing.[76]

This expiration imposes significant new obligations on employers, who must now:

- Provide a "Notice at Collection" to all job applicants and employees.[69]
- Update their main CCPA privacy policy to reflect the processing of HR data.[69]
- Establish and manage a process for receiving and responding to HR-DSARs (Data Subject Access Requests).[82]
- Ensure all HR-related vendors (e.g., payroll providers, benefits administrators) have CCPA-compliant "service provider" contracts in place.[81]

This is not a theoretical risk. In July 2023, the California Attorney General announced an *immediate* enforcement sweep targeting large California employers for non-compliance with these new HR data requirements.[69] This action signaled that regulators view HR data as a high-priority area and *would not wait* for further CPPA rulemaking to begin enforcement.[82]

The extension of CCPA rights to employees also creates a powerful new pre-litigation discovery tool for employment lawyers. The "Right to Know" is broader in some respects than the existing right to a personnel file [76], as it allows an employee to request "inferences drawn" [15] or "internal research" [21] that might relate to performance, promotion, or termination. A disgruntled employee can use a "Right to Know" request to find evidence for a discrimination or wrongful termination lawsuit. This high-risk legal dynamic means that HR-DSAR processes must be co-managed by the Legal and HR departments, not just IT.

Tracking Technologies: Cookies and Pixels as "Sale/Sharing"

As established in the *Sephora* settlement, it is the clear position of California regulators that the use of third-party cookies, pixels, and other tracking technologies for analytics or cross-context behavioral advertising *constitutes* a "sale" or "sharing" of personal information.[25] This means businesses *must* provide a clear "Do Not Sell or Share" link that disables these trackers for opting-out consumers and *must* honor GPC signals.[41]

10. Exemptions and Federal Interactions

A common and costly compliance mistake is the belief that entities in regulated industries are exempt from the CCPA. The CCPA's primary exemptions are *data-level*, not *entity-level*.[86]

- **HIPAA:** The CCPA exempts "Protected Health Information" (PHI) that is collected by a "covered entity" or "business associate" subject to HIPAA.[86] *However*, any non-PHI data collected by that same entity—such as employee HR data, job applicant data, or website marketing data—is *fully subject* to the CCPA.[86]
- **Gramm-Leach-Bliley Act (GLBA):** The CCPA exempts "Nonpublic Personal Information" (NPI) collected by financial institutions subject to the GLBA.[87] *However*, the CCPA's *private right of action for a data breach still applies* to this data.[87]
- **Fair Credit Reporting Act (FCRA):** The CCPA exempts personal data handled by consumer reporting agencies under the FCRA.[86] As with the GLBA, the *private right of action for a data breach still applies*.[86]

The only full *entity-level* exemptions are for non-profit organizations and government agencies.[86]

This data-level, "patchwork" [91] model creates a compliance burden that is arguably *more* complex than being subject to one law or the other. A hospital, for example, is not "HIPAA-exempt." It must run *two parallel compliance programs*: a HIPAA program for patient data (PHI) and a *full CCPA program* for all other "consumer" data, which now includes its website visitors, employees, and job applicants. This requires bifurcated data systems, separate DSAR-intake portals that can distinguish a patient (HIPAA) request from an employee (CCPA) request, and dual-track training for staff.

11. Strategic Recommendations for End-to-End Compliance

Based on the foregoing analysis, a comprehensive compliance strategy should prioritize the following actions:

1. **Prioritize Data Mapping:** The foundation of all compliance is knowing what data is collected, where it is stored, and where it flows. This data mapping exercise must now be expanded to include all HR data [82], B2B data [93], and must *specifically* tag all categories of SPI to enable compliance with the "Right to Limit".[17]
2. **Audit and Remediate Vendor Contracts:** In light of the *Sephora* precedent [25], the single most urgent task is to review *all* vendor contracts—especially for HR/payroll [81], analytics, and marketing—to ensure they contain the CCPA-mandated "service provider" clauses. This is the primary legal defense against "sale/sharing" allegations.[73]
3. **Implement a GPC-Compliant Cookie Banner:** The *Sephora* case [42] and AG statements

[41] confirm that honoring the Global Privacy Control signal is not optional. A cookie consent tool must be configured to recognize GPC signals as a valid opt-out of "sale/sharing" and automatically disable the relevant trackers.

4. **Develop a "New Wave" Compliance Roadmap:** Use the timeline in Table 5 to begin long-range planning *now* for the 2026–2027 deadlines. This includes inventorying *all* ADMT use cases [48], developing a "high-risk processing" inventory to scope risk assessment obligations [35], and conducting a gap analysis of security practices against the CIS 20 Controls [61] to prepare for audits and defend against the private right of action.
5. **Operationalize HR and B2B DSAR Workflows:** Establish a distinct intake and processing workflow for data requests from employees, applicants, and B2B contacts.[82] This process must be co-owned by Legal, HR, and IT to manage the high litigation risk inherent in employee data requests.[76]
6. **Overhaul Transparency Disclosures:** All Notices at Collection and Privacy Policies must be updated to include HR and B2B data processing activities [69], *specific* data retention periods *per category* of PI [36], and clear, conspicuous, and (if desired) combined links for "Do Not Sell/Share" and "Limit SPI".[6]

Works cited

1. California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General, accessed November 7, 2025, https://oag.ca.gov/privacy/ccpa
2. Law & Regulations - California Privacy Protection Agency (CPPA), accessed November 7, 2025, https://cppa.ca.gov/regulations/
3. CCPA and CPRA - IAPP, accessed November 7, 2025, https://iapp.org/resources/topics/ccpa-and-cpra/
4. California Consumer Privacy Act, California Privacy Rights Act FAQs for Covered Businesses - Jackson Lewis, accessed November 7, 2025, https://www.jacksonlewis.com/insights/california-consumer-privacy-act-california-privacy-rights-act-faqs-covered-businesses
5. About Us - California Privacy Protection Agency (CPPA) - CA.gov, accessed November 7, 2025, https://cppa.ca.gov/about_us/
6. Frequently Asked Questions (FAQs) - California Privacy Protection ..., accessed November 7, 2025, https://cppa.ca.gov/faq.html
7. California Privacy Protection Agency (CPPA) - CA.gov, accessed November 7, 2025, https://www.ca.gov/departments/315/
8. accessed November 7, 2025, https://cppa.ca.gov/regulations/#:~:text=The%20Agency%20is%20responsible%20for,rulemaking%20process%20under%20both%20laws.
9. Meet the California Privacy Protection Agency (CPPA) - Osano, accessed November 7, 2025, https://www.osano.com/articles/california-privacy-protection-agency
10. CCPA Text – California Consumer Privacy Act As Amended by SB-1121 - Clarip,

accessed November 7, 2025, https://www.clarip.com/data-privacy/ccpa-text/

11. Who Does CCPA Apply To? 5 Key Criteria - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/blog/who-does-ccpa-apply-to/
12. The California Privacy Rights Act: Determining if a Business Qualifies under New California Privacy Law Amendments - Butzel Long, accessed November 7, 2025, https://www.butzel.com/alert-the-california-privacy-rights-act-determining-if-a-business
13. Comprehensive FAQs on the CCPA - Fisher Phillips, accessed November 7, 2025, https://www.fisherphillips.com/en/news-insights/comprehensive-faqs-on-the-ccpa.html
14. CCPA Privacy Policy: The Complete Guide - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/blog/ccpa-privacy-policy/
15. What is personal information? - privacy.ca.gov, accessed November 7, 2025, https://privacy.ca.gov/protect-your-personal-information/what-is-personal-information/
16. Personal vs. Sensitive Personal Information - Termly, accessed November 7, 2025, https://termly.io/resources/articles/sensitive-personal-information/
17. 6 Key CCPA Rights Every Consumer Should Know - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/blog/ccpa-rights/
18. “Sensitive Personal Information” – Understanding and Complying with the New Rules in the United States | BCLP, accessed November 7, 2025, https://www.bclplaw.com/en-US/events-insights-news/sensitive-personal-information-understanding-and-complying-with-the-new-rules-in-the-united-states.html
19. What is CPRA Sensitive Personal Information and How to Handle it? - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/blog/cpra-sensitive-personal-information/
20. California Expands Definition of Sensitive Personal Information Covered Under CCPA | Akin, accessed November 7, 2025, https://www.akingump.com/en/insights/blogs/ag-data-dive/california-expands-definition-of-sensitive-personal-information-covered-under-ccpa
21. What is a CCPA business purpose or commercial purpose? - Clarip, accessed November 7, 2025, https://www.clarip.com/data-privacy/ccpa-business-commercial-purposes/
22. California Consumer Privacy Act: A Compliance Guide - Skadden, accessed November 7, 2025, https://www.skadden.com/-/media/files/publications/2019/03/cybersecurity_california_privacy.pdf?la=en
23. What is a CPRA Business Purpose or Commercial Purpose? - Captain Compliance, accessed November 7, 2025, https://captaincompliance.com/education/what-is-a-cpra-business-purpose-or-commercial-purpose/
24. CCPA enforcement action: A case study at the intersection of privacy and marketing | IAPP, accessed November 7, 2025, https://iapp.org/news/a/ccpa-enforcement-action-a-case-study-at-the-intersecti

on-of-privacy-and-marketing

25. CCPA Enforcement: The Sephora Settlement Is Just the Start - Troutman Pepper Locke, accessed November 7, 2025, https://www.troutman.com/insights/ccpa-enforcement-the-sephora-settlement-is-just-the-start/
26. Cross-Context Behavioral Advertising: What You Need to Know - Usercentrics, accessed November 7, 2025, https://usercentrics.com/knowledge-hub/cross-context-behavioral-advertising/
27. What is cross-context behavioral advertising in CPRA? - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/knowledge-base/ccpa/cross-context-behavioral-advertising/
28. Marketing & the CPRA | What do you need to know | Cross-context Behavioral Advertising, accessed November 7, 2025, https://secureprivacy.ai/blog/cpra-cross-context-behavioral-advertising
29. Digital Trackers & Data Protection: How the CPRA Closes CCPA Gaps in Addressing Cross-Contextual Behavioral Tracking - California Lawyers Association, accessed November 7, 2025, https://calawyers.org/business-law/digital-trackers-data-protection-how-the-cpra-closes-ccpa-gaps-in-addressing-cross-contextual-behavioral-tracking/
30. Text of the CPRA - Californians for Consumer Privacy, accessed November 7, 2025, https://www.caprivacy.org/cpra-text/
31. Your Guide to CCPA: California Consumer Privacy Act - TrustArc, accessed November 7, 2025, https://trustarc.com/resource/ccpa-guide/
32. California Consumer Privacy Act FAQs for Covered Businesses - Jackson Lewis, accessed November 7, 2025, https://www.jacksonlewis.com/insights/california-consumer-privacy-act-faqs-covered-businesses
33. CCPA Look Back Period Requirement - Clarip, accessed November 7, 2025, https://www.clarip.com/data-privacy/ccpa-look-back/
34. The CCPA's 12-Month Look Back Period May Extend Beyond That, accessed November 7, 2025, https://www.troutman.com/insights/the-ccpas-12-month-look-back-period-may-extend-beyond-that/
35. California Finalizes CCPA Regulations for Automated Decision-Making Technology, Risk Assessments and Cybersecurity Audits | Insights | Skadden, Arps, Slate, Meagher & Flom LLP, accessed November 7, 2025, https://www.skadden.com/insights/publications/2025/10/california-finalizes-cppa-regulations
36. What General Notices Are Required By The CCPA? - California Privacy Protection Agency, accessed November 7, 2025, https://cppa.ca.gov/pdf/general_notices.pdf
37. Wells Fargo California Consumer Privacy Act Notice and Notice at Collection, accessed November 7, 2025, https://www.wellsfargo.com/privacy-security/notice-of-data-collection/
38. Breaking News: California Can Immediately Enforce CCPA Regulations – Your

7-Step Plan for Data Privacy Compliance | Fisher Phillips, accessed November 7, 2025, https://www.fisherphillips.com/en/news-insights/california-can-immediately-enforce-ccpa-regulations.html

39. Applying the 9 CCPA Exemptions to Deletion Requests - Clarip, accessed November 7, 2025, https://www.clarip.com/data-privacy/ccpa-erasure-exemptions/
40. CCPA Explained: Complete Guide to California Privacy Compliance - Osano, accessed November 7, 2025, https://www.osano.com/ccpa
41. California Consumer Privacy Act: what is CCPA compliance? - Cookie Information, accessed November 7, 2025, https://cookieinformation.com/regulations/ccpa/
42. $1.2 Million CCPA Settlement with Sephora Focuses on Sale of Personal Information and Global Privacy Controls | Crowell & Moring LLP, accessed November 7, 2025, https://www.crowell.com/en/insights/client-alerts/1-2-million-ccpa-settlement-with-sephora-focuses-on-sale-of-personal-information-and-global-privacy-controls
43. Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act, accessed November 7, 2025, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement
44. 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information. - View Document - California Code of Regulations - Westlaw, accessed November 7, 2025, https://govt.westlaw.com/calregs/Document/IF443CE30D45011ED9036C8DABB00C18F?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)
45. The six CCPA rights of California consumers - Cookiebot, accessed November 7, 2025, https://www.cookiebot.com/en/ccpa-rights-for-consumers-ccpa-compliance-with-cookiebot-cmp/
46. CCPA Compliance Guide | Coalition, accessed November 7, 2025, https://www.coalitioninc.com/topics/ccpa-compliance-guide
47. How to Handle Consumer Requests Under CCPA (Before it's too late!) | TrustArc, accessed November 7, 2025, https://trustarc.com/resource/handle-consumer-requests-under-ccpa/
48. Automated Decision-Making Under the Microscope: CPPA Finalizes New CCPA Rules, accessed November 7, 2025, https://www.lowenstein.com/news-insights/publications/client-alerts/automated-decision-making-under-the-microscope-cppa-finalizes-new-ccpa-rules-data-privacy
49. California's Long-Awaited Final Regulations on Automated Decisionmaking Create New Compliance Challenges for Employers | Littler, accessed November 7, 2025, https://www.littler.com/news-analysis/asap/californias-long-awaited-final-regulati

ons-automated-decisionmaking-create-new

50. How to Comply With the CPRA's "Limit the Use of My Sensitive Personal Information" Requirement - TermsFeed, accessed November 7, 2025, https://www.termsfeed.com/blog/how-comply-cpra-limit-use-sensitive-personal-information/
51. Notice at Collection (CCPA and CPRA) - Westlaw, accessed November 7, 2025, https://content.next.westlaw.com/Link/Document/Blob/Ied14254c869611ed8636e1a02dc72ff6.pdf?targetType=PLC-multimedia&originationContext=document&transitionType=DocumentImage&uniqueId=508808f3-0368-4178-b282-a38d260d40f8&ppcid=e5ba0e9d3615488abd85416e972616e0&contextData=(sc.DocLink)
52. Cal. Code Regs. Tit. 11, § 7012 - Notice at Collection of Personal Information, accessed November 7, 2025, https://www.law.cornell.edu/regulations/california/11-CCR-7012
53. CCPA Privacy Policy: Requirements and Best Practices - Cookiebot, accessed November 7, 2025, https://www.cookiebot.com/en/ccpa-privacy-policy/
54. What Is a CCPA Privacy Policy? Do You Need One? - Bloomberg Law, accessed November 7, 2025, https://pro.bloomberglaw.com/insights/privacy/what-is-a-ccpa-privacy-policy-do-you-need-one/
55. Guide to CCPA Regulations Modifications, accessed November 7, 2025, https://www.mmmlaw.com/news-resources/102l0gn-guide-to-ccpa-regulations-modifications/
56. LOCKED Series: Right to Equal Treatment & Right to Delete - privacy.ca.gov, accessed November 7, 2025, https://privacy.ca.gov/2025/08/locked-series-right-to-equal-treatment-right-to-delete/
57. Summary of California Consumer Rights and Business Deadlines for Responding to Privacy-Related Requests | Fisher Phillips, accessed November 7, 2025, https://www.fisherphillips.com/en/news-insights/summary-california-consumer-rights-business-deadlines-for-responding-to-privacy-related-requests.html
58. CCPA Requirements: What Is Reasonable Security? - tenfold, accessed November 7, 2025, https://www.tenfold-security.com/en/ccpa-security-requirements/
59. Reasonable Security Measures Under the CCPA/CPRA - TermsFeed, accessed November 7, 2025, https://www.termsfeed.com/blog/ccpa-reasonable-security-measures/
60. Year in Review: CCPA Litigation Trends from 2023 - WilmerHale, accessed November 7, 2025, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240226-year-in-review-ccpa-litigation-trends-from-2023
61. CCPA Is Here – Is Your Security "Reasonable"? | Global Privacy ..., accessed November 7, 2025, https://www.stoelprivacyblog.com/2020/01/articles/uncategorized/ccpa-is-here-is-your-security-reasonable/
62. CCPA: Proposed Bill Would Link Reasonable Security to NIST Standards | Byte

Back, accessed November 7, 2025, https://www.bytebacklaw.com/2019/05/ccpa-proposed-bill-would-link-reasonable-security-to-nist-standards/

63. CCPA Requires "Reasonable Security": but You Can't have Reasonable Security Without Proper Vulnerability Management | News & Resources | Dorsey, accessed November 7, 2025, https://www.dorsey.com/newsresources/publications/client-alerts/2019/09/ccpa-requires-reasonable-security
64. California Unleashes Groundbreaking AI Regulations: A Wake-Up Call for Businesses, accessed November 7, 2025, https://markets.financialcontent.com/wral/article/tokenring-2025-11-6-california-unleashes-groundbreaking-ai-regulations-a-wake-up-call-for-businesses
65. California's ADMT Regulations Reshape the AI Business Landscape, accessed November 7, 2025, https://www.jdsupra.com/legalnews/california-s-admt-regulations-reshape-9616681/
66. California Finalizes Regulations to Strengthen Consumers' Privacy, accessed November 7, 2025, https://cppa.ca.gov/announcements/2025/20250923.html
67. California Consumer Privacy Act (CCPA): An Overview - Usercentrics, accessed November 7, 2025, https://usercentrics.com/knowledge-hub/california-consumer-privacy-act/
68. Top 5 Operational Impacts of CCPA: Part 5 - Penalties and enforcement mechanisms | IAPP, accessed November 7, 2025, https://iapp.org/news/a/top-5-operational-impacts-of-cacpa-part-5-penalties-and-enforcement-mechanisms
69. Looking ahead to 2024: California privacy law action items for employers, accessed November 7, 2025, https://www.theemployerreport.com/2023/12/looking-ahead-to-2024-california-privacy-law-action-items-for-employers/
70. CCPA Settlement Illustrates Continued Focus on the Sale of Consumer Personal Information, accessed November 7, 2025, https://www.whitecase.com/insight-alert/ccpa-settlement-illustrates-continued-focus-sale-consumer-personal-information
71. Not So Pretty: Five Takeaways from New CCPA Settlement with Sephora and Other Enforcements, accessed November 7, 2025, https://www.troutman.com/insights/not-so-pretty-top-takeaways-from-first-ccpa-settlement-with-sephora-and-updated-enforcement-case-examples/
72. First CCPA Enforcement Action's $1.2 Million Fine to Sephora is a Wakeup Call for the Ad Tech Industry - Davis+Gilbert LLP, accessed November 7, 2025, https://www.dglaw.com/first-ccpa-enforcement-actions-1-2-million-fine-to-sephora-is-a-wakeup-call-for-the-ad-tech-industry/
73. CCPA Do Not Sell My Personal Information: An Overview - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/blog/do-not-sell-my-personal-information/
74. CCPA Fines & Penalties: What Happens if You Fail to Comply? - CookieYes,

accessed November 7, 2025, https://www.cookieyes.com/blog/ccpa-fines/

75. CCPA penalties and fines: What are the consequences of noncompliance? - Usercentrics, accessed November 7, 2025, https://usercentrics.com/knowledge-hub/ccpa-penalties/
76. California Consumer Privacy Act's Employee and Business-to-Business Exemptions Expire Effective January 1, 2023 How Should Employers Prepare? - Stinson LLP, accessed November 7, 2025, https://www.stinson.com/newsroom-publications-California-Consumer-Privacy-Acts-Employee-and-Business-to-Business-Exemptions-Expire-Effective-January-1-2023
77. California Consumer Privacy Act's Employee and B2B Exemptions to Expire on January 1, 2023 | Katten Muchin Rosenman LLP, accessed November 7, 2025, https://katten.com/california-consumer-privacy-acts-employee-and-b2b-exemptions-to-expire-on-january-1-2023
78. California Privacy Rights Act for Employers: The Rights to Opt Out of Sales and Sharing, Restrict Sensitive Personal Information, and Non-Discrimination | Littler, accessed November 7, 2025, https://www.littler.com/news-analysis/asap/california-privacy-rights-act-employers-rights-opt-out-sales-and-sharing
79. HR/Employee Data & B2B Data to Come Within Scope of CCPA on January 1, 2023 - California Lawyers Association, accessed November 7, 2025, https://calawyers.org/privacy-law/hr-employee-data-b2b-data-to-come-within-scope-of-ccpa-on-january-1-2023/
80. California Consumer Privacy Act: Employee and B2B Exemptions Expire January 1, 2023, accessed November 7, 2025, https://www.morganlewis.com/pubs/2022/10/california-consumer-privacy-act-employee-and-b2b-exemptions-expire-january-1-2023
81. Employee Data under the CCPA: Expiration of Employer Exemptions Requires Compliance as of January 1, 2023 - Farella Braun + Martel LLP, accessed November 7, 2025, https://www.fbm.com/publications/employee-data-under-the-ccpa-expiration-of-employer-exemptions-requires-compliance-as-of-january-1-2023/
82. California Attorney General's CCPA Sweep Indicates Focus on HR ..., accessed November 7, 2025, https://www.debevoise.com/insights/publications/2023/07/california-attorney-generals-ccpa-sweep-indicates
83. January 1, 2023 Expiration of Employee and B2B Exceptions to CCPA Raise Privacy Compliance Concerns for Private Fund Managers and Investment Advisers | Advisories | Arnold & Porter, accessed November 7, 2025, https://www.arnoldporter.com/en/perspectives/advisories/2023/01/january-1-2023-expiration-of-employee-and-b2b
84. Beyond the Breach: How CCPA Enforcement Is Targeting Website Cookies and Tracking, accessed November 7, 2025, https://cookie-script.com/news/how-ccpa-enforcement-is-targeting-website-cookies-and-tracking

85. Cross-context behavioral advertising is 'sale.' It is time to get over it ..., accessed November 7, 2025, https://iapp.org/news/a/cross-context-behavioral-advertising-is-sale-it-is-time-to-get-over-it
86. CCPA Exemptions: 7 Key Cases Where the Law Doesn't Apply - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/blog/ccpa-exemptions/
87. CCPA Exemptions: HIPAA, GLBA, and FCRA - TrueVault, accessed November 7, 2025, https://www.truevault.com/learn/ccpa-exemptions-hipaa-glba-and-fcra
88. Data Privacy Laws: What You Need to Know in 2025 - Osano, accessed November 7, 2025, https://www.osano.com/articles/data-privacy-laws
89. CPRA Exemptions Explained: A Business-Friendly Guide for 2025 - CookieYes, accessed November 7, 2025, https://www.cookieyes.com/blog/cpra-exemptions/
90. CCPA Exemptions: What They Really Mean for Health Companies - Datavant, accessed November 7, 2025, https://www.datavant.com/hipaa-privacy/ccpa-exemptions-what-they-really-mean-for-health-companies
91. Understanding Consumer Data Privacy Laws in the US, accessed November 7, 2025, https://thedataprivacygroup.com/us/blog/understanding-consumer-data-privacy-laws-in-the-us/
92. No More Exceptions: What to Do When the California Privacy Exemptions for Employee, Applicant and B2B Data Expire on January 1, 2023 - Workforce Bulletin, accessed November 7, 2025, https://www.workforcebulletin.com/no-more-exceptions-what-to-do-when-the-california-privacy-exemptions-for-employee-applicant-and-b2b-data-expire-on-january-1-2023
93. CCPA/CPRA grace period for HR and B2B ends Jan. 1 - IAPP, accessed November 7, 2025, https://iapp.org/news/a/ccpa-cpra-grace-period-for-hr-and-b2b-ends-jan-1