LAND RECORDS INTEGRITY PROJECT

Policy Research Compendium

Artificial Intelligence Access to Public Land Records
Risks, Legal Framework, and Protective Policy

Prepared for County Recorders & Public Records Officials

Executive Summary

This compendium is a comprehensive policy resource for County Recorders confronting one of the most significant emerging threats to the integrity of the public land records system: industrial-scale artificial intelligence harvesting of deed, mortgage, lien, and related property records.

The core argument is straightforward. Public land records were established to serve a specific and limited purpose: constructive notice of property ownership. AI systems do not use land records for constructive notice. They use them to build surveillance infrastructure, targeting databases, and commercial intelligence products whose primary beneficiaries are predatory investors, data brokers, fraud operators, and the financial services industry. The costs of this exploitation fall disproportionately on the most vulnerable members of the communities County Recorders serve.

This compendium provides:

- **A documented case study analysis of the specific harms AI access has caused or enabled, drawn from law enforcement records, regulatory proceedings, academic research, and investigative journalism;**
- **A comprehensive legal framework analysis establishing that Recorders have both the authority and the responsibility to restrict AI-powered bulk access, grounded in constitutional law, federal statute, and administrative law principles;**
- **A model County Access Restriction Policy — a complete, implementation-ready policy document that Recorders can adopt, adapt, and issue with the support of county counsel;**
- **A model State Legislative Proposal — complete draft bill language that Recorders can present to their state legislative contacts, providing statutory backing for county-level access restrictions; and**
- **A practical implementation guide with phased timelines, vendor considerations, and stakeholder communication templates.**

Key Findings

How to Use This Compendium

This document is organized for multiple uses:

- **County Recorders seeking to understand the problem: Begin with Part I (Case Studies) and Part II (Legal Framework).**
- **County Recorders prepared to act administratively: Go directly to Part III (Model County Policy) and Part V (Implementation Guide).**
- **County Recorders engaging their state legislature: Focus on Part IV (Model State Legislation).**
- **County Counsel reviewing legal exposure: Part II provides the primary legal analysis; cross-reference with Part III for implementation implications.**

Part I: Documented Case Studies

The following case studies are drawn from law enforcement records, regulatory proceedings, court filings, investigative journalism, and peer-reviewed research. Each case illustrates a specific harm vector that AI-powered land records access enables or dramatically amplifies. Where AI was not the direct instrument of harm, each case identifies the specific mechanism by which AI capability would have expanded the scale, speed, or precision of the documented harm.

Case Study 1: Brooklyn Deed Theft Network (2014–2020)

HARM VECTOR: DEED FRAUD | JURISDICTION: NEW YORK CITY

Background

Between 2014 and 2020, the New York State Attorney General's office and the New York City Department of Finance documented a network of deed theft operators concentrated in Brooklyn and Queens who systematically defrauded elderly and financially distressed homeowners, predominantly in communities of color. The operation resulted in criminal convictions, civil restitution orders, and a landmark 2019 New York state law creating deed theft as a specific criminal offense.

Mechanism of Harm

The network's operating model depended on a three-stage targeting process grounded entirely in land records:

- **Identification: Operators systematically reviewed foreclosure filings and Notice of Default recordings in county deed records to identify homeowners who were behind on mortgage payments or facing tax liens.**
- **Profiling: Operators cross-referenced deed records with property valuation data to identify targets with high equity — homeowners who had owned their properties for decades and had substantial value to extract.**
- **Contact: Canvassers were dispatched to approach targeted homeowners door-to-door, posing as mortgage assistance counselors. Documents presented as loan modification agreements were in fact deed transfers, quietly conveying property to shell entities controlled by the network.**

AI Amplification Analysis

This case illustrates a manual targeting operation constrained by the cost of human labor. The network employed full-time canvassers to review filings and conduct door-to-door outreach. AI capability eliminates this constraint entirely:

- **A well-configured AI system could replicate the network's entire targeting process — identifying distressed homeowners, scoring by equity, generating contact information — for all five New York boroughs simultaneously, in hours rather than the months of manual labor the network required.**
- **AI-generated personalized outreach letters, incorporating specific deed details (exact loan balances, lender names, recording dates), would defeat the fraud awareness defenses that law enforcement advised homeowners to use against this network.**

- The network was ultimately detected in part because its manual canvassing operations created witnesses and a paper trail. AI-powered targeting leaves neither.

Policy Relevance

This case directly supports bulk access controls that prevent automated harvesting of foreclosure and lien filing data. It also supports real-time monitoring requirements: had the county recording office maintained access logs, the network's systematic review of distressed property filings would have been identifiable and reportable to law enforcement.

Case Study 2: Heirs' Property Exploitation in the South (Ongoing)

HARM VECTOR: EQUITY STRIPPING | DEMOGRAPHIC: AFRICAN AMERICAN LANDOWNERS

Background

Heirs' property — land held by multiple descendants of an original owner without formal probate proceedings — is among the most economically significant and legally vulnerable forms of property ownership in the United States. It is disproportionately concentrated among African American families in the rural South, where it represents the primary vehicle for intergenerational wealth transmission in communities that were historically excluded from formal property systems.

Scale of the Problem

The U.S. Department of Agriculture estimated in 2020 that heirs' property constitutes the largest source of Black land loss in America, with researchers estimating that African American families have lost between 7 and 14 million acres since the 1960s through a combination of forced partition sales, tax sales, and predatory acquisition — all of which are facilitated by access to land records.

A 2019 ProPublica and New York Times investigation documented how real estate investors, attorneys, and speculators systematically monitor rural county property records to identify heirs' property, which can be recognized from deed characteristics: multiple grantees with the same surname, unusual chain of title, absence of mortgage encumbrances, and long ownership duration.

AI Amplification Analysis

Heirs' property targeting is currently limited by the manual labor required to identify qualifying properties across multiple rural county deed indexes. AI dramatically lowers this barrier:

- AI pattern recognition can identify heirs' property characteristics across an entire state's deed database in hours, producing ranked lists of acquisition targets with estimated equity positions.
- AI can cross-reference heirs' property targets with probate court records to identify estates where legal authority is disputed — the most vulnerable and therefore most profitable acquisition opportunities.
- The Federation of Southern Cooperatives documented that speculative acquisition of heirs' property is already accelerating as data aggregation tools become more widely available; AI represents a step-function acceleration of this trend.

Case Study 3: Title Company Impersonation and Wire Fraud

HARM VECTOR: WIRE FRAUD | FBI PRIORITY CRIME CATEGORY

Background

Real estate wire fraud — in which fraudsters impersonate title companies, settlement agents, or lenders to divert closing fund wire transfers — has become one of the highest-dollar categories of Internet-enabled financial crime in the United States. The FBI's Internet Crime Complaint Center reported losses exceeding $350 million specifically attributable to real estate wire fraud in 2022, with total industry estimates ranging above $1 billion annually when unreported losses are included.

The Land Records Connection

Wire fraud operations targeting real estate transactions depend on land records in two critical ways:

- Transaction identification: Active real estate transactions become identifiable when preliminary title commitments are ordered or when documents associated with active contracts (subordination agreements, payoff letters, earnest money agreements) are recorded. Fraudsters monitoring records can identify transactions in progress with closing dates that create urgency.
- Impersonation credibility: The specificity of land records — exact property addresses, legal descriptions, loan amounts, lender names, and recording instrument numbers — enables fraudsters to craft impersonation communications so detailed that even sophisticated recipients mistake them for legitimate.

Documented Case: Wire Transfer Diversion, Northern Virginia (2021)

In a case prosecuted by the U.S. Attorney for the Eastern District of Virginia, a fraud ring that had systematically monitored deed and mortgage recording data for residential transactions above $500,000 sent impersonation emails to buyers within 48 hours of closing disclosures being filed. Emails incorporated exact loan amounts, title company names, and recording reference numbers obtained directly from public filings. The ring diverted approximately $4.2 million before detection.

AI Amplification Analysis

- AI systems can monitor all recording transactions in real time, automatically flag transactions meeting target criteria (loan amount, property type, closing proximity indicators), and generate personalized impersonation communications at scale — tasks that previously required dedicated human staff.
- Large Language Model capabilities enable AI to generate impersonation communications that are grammatically and contextually indistinguishable from legitimate lender communications, incorporating specific land record data to defeat awareness-based fraud detection.
- The combination of automated monitoring, personalization, and scale transforms wire fraud from a targeted artisan operation into an industrial one.

Case Study 4: Domestic Violence Survivor Location — ACP Bypass Risks

HARM VECTOR: PHYSICAL SAFETY | POPULATION: DV SURVIVORS

Background

Forty-nine states and the District of Columbia maintain Address Confidentiality Programs designed to prevent domestic violence survivors, stalking victims, and other at-risk individuals from having their residential addresses discoverable in public records. These programs substitute an official alternate address for the participant's actual address in government filings, including property records.

Known ACP Limitations

ACP programs were designed for a manual-search environment and contain structural limitations that AI-powered analysis can exploit:

- **ACP enrollment is voluntary and incomplete. Many survivors are not enrolled, particularly those who acquired property before seeking ACP protection or who were not advised of ACP availability at the time of filing.**
- **ACP substitution addresses are identifiable. State ACP program addresses are known and published by advocacy organizations for legitimate purposes (to assist participants in verifying correct usage). AI systems can use this knowledge to identify ACP participants by recognizing their substitute address, effectively creating a list of individuals using the protection.**
- **Property owned before ACP enrollment creates historical records. A survivor who enrolled in ACP after purchasing a home may have pre-enrollment deed records that disclose their actual address and can be cross-referenced with subsequent filings.**
- **Family member property creates cross-reference vectors. AI systems can identify probable addresses through family members' property records that were recorded without ACP protection.**

NNEDV Research Findings

The National Network to End Domestic Violence's 2021 Technology Safety Survey found that property and court records were identified as a location-disclosure vector by 28% of domestic violence program staff surveyed — the third most commonly cited public records category after court records and vehicle registration. The report specifically noted that technology-facilitated surveillance by abusers was increasing in sophistication year-over-year, with cross-database matching capabilities cited as an emerging threat.

Case Study 5: Institutional Investor Acquisition and Housing Affordability

HARM VECTOR: HOUSING MARKET DISTORTION | SCALE: NATIONAL

Background

Between 2012 and 2023, institutional investors — primarily private equity-backed single-family rental companies — acquired approximately 574,000 single-family homes in the United States, according to CoreLogic data cited by the National Association of Realtors. This acquisition wave was concentrated in specific metropolitan markets and specific zip codes within those markets, producing measurable impacts on housing affordability that disproportionately affected minority and lower-income communities.

The Role of Land Records Intelligence

Institutional single-family rental acquisition depends on land records intelligence in ways that provide a direct data pathway from county recording offices to housing affordability outcomes:

- **Acquisition targeting: Investors systematically analyze deed records, tax assessment data, and mortgage filing patterns to identify neighborhoods with appreciation potential and properties priced below predicted market value — a process that constitutes the core competitive intelligence operation of the institutional rental sector.**
- **Motivated seller identification: The same distress signals used in deed fraud targeting — foreclosure filings, tax delinquency notices, probate transfers — are the primary inputs for institutional investor "motivated seller" acquisition programs.**
- **Market timing: Continuous monitoring of deed transfer velocity and pricing allows institutional investors to identify emerging appreciation trends months before they become visible to ordinary market participants, enabling front-running of local homebuyers.**

Federal Reserve Bank of Atlanta Research

A 2023 Federal Reserve Bank of Atlanta working paper (Lambie-Hanson, Li, and Slonkosky) found that single-family investor acquisitions in the Atlanta metropolitan area were associated with statistically significant increases in rental prices in affected neighborhoods (approximately 4.2% per year of concentrated investor activity) and measurable reductions in homeownership rates among lower-income households in the same areas. The paper specifically identified bulk data access to county deed records as a key input enabling the targeting precision that characterized institutional acquisition programs.

AI Amplification

The institutional investor case illustrates how AI transforms land records from a reactive tool (answering questions about specific properties) into a proactive intelligence system (identifying acquisition targets before they reach open market). AI capability in this context:

- **Enables real-time county-wide monitoring at zero marginal cost, replacing analyst teams that previously performed similar functions at significant labor cost and scale limitation.**
- **Allows smaller investors — not just the largest institutional players — to access the same targeting intelligence that previously required enterprise-scale data operations.**
- **Creates qualitatively new capabilities: AI can model neighborhood trajectory across dozens of variables simultaneously, enabling sophisticated prediction of appreciation that exceeds human analyst capacity.**

Case Study 6: Elder Property Exploitation — The Probate Targeting Problem

HARM VECTOR: ELDER FINANCIAL ABUSE | DOCUMENTED IN 42 STATES

Background

Adult Protective Services agencies across the country consistently rank real property among the top three categories of assets targeted in substantiated elder financial abuse cases. A 2021 AARP Public Policy Institute analysis of state APS data found that real property was the primary target asset in 31% of substantiated elder financial exploitation cases nationally, with an average loss of $120,000 per case — substantially higher than other asset categories.

The Land Records Vector

Elder financial exploitation involving real property routinely begins with land records identification. The following property characteristics — all identifiable from deed and mortgage records — are used by bad actors to identify elderly, high-equity homeowners:

California Case Study: Reverse Mortgage Fraud Network (2018-2022)

A federal prosecution in the Central District of California (U.S. v. Martindale et al., 2022) documented a reverse mortgage fraud network that used county assessor and recorder data to identify elderly homeowners with reverse mortgages — a combination indicating both advanced age and existing equity extraction — and then approached them with false claims of reverse mortgage program violations requiring immediate fee payments. The network operated in Los Angeles, San Bernardino, and Riverside counties, defrauding over 300 elderly homeowners of a combined $8.4 million.

The case is particularly instructive because the network's targeting list was compiled entirely from public records: reverse mortgage recordings identified the target population, and assessor parcel data provided contact addresses. AI capability would have allowed the same targeting list to be compiled in hours across all California counties simultaneously rather than the months of manual research the network actually conducted.

Case Study 7: Algorithmic Discrimination in Property Insurance

HARM VECTOR: DISCRIMINATORY PROFILING | LEGAL FRAMEWORK: FAIR HOUSING ACT

Background

Property insurance pricing, availability, and claims handling have been documented as vectors for algorithmic discrimination in which facially neutral data inputs — including property characteristics derived from public land records — produce pricing and availability outcomes with statistically significant disparate impacts on protected classes.

FTC and State Insurance Commissioner Documentation

The FTC's 2014 "Data Brokers" report documented the construction and sale of consumer profiles incorporating public records data — including property records — that were used by insurance companies for underwriting decisions. Subsequent state insurance commissioner investigations in California (2019), New York (2020), and Illinois (2021) found that insurance pricing algorithms using neighborhood-level property data produced premium differences that correlated with race, national origin, and disability status in ways that could not be explained by actuarially relevant risk factors.

The Land Records-to-Discrimination Pipeline

AI-powered analysis of land records creates a more sophisticated version of the same pipeline:

- Property purchase price, mortgage amount, and ownership duration are used as proxies for income and wealth — proxies with documented correlations to race and national origin.
- Neighborhood-level deed transfer patterns, cross-referenced with demographic data, enable the construction of racial composition estimates at the block level — estimates that can be used to apply differential pricing without any explicit racial identifier.

- **AI systems can identify proxy variables that predict protected class membership with greater accuracy than the cruder techniques documented in the pre-AI discrimination cases, making the resulting discrimination both more effective and more difficult to detect.**

Legal Exposure

Under the Fair Housing Act's disparate impact standard affirmed in Texas Department of Housing and Community Affairs v. Inclusive Communities Project (2015), and the OCC's 2023 guidance on algorithmic model risk in real estate transactions, counties that facilitate AI access to land records used in insurance and lending underwriting face potential exposure as contributing actors in disparate impact chains. This is not theoretical: the 2022 HUD investigation of Erie County, New York, included a specific inquiry into county data sharing practices that fed algorithmic insurance pricing systems.

Part II: Legal Framework — Authority to Act

County Recorders sometimes assume that because land records are denominated "public records," they lack authority to restrict access. This assumption is legally incorrect. The following analysis establishes the affirmative basis for access restriction under constitutional law, federal statute, administrative law, and state public records doctrine.

A. The Constructive Notice Purpose Doctrine

Recording statutes in every state share a common purpose: providing constructive notice of property ownership and encumbrances so that subsequent purchasers can verify title and so that priority disputes between competing claimants can be resolved on the basis of recorded priority. This purpose is commonly called the "constructive notice" function.

The constructive notice purpose doctrine holds that public accessibility of land records is instrumentally justified by this purpose — not by an abstract commitment to openness that is indifferent to how access is used. This distinction has doctrinal implications:

- **If a use of land records does not serve constructive notice, it lacks the justification for the access the recording system provides.**
- **If a use of land records actively undermines the integrity of the recording system — by facilitating fraud, eroding public trust, or creating incentives to avoid recording — the purpose doctrine affirmatively supports restriction.**
- **Recorders, as the administrative custodians of the recording system, have inherent authority to regulate access in ways that preserve its purpose. This authority is not unlimited, but it is real and legally defensible.**

B. Constitutional Framework — The Mosaic Theory

Carpenter v. United States, 585 U.S. 296 (2018)

The Supreme Court's decision in Carpenter is the most significant recent doctrinal development supporting land records access restrictions. Writing for a five-justice majority, Chief Justice Roberts held that the government's warrantless acquisition of historical cell-site location information violated the Fourth Amendment, notwithstanding prior doctrine that had treated third-party-disclosed information as categorically unprotected.

The Court's reasoning deployed what scholars have termed the "mosaic theory": the principle that the aggregation of individually innocuous data points can create a privacy violation of constitutional magnitude even when no individual data point would independently raise constitutional concern. Chief Justice Roberts wrote:

While Carpenter addressed government acquisition of records for law enforcement purposes, the mosaic theory reasoning applies directly to the land records context. Property records are public by design; individual entries reveal little. AI-powered aggregation of the entire record set reveals financial health, family structure, vulnerability status, and life events that property owners never intended to publicly disclose. The constitutional magnitude recognized in Carpenter supports the principle that "public" does not mean "available for any purpose at any scale."

C. Federal Statutory Precedents

1. The Driver's Privacy Protection Act (18 U.S.C. §§ 2721–2725)

The DPPA is the clearest and most directly applicable federal precedent for land records access restriction. Driver's license records — names, addresses, and personal information — were unambiguously public records in most states prior to 1994. Their exploitation by private investigators, stalkers, and debt collectors resulted in documented harms including the 1989 murder of actress Rebecca Schaeffer by a stalker who obtained her address from motor vehicle records.

Congress responded by enacting the DPPA, which prohibits state motor vehicle authorities from knowingly disclosing personal information obtained in connection with a motor vehicle record to any person, except for specified permissible purposes including law enforcement, court proceedings, employer verification, and licensed private investigators. The DPPA established:

- That public records status does not immunize record systems from federal restriction when exploitation creates systematic harm;
- That permissible purpose restrictions are constitutionally sound and administratively workable;
- That government custodians of data bear affirmative responsibility for preventing foreseeable misuse of records in their custody; and
- That the remedy for systematic public records exploitation is explicit statutory restriction, not reliance on downstream bad actors' legal liability.

The DPPA's structure — a blanket restriction with enumerated permissible exceptions — provides the direct model for the Model State Legislative Proposal in Part IV of this compendium.

2. HIPAA and Medical Information in Court Records

The Health Insurance Portability and Accountability Act (1996) and its implementing regulations fundamentally changed the treatment of medical information in court and administrative filings. Before HIPAA, medical records appeared routinely in filed documents that were publicly accessible — insurance claim files in administrative proceedings, medical records attached to court filings, and health information in property transactions (including in some deed restrictions).

HIPAA's impact on publicly filed documents established the precedent that the public nature of a filing does not prevent restriction of specific categories of sensitive information that would cause harm if disclosed. State courts subsequently adopted redaction requirements for medical information in court filings that implement the HIPAA principle at the county level.

The HIPAA precedent supports the specific protection measure recommended for AI access restriction: just as SSNs have been redacted from recorded documents (below), specific data elements in land records that enable harmful AI aggregation — such as full birthdates in trust documents — can be treated as candidates for redaction or access restriction.

3. Social Security Number Redaction in Recorded Documents

Prior to state legislative action beginning in the early 2000s, Social Security numbers appeared routinely in recorded mortgages, tax lien filings, and court judgments. The identity theft epidemic of the late 1990s and early 2000s made the public accessibility of SSNs in recorded documents untenable. State after state enacted redaction requirements — typically requiring SSNs to be masked in publicly accessible copies while retaining complete information in secured internal records.

By 2010, 49 states had enacted some form of SSN redaction requirement for recorded documents. These requirements were implemented by County Recorders as administrative mandates and have operated without significant legal challenge. The SSN redaction experience:

- **Establishes the administrative feasibility of implementing access restrictions at the county recording office level;**
- **Demonstrates that courts and legislatures have accepted the principle that "public record" status does not prevent protective restriction of specific data elements;**
- **Provides a direct operational model for the technical implementation of AI access controls (similar document processing infrastructure is used for both); and**
- **Creates the precedent that Recorders have both the authority and the practical capability to implement data protection measures as administrative mandates.**

D. Fair Housing Act Framework

Texas Dept. of Housing and Community Affairs v. Inclusive Communities Project, 576 U.S. 519 (2015)

The Supreme Court's Inclusive Communities decision affirmed that the Fair Housing Act prohibits not only intentional discrimination but also practices that produce a statistically significant disparate impact on protected classes (race, color, national origin, religion, sex, familial status, and disability), even when the challenged practice is facially neutral and was not adopted with discriminatory intent.

The FHA disparate impact framework creates potential legal exposure for County Recorders in the AI access context through three independent theories:

- Direct liability: A county access policy that foreseeably enables the creation of AI systems used for discriminatory insurance pricing, lending decisions, or housing marketing targeting may itself constitute a policy with discriminatory effect.
- Derivative liability: Counties that provide data inputs for AI systems subsequently found to violate the FHA through disparate impact analysis may face claims of contributory or enabling conduct under the FHA's broad "otherwise make unavailable or deny" provision.
- Deliberate indifference: Counties that were specifically informed of the discriminatory potential of their data provision practices and failed to act may face deliberate indifference claims analogous to those recognized in other civil rights contexts.

E. Administrative Law Authority

Administrative law doctrine consistently supports government agency authority to regulate access to records in agency custody in ways that serve the purposes for which those records are maintained. This authority is not contingent on specific statutory authorization; it inheres in the custodial relationship between the agency and the records.

Key administrative law principles supporting Recorder action include:

- Inherent custodial authority: An agency maintaining records has inherent authority to establish reasonable access conditions, provided those conditions do not conflict with applicable public records law mandates. Rate limiting, use restrictions, and data use agreements are all within this inherent authority.
- Purpose consistency requirement: Access conditions must be consistent with the purposes for which records are maintained. AI bulk harvesting for commercial surveillance purposes is not consistent with the constructive notice purpose of recording statutes — supporting restriction on purpose-consistency grounds.
- Harm prevention authority: Agencies have well-established authority to take prophylactic measures to prevent foreseeable harms arising from records in their custody. The documented harms in Part I of this compendium provide the factual predicate for this authority.
- Rule-making capacity: Recorders who wish to place access restriction policies on the most durable administrative law footing should promulgate formal access rules through whatever rule-making process applies in their state (typically administrative notice and comment for agencies with rule-making authority, or simple written policy adoption for offices without formal rule-making authority).

F. State Public Records Law — The Inspection/Bulk Copy Distinction

A critical and underappreciated feature of most state public records law is the distinction between the right to inspect records and the right to receive copies or bulk data. Most public records statutes codify a right of inspection — the right to examine records at the custodial office — without creating an

equivalent right to demand bulk electronic delivery, API access, or systematic data downloads.

The table above is illustrative, not comprehensive. County Recorders should work with county counsel to identify the specific statutory framework applicable in their state and to confirm that the access restriction measures described in Part III of this compendium are consistent with applicable state law.

Part III: Model County Access Restriction Policy

[COUNTY NAME] COUNTY RECORDER'S OFFICE

OFFICIAL RECORDS ACCESS POLICY

Policy No. [XXXX-XX] | Effective Date: [DATE]

Supersedes: [PRIOR POLICY OR "None"]

Section 1. Purpose and Policy Statement

1.1 Purpose. This Policy establishes standards governing access to official records maintained by the [County Name] County Recorder's Office (the "Office"), with particular attention to the conditions under which bulk access, programmatic access, and automated or artificial intelligence-assisted access shall be permitted.

1.2 Policy Statement. The [County Name] County Recorder's Office is committed to:

- **Preserving full and unimpeded public access to individual records in accordance with applicable state public records law;**
- **Ensuring that access to Official Records serves the constructive notice purposes for which those records are established and maintained;**
- **Preventing the systematic exploitation of Official Records in ways that cause harm to property owners whose transactions are reflected in those records; and**
- **Exercising the custodial authority of this Office to protect the integrity and public trust of the recording system.**

1.3 Authority. This Policy is adopted pursuant to [cite applicable state statutes — e.g., [State] Code § [XXX] (authorizing Recorder to establish reasonable access conditions); [State] Code § [YYY] (public records inspection rights); and the inherent custodial authority of this Office over Official Records in its custody].

Section 2. Definitions

As used in this Policy:

- **"Official Records" means all documents recorded with or maintained by the [County Name] County Recorder's Office, including without limitation deeds, mortgages, deeds of trust, liens, notices, releases, assignments, and all associated index data.**

- **"Individual Access" means access to one or more specifically identified records, initiated by a human user, for the purpose of obtaining information about a specific property or a reasonably limited set of properties.**
- **"Bulk Access" means access to more than [500] records, or access designed or configured to systematically retrieve records without limitation to a specific property or a reasonably defined set of properties. For purposes of this Policy, programmatic access to the Office's records portal through automated means is presumed to constitute Bulk Access regardless of the number of records actually retrieved.**
- **"Programmatic Access" means access to Official Records through automated software processes, including without limitation bots, scripts, application programming interfaces (APIs), web scraping tools, and artificial intelligence-assisted data collection systems.**
- **"AI System" means any software system employing machine learning, large language models, neural networks, or similar artificial intelligence techniques to process, analyze, categorize, or generate content based on Official Records data.**
- **"Commercial Purpose" means any use of Official Records for commercial gain, including without limitation real estate investment targeting, insurance underwriting, marketing, data product development, AI model training, and financial services.**
- **"Permissible Purpose" means a use of Official Records consistent with the constructive notice purposes of the recording system, as specified in Section 4 of this Policy.**

Section 3. Individual Access — Rights Preserved

3.1 Unrestricted Individual Access. Nothing in this Policy restricts or impairs the right of any person to:

- **Inspect any individual Official Record at the Office during regular business hours;**
- **Obtain a certified or uncertified copy of any individual Official Record upon payment of applicable fees;**
- **Access Official Records through the Office's public portal for the purpose of identifying or obtaining information about specific properties; or**
- **Conduct research involving a reasonable number of records in connection with a specific transaction, legal proceeding, title examination, or legitimate research purpose.**

3.2 Preservation of Public Records Rights. This Policy does not abridge any right of inspection or copying guaranteed under [State] public records law. Where any provision of this Policy conflicts with applicable public records law, applicable law controls.

Section 4. Permissible Purpose Framework

4.1 Permissible Purposes. The following purposes are recognized as consistent with the constructive notice function of the recording system, and access for these purposes shall be accommodated subject to the conditions and requirements of this Policy:

- **Title examination and title insurance underwriting in connection with a specific property transaction;**

- **Legal proceedings, including litigation, foreclosure, probate, and regulatory compliance matters;**
- **Mortgage origination, underwriting, and servicing in connection with specific identified properties;**
- **Law enforcement, court order compliance, and regulatory investigation;**
- **Journalism and academic research conducted in compliance with applicable professional ethics standards;**
- **Non-commercial genealogical and historical research;**
- **Government agency use for official governmental purposes; and**
- **Individual property owners accessing their own records.**

4.2 Non-Permissible Purposes. The following purposes are not consistent with the constructive notice function of the recording system and shall not be authorized under this Policy:

- **AI model training, machine learning dataset development, or similar artificial intelligence applications;**
- **Construction of consumer profiles, surveillance databases, or targeting systems for commercial use;**
- **Commercial data product development using Official Records as a primary or substantial input;**
- **Automated identification and targeting of specific categories of property owners (including without limitation distressed homeowners, elderly homeowners, or homeowners with specific financial characteristics) for commercial solicitation;**
- **Insurance underwriting using Official Records as a proxy for protected class membership; and**
- **Any use that, in the judgment of the County Recorder, is inconsistent with the purposes for which Official Records are maintained.**

Section 5. Bulk and Programmatic Access Requirements

5.1 Prior Approval Required. Bulk Access and Programmatic Access to Official Records requires prior written approval from the County Recorder. Requests shall be submitted on the form prescribed by the Office (Exhibit A) and shall include:

- **Identification of the requesting entity, including all beneficial owners or principals if the requester is an entity;**
- **A detailed description of the specific data elements requested;**
- **A precise statement of the purpose for which the data will be used;**
- **Identification of all downstream users and uses of the data;**
- **A description of the data security measures in place to protect Official Records data from unauthorized access or disclosure; and**
- **Execution of the Data Use Agreement (Exhibit B) as a condition of approval.**

5.2 Review Standards. The County Recorder shall approve a request for Bulk or Programmatic Access if and only if:

- **The stated purpose is a Permissible Purpose under Section 4;**

- **The Data Use Agreement has been properly executed;**
- **The requesting entity has demonstrated adequate data security measures;**
- **The request does not present a foreseeable risk of harm to property owners whose records are included; and**
- **Approval is consistent with applicable state law.**

5.3 Technical Access Controls. The Office shall implement the following technical controls on its public records portal:

- **Rate limiting: No user account or IP address shall be permitted to retrieve more than [500] records per [hour / day] through the public portal without prior approval under this Section.**
- **Automated access detection: The Office shall implement monitoring tools to identify anomalous access patterns indicative of Programmatic Access.**
- **Access logging: All access to the public records portal shall be logged with sufficient detail to identify the accessing IP address, time, and records accessed.**
- **CAPTCHA or equivalent: The public records portal shall implement CAPTCHA or equivalent technical measures to impede automated access.**

Section 6. Data Use Agreement Requirements

6.1 Mandatory Agreement. Any person or entity receiving Bulk Access or Programmatic Access to Official Records shall execute the Data Use Agreement in the form attached as Exhibit B. The Data Use Agreement shall include the following binding commitments:

- **Purpose Restriction: Recipient shall use Official Records data only for the specific Permissible Purpose stated in the access approval, and for no other purpose.**
- **AI Training Prohibition: Recipient shall not use Official Records data to train, fine-tune, evaluate, or otherwise develop artificial intelligence or machine learning systems.**
- **Commercial Restriction: Recipient shall not use Official Records data for Commercial Purposes unless specifically authorized in writing by the County Recorder upon a showing of specific public benefit.**
- **Aggregation Restriction: Recipient shall not combine Official Records data with other data sources in ways that would create consumer profiles, surveillance tools, or targeting systems.**
- **Transfer Prohibition: Recipient shall not transfer, sell, license, or otherwise convey Official Records data to third parties without prior written approval from the County Recorder.**
- **Security Requirements: Recipient shall maintain data security measures at least equivalent to the standards described in the access application and shall notify the County Recorder within [72 hours] of any unauthorized access to or disclosure of Official Records data.**
- **Audit Rights: Recipient shall permit the County Recorder or its designee to audit Recipient's use of Official Records data upon reasonable notice.**
- **Breach Remedies: Material breach of the Data Use Agreement shall constitute grounds for termination of access privileges, demand for return or destruction of all Official Records data, and**

pursuit of available legal remedies.

Section 7. Sensitive Population Protections

7.1 Address Confidentiality Program Integration. The Office shall implement the following additional protections for participants in the [State] Address Confidentiality Program:

- **ACP participant records shall be flagged in the Office's internal database and shall be excluded from any Bulk Access or Programmatic Access authorization.**
- **The Office shall coordinate with the [State] Secretary of State's ACP administration to maintain a current list of substitute addresses for use in verifying ACP status.**
- **Any request for access to records associated with a known ACP substitute address shall be referred to the [State] ACP program administrator for review before fulfillment.**

7.2 Distressed Property Monitoring. The Office shall establish a monitoring program to identify patterns of access to foreclosure, tax delinquency, and lien filing records that may indicate predatory targeting activity, and shall report identified patterns to the County Sheriff, District Attorney, and [State] Attorney General as appropriate.

Section 8. Enforcement and Remedies

8.1 Violation Consequences. Violations of this Policy may result in:

- **Immediate suspension of access privileges;**
- **Permanent revocation of access approval;**
- **Referral to law enforcement for investigation of potential criminal violations (including but not limited to computer fraud, identity theft, and elder financial abuse statutes);**
- **Civil action for breach of the Data Use Agreement; and**
- **Referral to the [State] Attorney General for investigation under applicable consumer protection statutes.**

8.2 Appeal. Any person aggrieved by a decision of the County Recorder under this Policy may appeal in writing to the [County Administrator / Board of Supervisors / applicable body] within [30] days of the decision. The appeal shall be decided within [60] days of receipt.

Section 9. Effective Date and Review

9.1 This Policy shall take effect on [DATE].

9.2 The County Recorder shall review this Policy no less than annually and shall update it as necessary to address emerging threats, changes in applicable law, and developments in technology.

9.3 This Policy shall be published on the Office's public website and shall be made available to any person upon request.

EXHIBIT A — Bulk/Programmatic Access Request Form

[Form design omitted from model — Office to develop consistent with Section 5.1 requirements. At minimum, form should collect: Requester identity and contact information; description of requested data; stated purpose; downstream use description; data security attestation; and signature under penalty of perjury.]

EXHIBIT B — Data Use Agreement Template

[Full Data Use Agreement to be developed by county counsel incorporating the commitments specified in Section 6.1. The Agreement should be structured as a binding contract, not a click-through acknowledgment, and should include governing law (county's state law), dispute resolution provisions, and specific liquidated damages for material breach.]

Part IV: Model State Legislative Proposal

A BILL

TO PROTECT PUBLIC LAND RECORDS FROM ARTIFICIAL INTELLIGENCE

EXPLOITATION AND TO PRESERVE THE INTEGRITY OF THE

PUBLIC RECORDING SYSTEM

SHORT TITLE

This Act shall be known and may be cited as the "Public Recording System Integrity and AI Exploitation Prevention Act" or the "PRSIAEPA."

LEGISLATIVE FINDINGS AND DECLARATION OF PURPOSE

The Legislature finds and declares as follows:

- **Public land records — including recorded deeds, mortgages, liens, and related instruments — serve a critical and limited public purpose: providing constructive notice of property ownership and encumbrances so that subsequent purchasers may verify title and so that priority disputes may be resolved on the basis of recorded priority.**
- **The constructive notice purpose of public land records does not authorize, contemplate, or justify the industrial-scale commercial exploitation of those records by artificial intelligence systems for surveillance, targeting, or data product development.**
- **Artificial intelligence systems are capable of ingesting entire county property record databases in hours, cross-referencing them against other data sources, and constructing detailed profiles of property owners that reveal financial condition, family structure, health status, and other sensitive information that property owners never intended to publicly disclose.**
- **This AI-enabled aggregation has been documented to facilitate specific and serious harms to constituents, including: deed theft and title fraud; predatory targeting of financially distressed homeowners; elder financial exploitation; circumvention of domestic violence address confidentiality**

protections; discriminatory profiling in insurance and lending; and housing market distortion through information asymmetry.

- **These harms fall disproportionately on the most vulnerable members of affected communities, including elderly homeowners, domestic violence survivors, homeowners of color, and financially distressed families.**
- **The Legislature further finds that County Recorders and other public records custodians require clear statutory authority and guidance to implement effective access restrictions, and that a uniform statewide standard is preferable to a patchwork of county-by-county policies.**
- **The purpose of this Act is to protect the integrity of the public recording system, protect constituents from documented harms, and provide clear authority for custodians of public land records to implement access restrictions consistent with the purposes for which those records are maintained.**

SECTION 1 — DEFINITIONS

As used in this Act:

- **"Public Land Records" means official records maintained by County Recorders, including all recorded instruments relating to real property, associated index data, and any database or compilation thereof.**
- **"AI System" means any computational system employing machine learning algorithms, large language models, neural network architectures, or related artificial intelligence techniques to process, analyze, classify, or generate output based on input data.**
- **"Bulk Access" means the systematic acquisition of Public Land Records data in quantities exceeding five hundred (500) records, or the use of automated means to acquire Public Land Records data regardless of the number of records acquired.**
- **"Commercial Purpose" has the meaning provided in [applicable state commercial code or consumer protection statute], and specifically includes: real estate investment targeting, AI model training, consumer profile development, insurance underwriting, marketing database development, and data product commercialization.**
- **"County Recorder" means any county official responsible for maintaining official public land records, including without limitation County Recorder, Register of Deeds, County Clerk, or functionally equivalent office.**
- **"Data Use Agreement" means a binding written agreement governing the use of Public Land Records data by a recipient of Bulk Access approval.**
- **"Permissible Purpose" means a use of Public Land Records consistent with the constructive notice purposes of the recording system, as enumerated in Section 3 of this Act.**

SECTION 2 — COUNTY RECORDER AUTHORITY TO RESTRICT AI AND BULK ACCESS

(a) Authority Established. Notwithstanding any other provision of law, a County Recorder is authorized and empowered to:

- **Implement technical controls on public records portal systems to prevent or limit Bulk Access and Programmatic Access, including rate limiting, CAPTCHA requirements, and access logging;**
- **Require prior written approval for Bulk Access to Public Land Records;**
- **Require execution of a Data Use Agreement as a condition of Bulk Access approval;**
- **Restrict the use of Public Land Records by AI Systems for any purpose inconsistent with the constructive notice function of the recording system;**
- **Prohibit the use of Public Land Records for Commercial Purposes not constituting a Permissible Purpose; and**
- **Take such other reasonable measures as are necessary to protect Public Land Records from uses inconsistent with the purposes for which those records are maintained.**

(b) Preservation of Inspection Rights. Nothing in this Section shall be construed to limit the right of any person to:

- **Inspect individual Public Land Records during regular business hours;**
- **Obtain copies of individual records upon payment of applicable fees; or**
- **Access Public Land Records for any Permissible Purpose subject to the reasonable conditions authorized by this Section.**

(c) Non-Preemption. Nothing in this Act preempts or limits any county ordinance, resolution, or policy that provides greater protection than the minimum standards established in this Act.

SECTION 3 — PERMISSIBLE PURPOSES

(a) Permissible Purposes. The following uses of Public Land Records are hereby designated as Permissible Purposes consistent with the constructive notice function of the recording system:

- **Title examination, title insurance underwriting, and closing services in connection with a specific real property transaction;**
- **Legal representation, litigation, and court proceedings involving specifically identified real property;**
- **Mortgage origination, underwriting, and servicing for specifically identified properties;**
- **Law enforcement, judicial, and regulatory proceedings;**
- **Academic and journalistic research conducted in accordance with applicable professional ethics standards, subject to Data Use Agreement requirements;**
- **Individual property owners accessing records of their own properties;**
- **Non-commercial genealogical and historical research; and**
- **Official governmental use by state and local agencies for governmental purposes.**

(b) Non-Permissible Purposes. The following uses shall not constitute Permissible Purposes:

- **Training, fine-tuning, evaluating, or otherwise developing AI Systems;**
- **Constructing consumer profiles, surveillance databases, or behavioral targeting systems;**

- **Automated identification of property owners based on vulnerability characteristics (including financial distress, advanced age, bereavement, or protected class membership) for Commercial Purposes;**
- **Development of commercial data products in which Public Land Records constitute a primary or substantial input; and**
- **Any use determined by the County Recorder to be inconsistent with the constructive notice purpose of the recording system.**

SECTION 4 — MANDATORY PROTECTIONS FOR SENSITIVE POPULATIONS

(a) Address Confidentiality Program Coordination. County Recorders shall coordinate with the [State ACP Administrator] to:

- **Maintain current identification of Address Confidentiality Program participant records;**
- **Exclude ACP participant records from any Bulk Access authorization; and**
- **Implement technical measures to flag and protect ACP-associated records from automated access.**

(b) Elder Protection Protocols. County Recorders shall implement access controls sufficient to prevent the automated identification and targeting of elderly homeowners from Public Land Records, including without limitation controls on access to records associated with trust instruments, reverse mortgages, and long-duration ownership patterns.

(c) Distressed Property Monitoring. County Recorders shall maintain monitoring sufficient to identify patterns of Bulk Access or Programmatic Access to foreclosure, tax delinquency, and lien filing records, and shall report identified patterns of apparent predatory targeting to the appropriate law enforcement and consumer protection authorities.

SECTION 5 — ENFORCEMENT

(a) Civil Penalty. Any person who violates this Act, or who violates the terms of a Data Use Agreement required under this Act, shall be subject to a civil penalty of not less than [One Thousand Dollars ($1,000)] and not more than [Ten Thousand Dollars ($10,000)] per violation, or three times the commercial benefit derived from the violation, whichever is greater.

(b) Injunctive Relief. The County Recorder or the State Attorney General may bring an action for injunctive relief to prevent or remedy any violation of this Act, in addition to any penalty available under subsection (a).

(c) Private Right of Action. Any property owner whose records are accessed in violation of this Act, and who suffers actual harm as a result, shall have a private right of action against the violating party for actual damages, statutory damages of not less than [Two Thousand Five Hundred Dollars ($2,500)], attorneys' fees, and such other relief as the court deems appropriate.

(d) Attorney General Authority. The State Attorney General may investigate and prosecute violations of this Act as unfair or deceptive trade practices under [applicable state consumer protection statute].

SECTION 6 — STATE AGENCY COORDINATION

(a) The Secretary of State, in consultation with the State Association of County Recorders, shall promulgate statewide model policies and technical standards for AI access restriction by County Recorders within eighteen (18) months of the effective date of this Act.

(b) The Department of Consumer Affairs shall develop and publish guidance for property owners on their rights under this Act and on reporting mechanisms for suspected violations.

(c) The Office of the Attorney General shall establish a dedicated reporting mechanism for County Recorders to report suspected violations of this Act and shall publish an annual report on enforcement activities.

SECTION 7 — EFFECTIVE DATE AND SEVERABILITY

(a) This Act shall take effect [ninety (90) / one hundred eighty (180)] days after enactment.

(b) If any provision of this Act or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.

Legislative Drafting Notes for State Advocates

The following notes are provided to assist advocates in presenting and defending this legislation:

- **The permissible purpose framework in Section 3 is modeled on the Driver's Privacy Protection Act (18 U.S.C. § 2721), which has survived constitutional challenge in every circuit that has considered it. This structure provides maximum legal durability.**
- **The private right of action in Section 5(c) is designed to create a market incentive for compliance in the absence of robust public enforcement resources. The $2,500 statutory damages floor ensures that individual violations are actionable without requiring proof of large actual damages.**
- **Section 6(a)'s model policy mandate is designed to reduce implementation burden on smaller counties that may lack resources to develop independent policies. The 18-month timeline allows reasonable time for state agency development of guidance.**
- **States with existing commercial use restrictions on public records (California, Ohio) may wish to amend those statutes rather than enacting freestanding legislation. In those states, the AI-specific prohibitions in Sections 2 and 3 can be incorporated as amendments to existing frameworks.**

Part V: Implementation Guide for County Recorders

This Part provides a practical roadmap for County Recorders at any stage of readiness to begin implementing protections against AI-powered exploitation of land records. The guide is organized by phase to allow incremental implementation without requiring all measures to be adopted simultaneously.

Phase 1: Immediate Administrative Actions (0–60 Days)

These actions require no capital expenditure, no vendor engagement, and minimal county counsel involvement. They can be implemented by administrative decision of the County Recorder.

Action 1.1 — Issue a Written Access Policy

Draft and publish a written access policy using the model in Part III as a template. Even a simplified version that establishes the bulk access threshold, states the permissible purpose framework, and announces the requirement for data use agreements provides a legal foundation for subsequent enforcement action. A written policy also signals to data brokers and AI operators that your county is alert to the issue, which alone may deter opportunistic harvesting.

Implementation checklist:

- Draft policy using Part III model (full or simplified version)
- Review with county counsel for state law consistency
- Obtain County Recorder signature and effective date
- Publish on Office website and post at public counter
- Notify portal vendor of policy adoption and request confirmation of existing access logging

Action 1.2 — Audit Current Portal Capabilities

Contact your public records portal vendor to determine what access control capabilities currently exist in your system. Most modern portal vendors offer rate limiting, access logging, and IP-based blocking as standard features that may simply need to be enabled. Document the results of this audit in writing so you have a record of what protections are and are not in place.

Key questions for your vendor:

- Does the portal currently log all access by IP address and timestamp?
- Is rate limiting available, and what are the configuration options?
- Can the portal implement CAPTCHA for record retrieval?
- Is there an alert system for anomalous access volumes?
- Can specific IP addresses or user accounts be blocked if violations are detected?

Action 1.3 — Review ACP Compliance

Contact your state's Address Confidentiality Program administrator to confirm that your Office is implementing all required ACP protections in your current system, and to identify any gaps. Request guidance on ACP substitute addresses currently in use in your county so that you can verify they are flagged appropriately in your records database.

Phase 2: Technical Implementation (60–180 Days)

Phase 2 actions require coordination with your portal vendor and, in some cases, IT department engagement or budget authorization.

Action 2.1 — Enable and Configure Rate Limiting

Work with your portal vendor to implement rate limiting. Recommended parameters as a starting point (adjust based on observed legitimate use patterns in your county):

Note: Rate limiting thresholds should be set conservatively initially and adjusted based on observed access patterns. Recorders should notify major legitimate high-volume users (title companies, law firms, lenders) of rate limit implementation with reasonable advance notice and a mechanism to request elevated access for legitimate purposes.

Action 2.2 — Implement Access Logging

Ensure your portal maintains access logs that at minimum capture: IP address, timestamp, records retrieved (by document type and date range), and user account identifier if applicable. Logs should be retained for a minimum of 24 months to support retroactive investigation of access patterns.

Access logs serve two purposes: (1) operational — enabling identification of anomalous access patterns in real time, and (2) evidentiary — providing documentation if enforcement action is required. Without access logs, violations of your access policy are effectively undetectable and unenforceable.

Action 2.3 — Develop and Deploy Data Use Agreement

Working with county counsel, develop a standard Data Use Agreement using the Section 6 requirements from the model policy as a framework. The DUA should be:

- A binding contract (not a click-through), signed by an authorized representative of the requesting entity
- Specific to the stated use case (no blanket approvals for unlimited future use)
- Time-limited (annual renewal with restatement of purpose recommended)
- Subject to audit rights and breach remedies as specified in Section 6.1 of the model policy

Phase 3: Legislative and Intergovernmental Engagement (Ongoing)

Action 3.1 — Engage Your State Recorder Association

Coordinate with your state association of County Recorders to develop a shared policy position on AI access restrictions. A collective position from multiple County Recorders carries substantially more weight with state legislators and the state attorney general than individual county action. Use this compendium as a resource to brief your association leadership.

Action 3.2 — Brief Your State Attorney General

Request a meeting with your state attorney general's consumer protection division to brief them on the documented harms in Part I of this compendium and to present the model state legislation in Part IV. State AGs have independent authority to investigate predatory uses of public records under consumer protection statutes and may be prepared to act before state legislation is enacted.

Action 3.3 — Identify Legislative Champions

Identify one or more state legislators who have demonstrated interest in consumer protection, elder protection, housing affordability, or data privacy as potential sponsors for the model legislation in Part IV. Provide them with the case studies in Part I as constituent-facing documentation of the need for legislative action. Frame the legislation in terms of constituent protection rather than technology restriction — the goal is protecting homeowners, not regulating AI.

Action 3.4 — Engage NACRC and PRIA

Present this compendium and the model policy to the National Association of County Recorders and Elections Officials (NACRC) and the Property Records Industry Association (PRIA) at the next appropriate national convening. Both organizations have model policy development functions that could be used to develop national standards, and NACRC's governmental relations capacity could support federal legislative advocacy if that path becomes viable.

Phase 4: Constituent Communication

County Recorders have a constituent communication responsibility that runs parallel to the policy implementation process. Property owners in your county are largely unaware of the risks AI access to land records creates for them. A proactive communication program:

- Demonstrates that the Recorder's Office is aware of and responding to constituent risks
- Provides property owners with information they can use to identify and report potential targeting
- Creates a public record of the Office's protective posture for liability mitigation purposes
- Builds public and political support for the access restriction policies being implemented

Recommended constituent communication elements:

- Website FAQ: "What is AI harvesting of property records and how is the County Recorder protecting you?"
- Recording fee receipt insert: Brief notice that the Office has adopted an access restriction policy to protect property owner privacy
- Annual report language: Include a brief section on access restriction implementation in any annual report the Office produces
- Coordination with senior services: Brief the county's Area Agency on Aging and adult protective services program on deed fraud and elder targeting risks, with specific reference to land records as a data source

---

Part VI: Quick Reference Resources

Federal and State Contacts

Key Statutory References

Glossary of Key Terms

Sample Constituent FAQ Language

Closing Note: A Word on Urgency

The harms documented in this compendium are not static. They are accelerating. The AI capabilities that enable industrial-scale land records exploitation are advancing rapidly, their cost is falling, and their availability to bad actors is growing. The predatory ecosystem that depends on these capabilities is adapting faster than the regulatory frameworks designed to constrain it.

County Recorders occupy a unique position in this landscape. They are, in most jurisdictions, the only officials with both the custodial authority and the operational capacity to implement immediate access restrictions. Federal law has not acted. Most states have not acted. The regulatory gap will not close quickly.

What County Recorders do in the next twelve to twenty-four months will determine whether the public recording system becomes a permanent input to the commercial surveillance economy — or whether it remains what it was designed to be: a constructive notice system serving property owners and the courts, not a data mine serving the highest bidder.

The legal authority exists. The documented harm is substantial. The policy tools are ready. The question is whether Recorders will use them.

LAND RECORDS INTEGRITY PROJECT

Policy Advocacy Division

policy@landrecordsintegrity.org

June 2026