Law Enforcement Access to Consumer Data

David LeDuc
Vice President, Public Policy

PRESENTED BY:

About the Network Advertising Initiative

Guidance

Practical resources to help ad-tech companies navigate a complex and rapidly evolving legal and compliance landscape.

Education

Building a culture of privacy within the industry — promoting it as a competitive advantage and foundation for long-term consumer trust.

Policy Engagement

Engaging federal and state policymakers to advocate for legislation that protects consumers while also preserving responsible data-driven advertising.

Not a traditional trade association. NAI members submit to independent privacy reviews, commit to enforceable standards, and support strong data protection policy.

The NAI Opposes Nonconsensual Sharing of Consumer Data for Law Enforcement

Our Track Record

- **2020** — Best practices on transparency for data shared beyond advertising purposes
- **2022** — Voluntary Enhanced Standards (VES) restricting precise location data from law enforcement / national security use
- **2024** — VES updated using NAICS codes to identify sensitive locations

The Core Principle

Consumers share data based on commercial terms — the expectation it will be used to provide commercial services and show relevant ads.

They are not agreeing to have their data repurposed as a tool of government surveillance.

Purpose Limitation Violation

Data used beyond its disclosed purpose

Chilling Effect

Discourages lawful online activity

Disparate Impact

Vulnerable communities most at risk

A Strong — but Incomplete — Foundation

Approach 1: Transparency & Control

- CCPA rights to know, delete, correct & limit use of personal information/sensitive personal information
- Delete Act: Data brokers must disclose types of data shared and with whom
- Empowers consumers to identify bad actors and exercise deletion rights

Approach 2: Clear Restrictions on Sharing

- CCPA § 7002: sharing must be reasonably necessary & proportionate to disclosed purpose
- Collecting and processing personal information to power commercial services and the advertising that supports them is reasonable & necessary, and commonly understood
- Voluntary law enforcement data sharing is **not** reasonable & necessary, and absent a completely separate and distinct disclosure and consent, should be considered inconsistent with the CCPA

⚠ **Potential Gaps:**

Delete Act: Companies selling personal information only to the government may not qualify as 'data brokers' under current law/regulations. Clarifying guidance or a targeted amendment would close this loophole.

CCPA: Regulatory clarity about the application of data minimization requirements, § 7002 to data sharing with law enforcement agencies.

What New Laws Should Look Like

Category 1 — Federal

Fourth Amendment Is Not for Sale Act: Bars agencies from purchasing data they could not obtain without a warrant. NAI strongly supports — urges CA to champion it.

Category 2 — State

Prohibition on commercial sharing: Government-side restrictions bind only U.S. agencies — they do not constrain foreign adversaries or non-U.S. actors who may purchase consumer data commercially. Restrictions on voluntary, non-consensual industry sharing for law enforcement purposes provides additional, more universal protection.

NAI Recommendation: Federal and state legislation can work in compliment, restricting government purchase AND restricting voluntary, nonconsensual sharing of consumer data for law enforcement purposes.

Targeted Solutions, Not Blanket Prohibitions

The Risk of Overly Broad Restrictions

- MD, OR & VA enacted sweeping data sales bans, curtailing legitimate commercial uses
- Strict limits on precise location / sensitive data would shut down many beneficial services provided by third-party partners
- Only the largest vertically integrated platforms are unaffected
- Result: market imbalance concentrating digital power in the few largest companies

✅ **We Support**

Targeted restrictions on law enforcement sharing and government acquisition of consumer data

❌ **We Oppose**

Blanket bans on selling/sharing precise location or sensitive data that eliminate legitimate, privacy-protective commercial uses

Not all government access is equal. Smart city services, public health research & emergency response are categorically different from warrantless law enforcement surveillance. Policies must be scoped accordingly.

SECTION VI — CONCLUSION

The NAI's Message to CalPrivacy

01 Consumer data collected to power digital media and advertising should not become the raw material for government surveillance. Consumers did not consent to that use.

02 Agency guidance, targeted CCPA/Delete Act amendments, and carefully scoped legislation can solve this problem — without sacrificing advertising-supported services.

03 The solution must be surgical: restrict law enforcement sharing and government acquisition, without broadly banning legitimate data-driven commercial uses.

04 The NAI stands ready to collaborate — sharing model language, technical expertise on data flows, and experience developing self-regulatory standards.