



From Emails to Algorithms: Emerging Public Records Challenges in the AI Era

Presented by Leah Castella, Partner and Alexandra Mulhall, Associate
Burke, Williams & Sorensen, LLP

League of California Cities, Spring
Conference - May 2026

A long way in a short time...

May 2010

California Discovery Act:

Beware the Myth of the Delete Button

J. Leah Castella, Esq.
McDonough Holland & Allen PC
1901 Harrison Street, 9th Floor
Oakland, CA 94612
(510) 273-8780
(510) 839-9104 fax
lcastella@mhalaw.com

May 2026

City Staff to Detail Limited Artificial Intelligence Pilots for City Operations, Stresses Staff Oversight and Data Safeguards

San Jose Warns Employees ChatGPT Use Is Public Record

The California city became one of the first to implement a strict set of guidelines for use of the artificial intelligence tool and clarified that ChatGPT is subject to the state's Public Records Act.

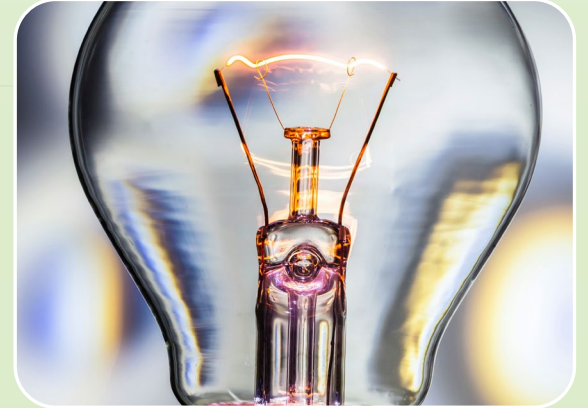
Latest News

HOUSING AND URBAN ISSUES

Cities Confront Fallout as Emerg
Vouchers Expire

April 28, 2026

Overview



What is a Public Record?

AI interactions, chats, and metadata under the CPRA

Record Retention

How long to keep AI, chat, and metadata records

Exemptions & Privilege Issues

Deliberative process, drafts, and waiver risks

Best Practices & Policies

AI for CPRA processing, internal policies, device search

What is a “public record” in
2026?

Public Records: An Administrative Double-Edged Sword

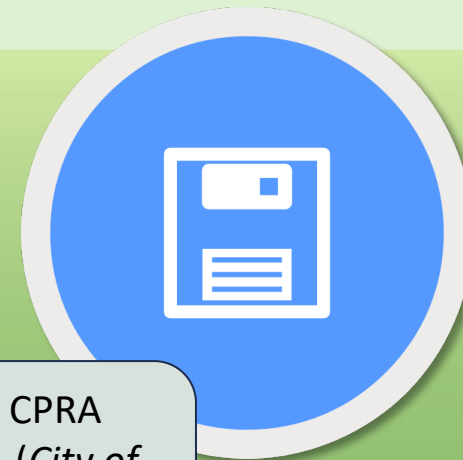
Public Records are Subject to Disclosure under the California Public Records Act

The CPRA ensures transparency in governance by granting members of the public the right to copy and inspect public records. (Gov. Code §§ 7920.000, et seq.)



Public Records are Subject to Record Retention Requirements

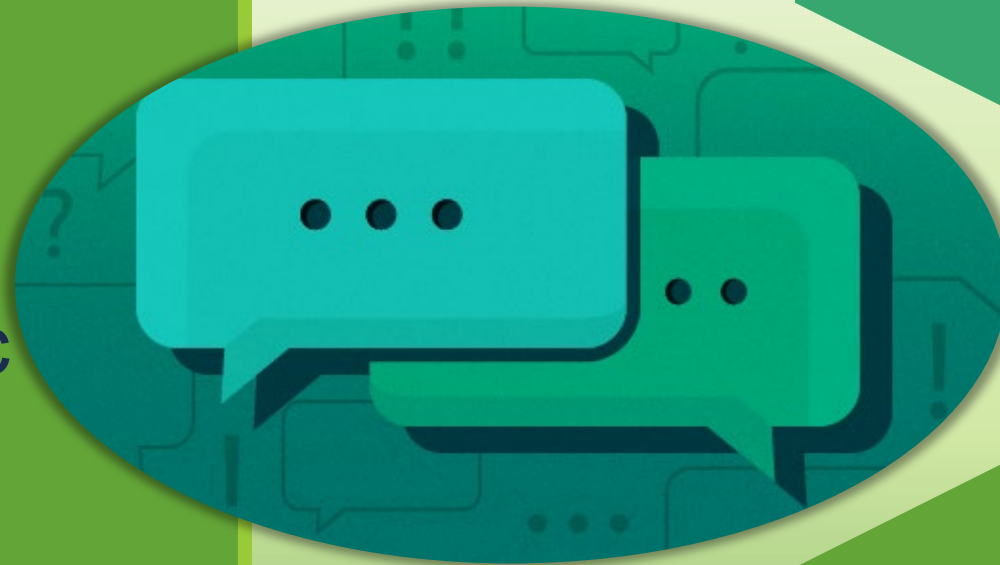
Public entities are required, by statute and regulations, to retain certain categories of documents for designated periods of time. (See, e.g., Gov. Code § 34090.)



Note: the CA Supreme Court recently confirmed that the CPRA does not impose any standalone retention requirements. (*City of Gilroy v. Superior Court of Santa Clara County* (Cal., Jan. 15, 2026, No. S282937) 2026 WL 111709.)



The Evolving Landscape of Potential Public Records



Social media DMs

Asking AI for drafting assistance (e.g., staff reports)

Asking AI for guidance or information (e.g., researching best practices or statistics)

Internal and external chat messages

Metadata from all electronic records

Using AI assistants to generate transcripts of meetings

AI Interactions as Public Records

- Courts have not directly addressed AI records under the CPRA
- Recommended to assume AI interactions are public records if they relate to the public's business
(See *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608, 618.)
- Utilize factors to determine if an AI interaction qualifies as a public record



"Any writing...relating to the conduct of the public's business prepared, owned, used, or retained by any...agency regardless of physical form."

Subject matter

Context & purpose of interaction

Whether employee using AI was acting in scope of employment

Chat Messages as Public Records

- California courts have made clear that records from messaging apps can qualify as public records (e.g., Microsoft Teams or Slack messages) (*City of San Jose v. Superior Court* (2017) 2 Cal.5th 608.) 
- When determining whether private messages relate to public business, courts will look to: (1) the subject matter of the messages; (2) the context or purpose of the messages; (3) whether the author was acting in the scope of public employment; and (4) the audience of the messages
- If a message is found to relate to public business under these factors, it is subject to disclosure, *even if the message is stored on a private account or device*
- Auto-delete apps and settings are discouraged to prevent public records from being prematurely deleted (e.g., disappearing messages on apps like Signal)

Metadata as a Public Record

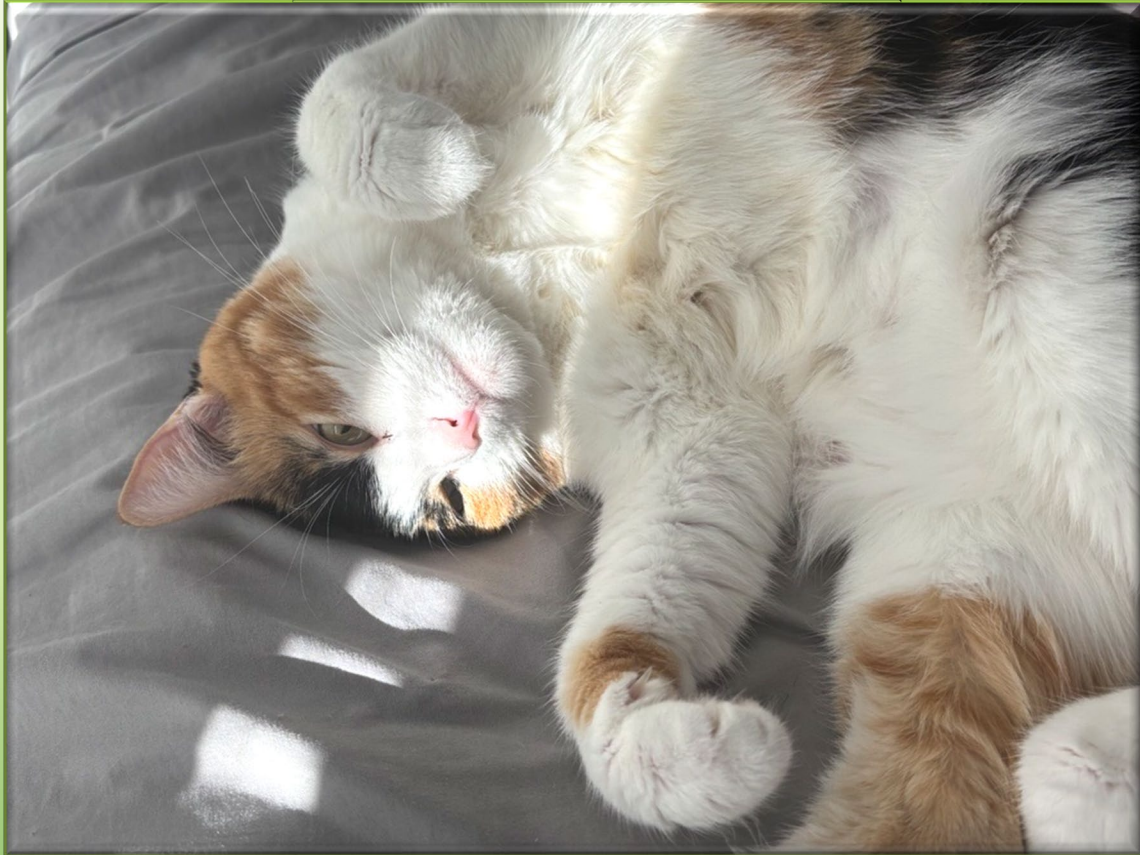
What is Metadata? The behind-the-scenes “data about data.” Not visible in the text of a record but provides details and context for the data it describes.

- Examples: information about the author of a document, document creation date, timestamps, device type, permissions, etc.
- Often Vital and Sensitive: Can contain personal or security info, crucial details for locating records, or even be necessary for preservation

Must Metadata be disclosed? Until CA courts hold otherwise, yes.

- Statutory support: CPRA requires production of native documents if requested (Gov. Code § 7922.570), supporting arguments that metadata must be disclosed
- Unique Exemption Considerations: Has a heightened likelihood of qualifying for exemptions based on privacy and security

The Data:



The Metadata:

Add a Caption

Information

File Name	IMG_2579.HEIC
Kind	HEIF Image
Size	2.2 MB
Created	July 8, 2025 at 7:32 AM
Modified	July 8, 2025 at 7:32 AM
Last Opened	April 28, 2026 at 6:35 PM
Dimensions	5712 × 4284
Image DPI	72 pixels/inch
Color Profile	Display P3
Device Make	Apple
Device Model	iPhone 15
Lens Model	iPhone 15 back dual wide camera 5.96mm f/1.6
Aperture Value	1.356
Exposure Time	1/591
Exposure Program	Normal
Focal Length	5.96 mm
ISO Speed	50
Flash	NO

Record Retention Requirements and Issues

The Problem: Data Storage



California law requires agencies to retain records in accordance with statute, regulations, and local retention schedules



For most records, this means they are retained for at least 2 years



Electronic files can create massive data to be stored, creating storage capacity and cost concerns



The Solution: Strategic Internal Policies

To manage the number of public records, public entities can utilize internal policies to guide record creation, including:

- Appropriate uses of certain technologies [e.g., use generative AI for brainstorming, but don't rely on it as a sole resource for policy decisions]
- When and where sensitive information may be used
- Guidance on when and how to save important records
- When agency-issued accounts are mandatory
- When/How to opt out of data collection



How Long Must Records be Kept?

Guiding Principle: Retain records based on their *content and purpose*, not their format.

AI INTERACTIONS

- Retain if content relates substantially to public business or a record series
- Create work-only AI accounts to separate personal use
- Save AI outputs that inform shared/final documents
- Simple queries (e.g., file format help) likely need not be retained
- Consider routine purges

CHAT MESSAGES

- Gov. Code § 34090 implies 2-year minimum for records
- Transitory messages (informal, short-lived) may arguably be purged sooner
- Policy must define custodian responsibilities for classification of chats
- Auto-deletion policies are legally defensible but carry litigation risk

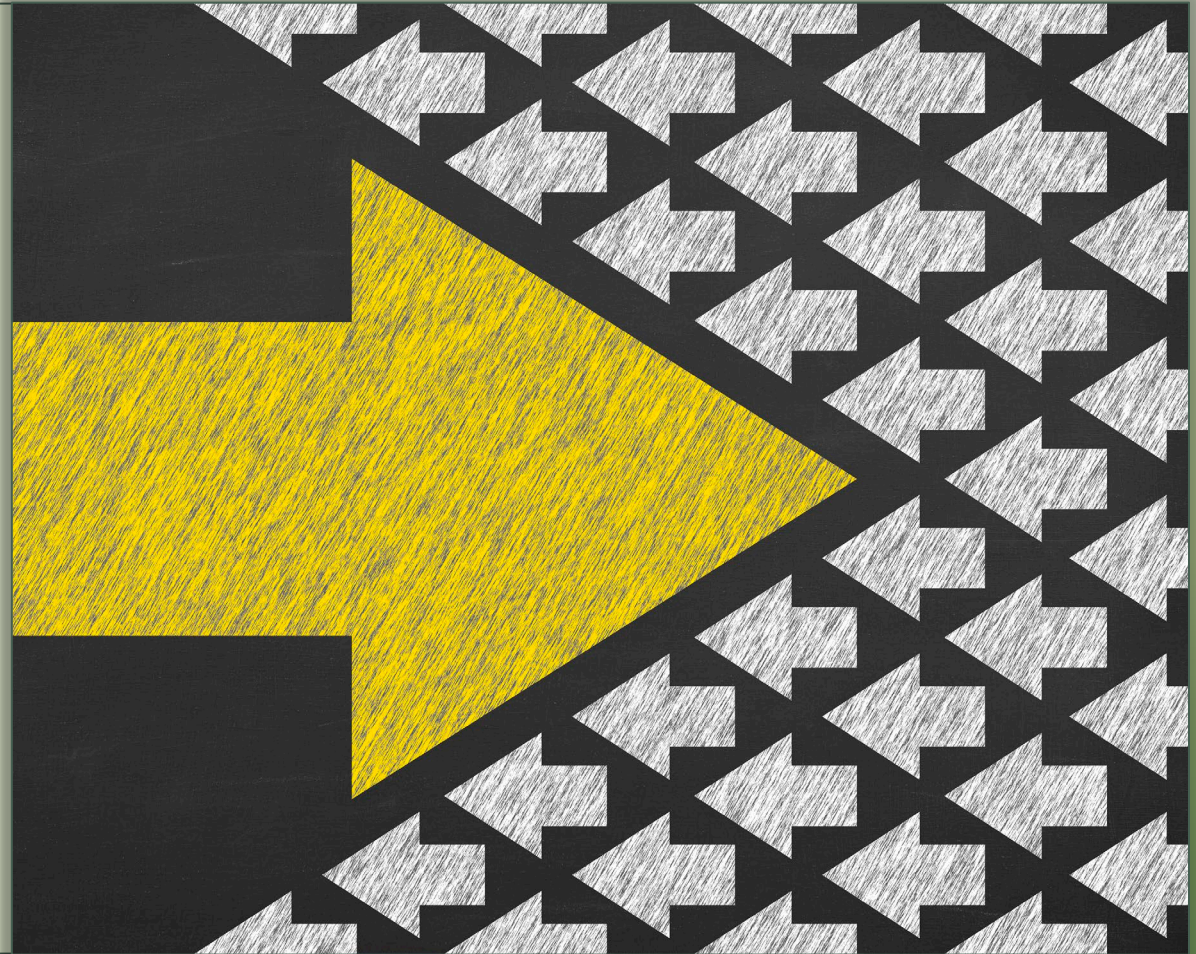
METADATA

- Retain alongside the primary record
- Retention period mirrors the primary document
- Coordinate with IT to prevent accidental loss during file conversion
- Review metadata before production to redact sensitive system data

Early Deletion of “Transitory” Chats

A Conflicting Legal Landscape:

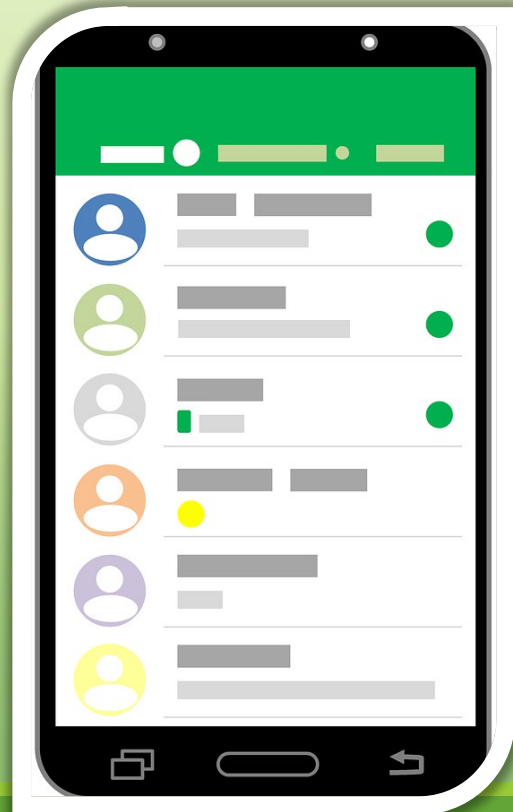
- Gov. Code sec. 34090 requires all records to be retained for at least 2 years
- Secretary of State guidelines provide that informal, short-lived, and/or limited purpose records may be destroyed once they served their purpose (e.g., informal emails and chats)
- Multiple bills have been introduced to explicitly require 2-year retention of emails, but all have failed ([AB 1184 \[2019\]](#); [AB 2093 \[2020\]](#); [AB 2370 \[2022\]](#).)



Early Deletion of “Transitory” Chats

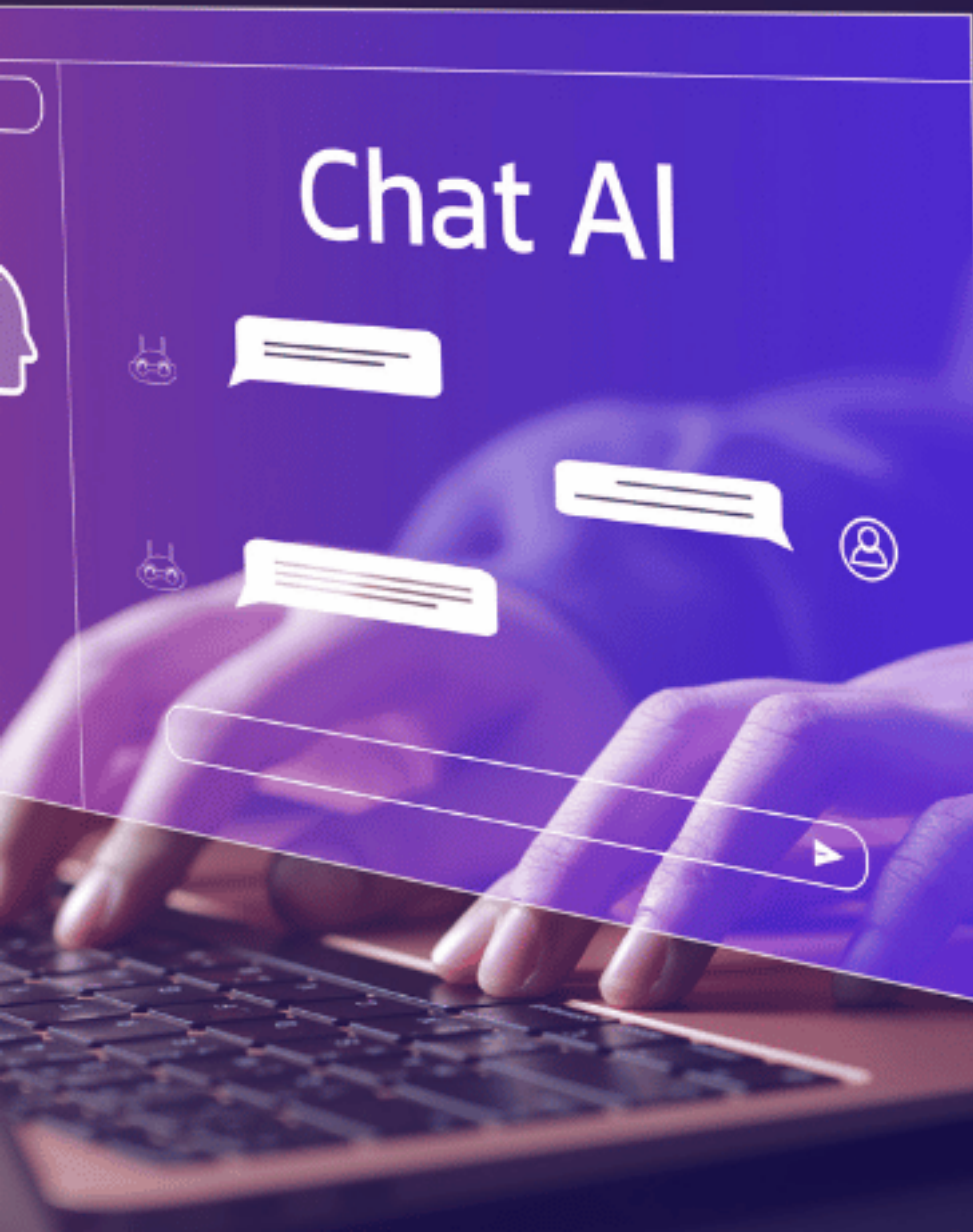
Managing Risk in the Gray Area:

- Create responsible auto-deletion policies (e.g., purges after 6 months to 1 year)
- If implemented, custodians must determine which chats to retain



Factors for determining “transitory” records:

- ✓ informal versus formal communication
- ✓ whether message loses value once purpose is served
- ✓ whether info is of short-term value
- ✓ whether the message provides evidence of a transaction, explains a decision, or is required for legal or financial audits



AI Transparency as Barometer for Retention

Consider encouraging citations to AI use in public entity documents

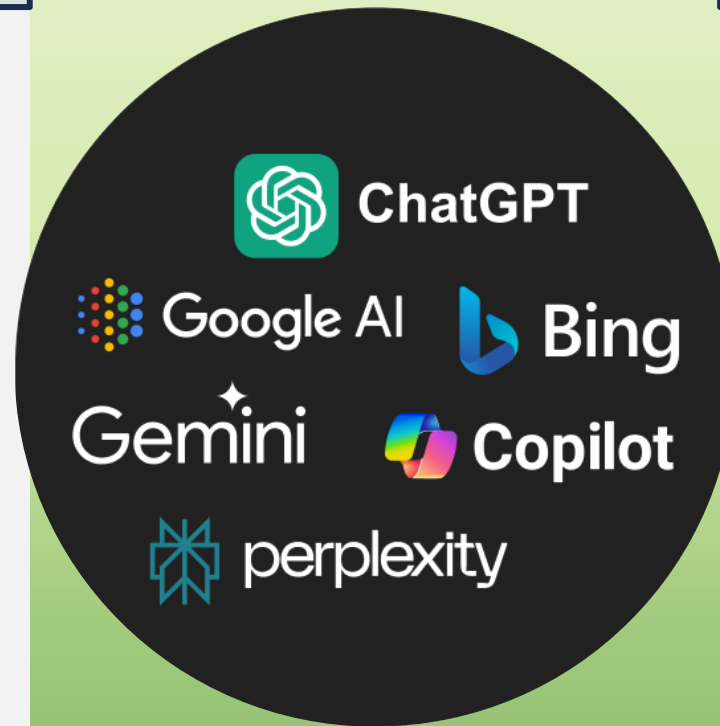
- ✓**Example:** City of Long Beach encourages employees to include citations such as, “This document was drafted with support from (GEN AI SYSTEM) on DD/MM/YYYY. The content was fact-checked by City staff. This information is unmodified.”
- ✓**Transparency Benefits:** Informs the public about how/when entities are utilizing AI and encourages honest use of AI by public employees
- ✓**Retention Benefits:** Can help signal when an AI interaction should be saved and retained; if you cite to AI use, retain the corresponding interaction

Produce or not produce? Exemptions and Privileges for AI and Chat Records

Risk of Waiver: Why Open vs. Closed AI Systems Matter

Open AI Systems

- Train from interactions of all users
- Data not guaranteed private
- Courts have already declined to consider AI use as privileged (See *United States v. Heppner*, 25-cr-00503-JSR (S.D.N.Y.).)



Closed AI Systems

- Operate in secure, private system
- Data security measures ensure privacy
- Entity can exercise greater control over data
- Privacy and security measures mean privilege is on the table

Exemption Analysis for AI Interactions

Privacy-based exemptions:

- Likely don't apply for interactions with open AI tools
- Records from use of closed system can be withheld/redacted

Public Interest Exemption ("catchall") is most likely to apply:

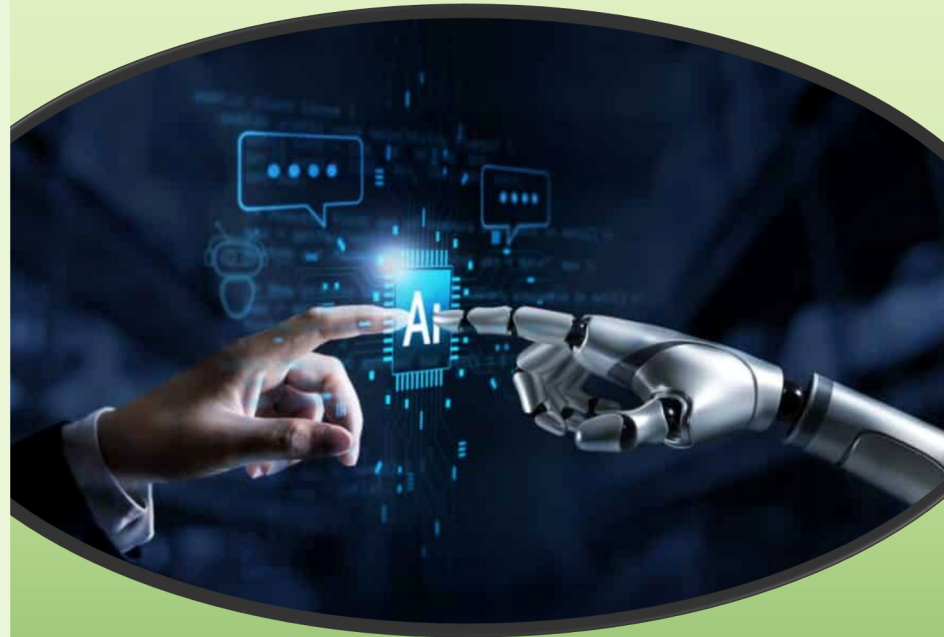
- Interest in non-disclosure must clearly outweigh public interest in disclosure

Exemption Analysis for AI Interactions

Public Interest Exemption (“catchall”) derivatives:

Deliberative Process:

- Requires novel idea that one can ‘deliberate’ with AI
- Ask: does release impair decision-making process?
- Time will tell...



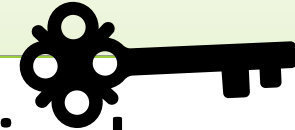
Preliminary Drafts:

- must be a preliminary draft, note, or memorandum; it must not be retained in the ordinary course of business
- Interests in AI transparency may weigh in favor of disclosure

Exemption Analysis for Chat Records

Like emails, many exemptions may apply:

- Public Interest Exemption - Deliberative process (e.g., predecisional discussions of a new policy)
- Public Interest Exemption - Drafts (e.g., exchange of draft language of a press release)
- Medical and personnel records (e.g., human resources emails about private personnel records or information)
- Attorney-client privilege (e.g., city attorney advice)
- General privacy (e.g., constituent contact information and other private data)



Managing mixed message threads

- If a thread contains exempt + non-exempt material, release with redactions if feasible
- If thread contains responsive + nonresponsive material, release full record unless redactions are justified

Managing the Benefits of Technology Against the Drawbacks

Leveraging AI to Process Public Records Requests

18.6%

of federal agencies use
AI/ML for FOIA
processing (NARA 2024)



Document Search

ML models search large repositories
for responsive records



Smart Redaction

AI identifies and redacts private
information automatically



Deliberation Flagging

Tools like FOIA Assistant highlight
deliberative language for review



Public Portals

AI chatbots help requesters find
already-published documents

⚠ Human review is essential — particularly for exemption determinations. AI creates risk of complacency and inconsistency.

Addressing the Growing Prevalence of Personal Device Searches

City of San Jose v. Superior Court (2017): Records on personal devices/accounts relating to public business ARE subject to CPRA disclosure.

01

Train officials: any record relating to public business is subject to disclosure, even on personal devices

02

Recommend public-only accounts for official business to minimize personal device exposure

03

Provide step-by-step search instructions for social media, chat apps, AI tools, and personal email

04

Require signed affidavit confirming personal device search was conducted (approved by CA Supreme Court)

05

Create enforcement mechanism: council-adopted policy with compliance attestation requirement

Policy Pillars for Proactive AI & Chat Governance

*There is a lot to learn when it comes to responsible use of AI and other technologies. Trainings for staff and officials are highly recommended!

1

Approved Uses & Best Practices

Define permitted AI and chat uses (drafting, translating, transitory comms only);
Highlight risks of bias and hallucinations

2

Information Restrictions

Prohibit input of privileged, private, or confidential data into open AI systems

3

Save & Retain Guidance

Step-by-step instructions for saving non-transitory AI and chat records

4

Official Accounts Only

Public business on public accounts; guidance for personal device/account searches

5

AI Attribution

Require citation when AI assists in drafting documents (e.g., Long Beach model)

6

Data Collection Opt-Out

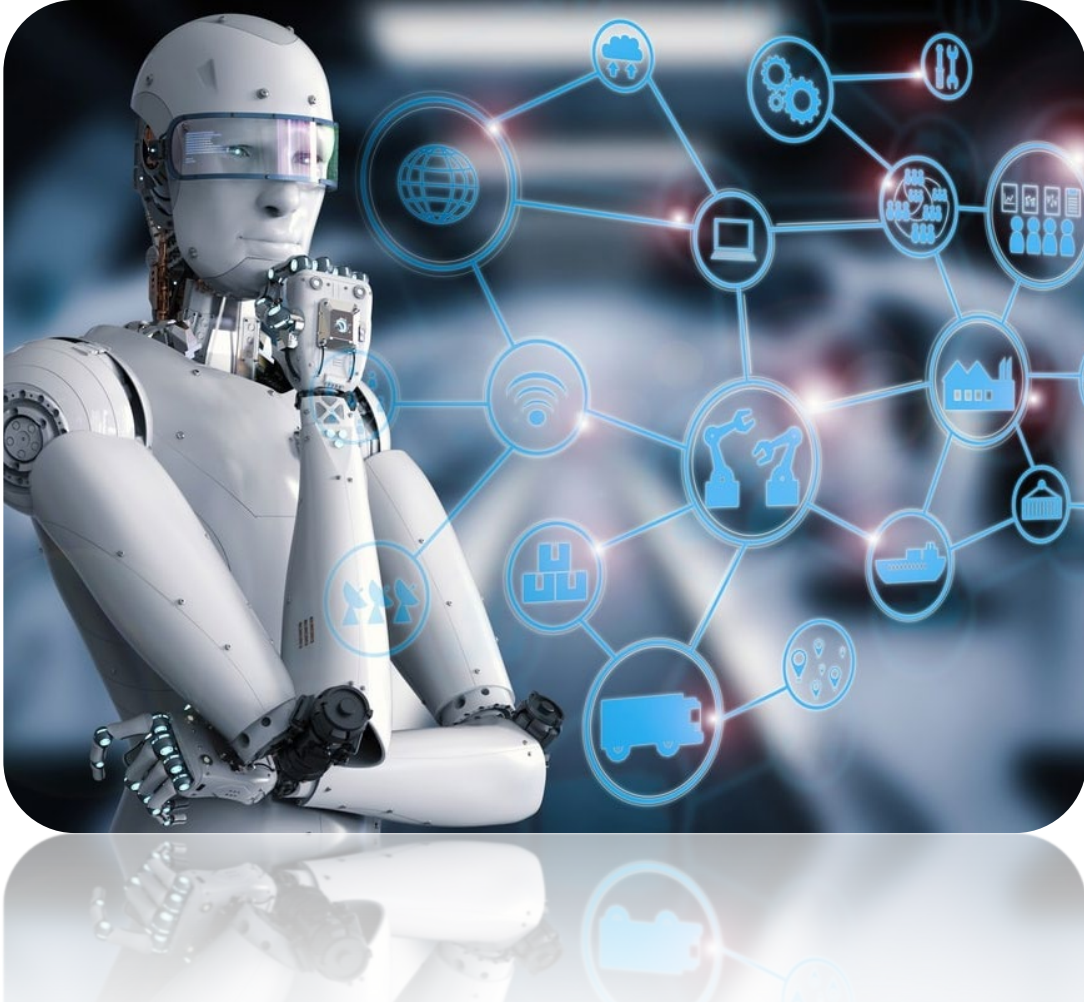
Provide guidance on opting out of data collection in approved apps

Summary & Key Takeaways

Record Type	Public Record?	Retention	Key Exemptions	Top Policy Action
AI Interactions	Presumed public if relates to entity business	2 years if substantive; 6 mo–2 yr before purge	Deliberative process (difficult); Drafts; Balancing test	Comprehensive AI use policy with citation requirements
Chat Messages	Presumed public if relates to entity business; informal personal chats likely not	2 years if substantive; transitory may be purged sooner	Many apply (same as email): privilege, drafts, personnel, privacy	Encourage minimal use; official accounts only; transitory classification
Metadata	Public if primary record is public	Same period as primary record	Same as primary record; additional redaction if security risk	IT protocols for metadata preservation; redaction before production

** Retention periods under 2 years may be subject to legal challenge under Gov. Code § 34090.*

Where Do We Go From Here?



1. Audit current AI & chat tool inventory: what are employees using today?
2. Develop or update written policies
3. Train department heads and public officials on CPRA obligations for AI/chat records
4. Engage IT to establish closed-system AI tools for sensitive government work
5. Assess AI tools to assist with CPRA request processing (search, redaction, flagging)
6. Watch for court decisions - this area of law is evolving rapidly

Thank You!