Urban Consortium Perspective on the Nevada Public Records Act (NPRA)

Las Vegas – Reno – Henderson – North Las Vegas - Sparks

- Local governments fully support transparency and the Nevada Public Records Act (NPRA)
- In our experience, a majority of public records requests are fulfilled quickly and at little to no cost
- Local governments have a **legal obligation** to both provide public records and to safeguard sensitive personal information and other types of records that the law says we must protect
- Local governments believe Nevada has an effective public records law that functions as intended, but that it would benefit from additional clarity
- Any proposed changes must be strategic, not wholesale, and developed thoughtfully with robust stakeholder input

Transparency and Privacy are not Mutually Exclusive Goals

Local governments are custodians of public records that contain sensitive personal data and other information that must or should be protected

- We are generally satisfied with the current public records framework
- What we are seeking is clearer statutory guidance to help in balancing the requirement to provide public records with the legal requirements to protect privacy and the need to ensure safety, fairness, and administrative practicality
- Better clarity would help agencies respond faster, treat requesters more consistently, and protect sensitive and/or restricted information that appears in public records

Privacy duties are real

Records requests routinely implicate victims, minors, home addresses, health details, personnel information, and sensitive audio/video.

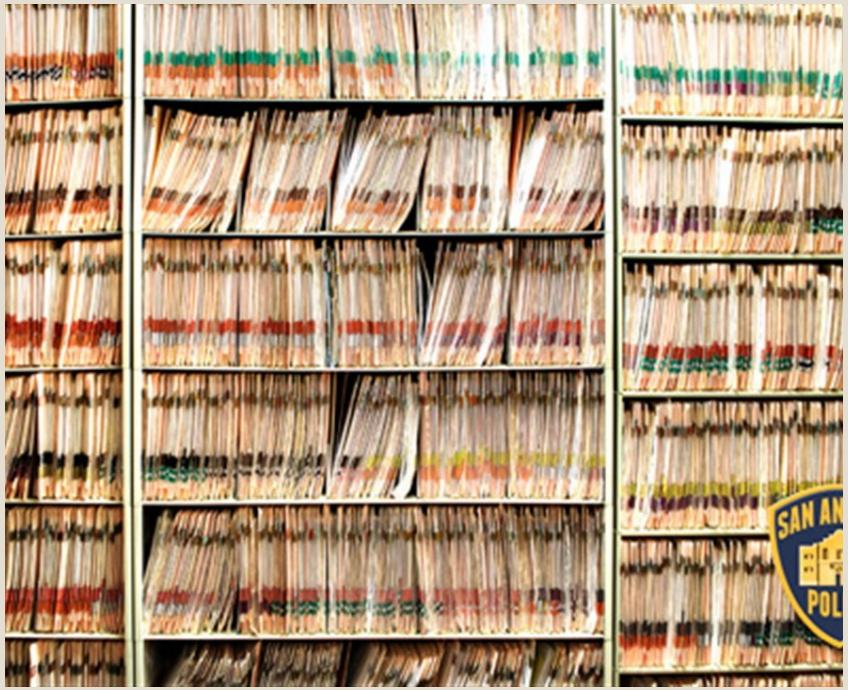
Clarity helps everyone

Requesters benefit from clearer response rules; agencies benefit from clearer authority; Individuals benefit from stronger, more predictable protection of legitimate privacy interests

Overly Broad or Harassing Requests can Dilute and Distort a Law Designed for Accountability

The problem is not ordinary public scrutiny. The problem is when request volume, scope, or motive turns the process into conflict.

- The volume of some requests consumes disproportionate staff time and should be more specific.
- The challenge is especially acute when former employees, former partners, or other aggrieved individuals use the process to target specific staff, offices, or individuals.
- The goal is to preserve broad access while still providing agencies with a reviewable means to address demonstrably problematic conduct.



What clearer law could do

Allow structured responses to unnecessarily broad or harassment-driven requests, subject to documentation and appeal.

What it should not do

Deny difficult, unpopular, or time-consuming requests simply because they are seen as burdensome or potentially embarrassing.

Ambiguity in the Law Creates Inconsistent Decisions and Avoidable Conflict

Expansive Definition of "public record" in NRS

Basis for withholding or redaction

Agencies need clearer statutory authority on privacy, safety, personnel, investigative, and victim-related exemptions.

Cost recovery

Production of bodycam, dashcam, and surveillance video can require hours of review and specialized labor.

Legitimate Disputes Should Have a Path to Resolution Short of Litigation

When agencies and requesters genuinely disagree, the only option should not be an all-or-nothing trip to court.

Commercial Requesters Raise a Distinct Policy Question

The law often treats a resident seeking oversight and a company seeking a monetizable dataset the same way — even when the downstream use is very different.

The core distinction

Open-records laws are meant to promote public oversight. They were not necessarily written for high-volume extraction of personal or quasi-personal data that can be packaged, resold, or used for lead generation and profiling.

Question for lawmakers

Should the law draw a clearer line between noncommercial civic use and commercial exploitation — especially where personal identifiers or bulk datasets are involved?

$282M

InvestigateTV said DMVs nationally pulled in at least this much in 2024 from personal-information sales.

Potential legislative options

- permit different fee rules for commercial bulk requests
- limit redisclosure of sensitive fields
- require stronger stated purpose for large dataset requests
- preserve full access for watchdog, journalistic, and individual use

AI Changes the Scale of the Risk

AI

A request that once produced a stack of documents can now feed tools that scrape, summarize, cross-reference, re-identify, and redistribute information at industrial speed

- Bulk public data can be used to build searchable profiles, infer identities, or generate misleading narratives about individuals.
- AI lowers the cost of harvesting records for monetization, targeted harassment, doxing, and deceptive “news” or content products.
- The legal framework has not caught up to the speed, scale, and synthetic-output risks created by modern tools.
- Potentially a significant cybersecurity risk

Wired, Feb. 2026

WIRED reported that state privacy laws give public servants few ways to stop data brokers from selling personal data sourced from public records, describing a “data-to-violence pipeline.”

Targeted clarifications can strengthen both access and trust

The ask is not less transparency. The ask is a better-operating law.

Bottom line

Clearer rules help local governments release what should be public, protect what should stay private, and resolve disputes more fairly.

- Define “public record” more clearly
- Clarify withholding/redaction authority where privacy, safety, and victim or employee protections are genuinely implicated.
- Create a fast, affordable dispute-resolution path short of litigation.
- Authorize a narrow, documented response to problematic requests, with appeal rights.
- Address commercial bulk extraction and AI-enabled exploitation without impairing ordinary civic oversight.