



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

The United States Constitution

Article II, Section 1 of the U.S. Constitution imposes only three eligibility requirements on persons serving as president, based on the officeholder's age, time of residency in the U.S., and citizenship status:

U.S. Constitution – Presidential Candidate Eligibility

"No person except a natural born Citizen, or a Citizen of the United States, at the time of the Adoption of this Constitution, shall be eligible to the Office of President; neither shall any person be eligible to that Office who shall not have attained to the Age of thirty-five Years, and been fourteen Years a Resident within the United States."

POLICY POSITION PAPER

Civilian Sovereignty in the Digital Age: Ending Corporate Surveillance, Behavioral Manipulation, and Population Control of the American People

Cordova 2028 Presidential Campaign Office of Policy Development

Cordova 2028 | cordova2028.com | info@cordova2028.com

EXECUTIVE SUMMARY

The United States currently operates without enforceable legal protections against mass civilian surveillance, psychological manipulation, and behavioral control conducted by private corporations. The constitutional framework that protects Americans from government overreach does not apply to corporate actors — a gap that has been deliberately and systematically exploited to build the most comprehensive civilian surveillance and manipulation infrastructure in human history.

Private equity firms and institutional asset managers have compounded this problem by financing surveillance operations across networks of smaller entities, deliberately fragmenting their architecture to avoid regulatory thresholds. No existing law reaches the capital layer behind the surveillance economy. No existing law prohibits the deliberate engineering of emotional states, information environments, or psychological compliance at population scale. No existing constitutional provision extends Fourth or First Amendment protections to corporate actors regardless of how much power they accumulate.

This policy document establishes the Cordova administration's complete framework for closing every one of those gaps through:



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

1. An immediate Executive Order closing the public-private surveillance loophole, prohibiting mass civilian surveillance and psychological manipulation with no size or contract threshold, and immediately banning the sale of psychological vulnerability data as a commercial product
2. The American Civilian Sovereignty Act — permanent federal legislation covering all entities at any scale, with affiliate and network liability reaching PE firms and institutional holders, an anti-fragmentation clause, full anti-manipulation prohibitions, a comprehensive data sale prohibition including the absolute ban on psychological vulnerability data, the National Do Not Sell Registry, the National Data Transaction Registry, a private right of action, and the Constitutional People's Counsel as a permanent Article I officer of Congress
3. The American Civilian Sovereignty Amendment — a constitutional amendment extending Bill of Rights protections to all corporate actors at any scale, establishing permanently that American civilian data is not a commodity, enshrining the right to an unmanipulated mind as non-waivable, and permanently establishing the Constitutional People's Counsel
4. Structural reforms to the data broker industry, government procurement, and institutional investor accountability

This framework responds directly to what the American people have asked for. 84% support stricter federal data privacy laws. 73% say they lack adequate control over how their data is used. 80% say government agencies should require a warrant before purchasing their location data. They are not confused. They are not divided. They have been waiting for a government that listens. This framework listens.

A central design principle of this framework is the rejection of new executive branch agencies. New agencies can be captured, defunded, or weaponized against the states and the public by future administrations. Enforcement authority is distributed — across the FTC, DOJ, State Attorneys General, congressional Inspectors General, and the Constitutional People's Counsel — specifically to prevent any single administration from controlling or corrupting the enforcement mechanism.

PART I — THE PROBLEM

1.1 The Surveillance Economy: Scale and Scope

Data Brokers



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

Approximately 4,000 data broker companies currently operate in the United States. The largest — Acxiom, LexisNexis, Equifax, Oracle Data Cloud, Epsilon, and others — hold files on virtually every American adult containing thousands of data points per individual: location history, purchasing behavior, health inferences, financial stress indicators, relationship status, political engagement patterns, religious practice indicators, and psychological profiles derived from behavioral data. These files are sold to advertisers, insurers, employers, landlords, political campaigns, and through a mechanism described in Section 1.3, to government agencies.

No federal law currently prohibits any of this. No threshold of size, revenue, or government contract status triggers a prohibition. A three-person data broker operating below every regulatory threshold can legally hold a complete behavioral profile on every American adult and sell it to any buyer, including foreign governments and federal agencies.

Artificial Intelligence and Behavioral Targeting

Raw surveillance data processed by artificial intelligence becomes a behavioral control instrument. The AI systems operating inside every major social media platform, retail platform, and digital communications service are not neutral content tools. They are behavioral engines — designed to predict human behavior and then alter it.

These systems are trained on surveillance data and optimized to maximize engagement by identifying what produces strong emotional responses: what makes individuals afraid, angry, or outraged. The commercial purpose is advertising revenue. The civic effect is the systematic manipulation of the information environment in which American citizens form their beliefs and make their democratic decisions.

This is not a side effect. It is the product. And it is currently legal.

Psychological Manipulation at Population Scale

Beyond passive surveillance, the surveillance economy has developed active psychological manipulation capabilities that operate without the knowledge or consent of the individuals targeted:

- Algorithmic amplification of fear, anger, and social division to maximize engagement and platform retention
- Filter bubbles and information environment control that restrict what individuals can see and know



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

- Exploitation of behavioral profile data to identify and target psychological vulnerabilities — grief, loneliness, financial stress, addiction — for commercial and political purposes
- Coordinated inauthentic behavior, synthetic content, and deepfake campaigns designed to alter beliefs at scale
- Addictive design systems that override autonomous decision-making

No federal law currently prohibits any of these practices. No consent framework adequately covers them because they are, by design, invisible to the individuals experiencing them.

The Institutional Holder Layer

The surveillance economy is a unified system financed through common ownership. BlackRock, Vanguard, State Street, and Fidelity are simultaneously among the largest shareholders in Google, Meta, Amazon, Microsoft, Palantir, and dozens of data broker and behavioral analytics firms. They exercise governance power over these entities through proxy voting, board appointments, and stewardship activity.

When the same capital controls the surveillance data collection layer, the AI behavioral manipulation layer, the social media distribution layer, and the government contracting layer simultaneously, the phrase "competitive market" becomes a fiction. What exists is a vertically integrated behavioral control system under common ownership with no democratic accountability.

Private Equity's Role and the Fragmentation Problem

Private equity firms have moved aggressively into the surveillance economy, financing and flipping data companies, behavioral analytics firms, and AI startups. Their operating model — acquire, extract, exit — is particularly dangerous here because behavioral data on the American civilian population is among the most valuable commodities on earth.

PE firms have also developed a specific mechanism for defeating regulatory prohibition: deliberate fragmentation. By spreading surveillance operations across multiple smaller entities — each individually below any regulatory threshold — PE firms and institutional holders can maintain full aggregate surveillance capability while ensuring no single entity in the network is technically subject to the prohibition. This is regulatory fragmentation, and it is one of the oldest and most reliable tactics in the private equity playbook.

No existing law addresses this. The Cordova framework does — at all three levels.



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

1.2 The Constitutional Gap

The Fourth Amendment protects Americans against unreasonable searches. The First Amendment protects freedom of speech, assembly, and belief from government interference. These protections apply to the government. They do not apply to corporations — at any scale, under any circumstance, regardless of how much power they accumulate.

In 1791, no private entity possessed surveillance or manipulation capabilities approaching those of the state. In 2024, the most powerful surveillance and behavioral manipulation infrastructure on earth is owned and operated by private entities. The constitutional framework has not kept pace.

The result: Americans have robust theoretical protection against a threat that is no longer the primary one, and almost no protection against the threats that are.

1.3 The Public-Private Surveillance Loophole

The most urgent specific problem is the mechanism by which government agencies circumvent constitutional constraints by purchasing from private intermediaries the surveillance data they are prohibited from collecting directly.

The Fourth Amendment requires a warrant. Private data purchases require a credit card.

Federal agencies — DHS, FBI, DEA, IRS, and elements of the Intelligence Community — have responded to constitutional constraint not by complying with it but by routing around it. They purchase from private data brokers information they cannot legally collect directly: location history, financial data, communication metadata, behavioral profiles.

The legal theory underlying this practice — that data "voluntarily" surrendered to a private party carries no Fourth Amendment protection — is constitutionally indefensible as applied to modern commercial surveillance. No American meaningfully volunteers their location data to every app on their phone or their search history to every platform they use in a way that constitutes a waiver of Fourth Amendment rights.

This loophole is not a technicality. It is the mechanism through which the surveillance state the Fourth Amendment was designed to prevent has been constructed through a private intermediary. The Cordova administration closes it on day one.

1.4 The Managed Population Problem



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

The aggregate effect of mass surveillance, psychological manipulation, AI behavioral targeting, government data acquisition through private intermediaries, and PE-coordinated fragmentation of surveillance networks is what this policy document calls the managed population problem.

A managed population is one in which:

- **Dissent is visible before it organizes.** Behavioral data and social graph analysis can identify organizing activity, political sentiment shifts, and potential civil unrest before they reach critical mass. This capability is currently marketed to government clients by private contractors.
- **Economic compliance is structurally enforced.** Access to credit, insurance, housing, and employment is increasingly determined by algorithmic assessments of behavioral data assembled without consent. Non-compliance carries real economic consequences — invisible, unappealable, systemic.
- **The information environment is controlled.** American citizens do not choose what information reaches them. The algorithm chooses — and the algorithm serves the commercial and ideological interests of the entity that operates it. A population that cannot access accurate, unmanipulated information cannot exercise meaningful democratic self-governance.
- **Fear and division are manufactured inputs.** The behavioral data shows what divides the population and what frightens it. These inputs are deliberately fed into the information environment because division and fear produce engagement, and engagement produces revenue. The political dysfunction Americans experience as a feature of modern democracy is, in significant part, a commercial product.
- **The mind itself is the target.** Psychological manipulation at population scale — engineering emotional states, exploiting vulnerabilities, manufacturing distrust — is not incidental to the surveillance economy. It is the surveillance economy's highest-value product.

This is not a free society. It is an administered one — administered by private entities with no democratic mandate and no public interest obligation, financed by capital that answers only to the return.

1.5 The Data Sale Economy — What Is Actually Happening and What the American People Want Done About It

What Is Happening



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

American civilian data is not merely being collected. It is being sold. Resold. Bundled. Packaged. Traded. Transferred to foreign entities. Purchased by government agencies. Bought by political campaigns, predatory lenders, anti-abortion groups, and employers — through a commercial supply chain that is largely invisible to the individuals whose lives it represents.

The data broker industry — approximately 4,000 companies operating with almost no federal regulation — functions as the wholesale market for American civilian data. These companies do not collect data directly from consumers. They buy it from retailers, apps, platforms, and other brokers, aggregate it into detailed files, and resell it to any buyer willing to pay. By the time a file has been through the resale chain three times, the entity holding it has no legal relationship to the person whose life it represents and no enforceable obligation to protect it.

The harms are documented and concrete. In 2024, a United States senator revealed that a data broker had sold location data tied to visits to nearly 600 Planned Parenthood clinics across 48 states. An anti-abortion group purchased that data and used it to target those individuals with millions of personalized ads. Those people did not consent to that transaction. They did not know it occurred. It was entirely legal.

The most dangerous product in the data sale economy is psychological vulnerability data — AI-generated assessments of an individual's grief, fear, loneliness, financial desperation, addiction vulnerability, and manipulation susceptibility. This data commands the highest prices in the commercial market because it is the most effective tool for exploitation. It is sold to political campaigns, predatory financial services, platforms optimizing for addictive engagement, and anyone else willing to pay for a map of a person's psychological weaknesses. No federal law prohibits this. No consent framework adequately covers it because these assessments are derived by AI from behavioral data — the individual never provided them and often does not know they exist.

45% of Americans have had their personal data stolen or exposed in a breach in the past five years. 40% were unaware until recently that government agencies purchase civilian data from private brokers. The harm is not theoretical. It is happening to real people, in real time, with real consequences.

What the American People Want

The American people have been asked, repeatedly and consistently, what they want. Their answers do not require interpretation.



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

84% say the federal government should implement stricter data privacy laws. This is not a partisan number. In 2023, Pew Research found **68% of Republicans** and **78% of Democrats** support more privacy regulation.

79% are concerned about how their data is used by companies and the government.

73% say they do not have enough control over how companies use their data.

80% say government agencies should be required to obtain a warrant before purchasing their location information. In 2024, a bipartisan majority in the U.S. House passed the Fourth Amendment Is Not For Sale Act — a direct response to this demand.

71% say they would stop doing business with a company if it gave away their sensitive data without permission.

73% are more concerned about their data privacy now than they were a few years ago.

The American people are not confused. They are not divided. They have been saying the same thing, across party lines, for years: stop collecting our data without our consent, stop selling it without our knowledge, and give us the tools to protect ourselves.

Washington has not listened. The American Privacy Rights Act — a bipartisan bill that would have provided basic data protections — was introduced in 2024 and expired in January 2025 without passage. The United States remains the only G20 country without a comprehensive federal data privacy law.

The Cordova administration listens. The framework in this document is the answer the American people have been waiting for.

The Six Gaps the Data Sale Prohibition Closes

Gap 1: Secondary market sales. A covered entity collects data with technically compliant consent, then sells it to a buyer who uses it for purposes the original consent never covered. This framework requires transaction-level consent — the original consent does not travel.

Gap 2: Bulk sale of aggregated profiles. Individual data points may be marginal. Aggregated population-level behavioral profiles are a surveillance weapon. Bulk sale is prohibited regardless of individual consent.



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

Gap 3: Psychological vulnerability data. The most harmful, most valuable, and most exploited category of data. The sale of grief indicators, fear profiles, addiction vulnerability scores, and manipulation susceptibility assessments is prohibited absolutely — no exceptions, no consent workaround, no commercial justification.

Gap 4: Sensitive category data. Location at health clinics, places of worship, political events, and legal proceedings; health and biometric data; religious and political beliefs; sexual orientation; immigration status; children's data — all require express written transaction-specific consent that cannot be conditioned on service access.

Gap 5: Recursive resale liability. Liability travels with the data through every transaction in the resale chain. Every reseller is as liable as the original seller. No party may assert as a defense that a prior seller warranted compliance.

Gap 6: Government acquisition of commercially sold data. The existence of a commercial sale does not launder the constitutional infirmity of government acquisition. Federal agencies may not purchase data that was sold in violation of this framework, and may not use the commercial data market to acquire what they cannot lawfully collect directly.

PART II — THE POLICY FRAMEWORK

2.1 Governing Principles

Principle One: Equivalence of Harm. The harm to a free person from being surveilled, profiled, and behaviorally manipulated is identical whether the actor is a government or a corporation. Legal protections must be equally applicable to both.

Principle Two: No Threshold. No Floor. No Minimum Scale. The right of every American civilian to be free from surveillance, manipulation, and behavioral control is not conditioned on the size of the entity violating it. A three-person data broker and a trillion-dollar platform are equally prohibited from conducting mass civilian surveillance without consent. Any threshold creates a floor that PE firms and institutional holders will engineer their portfolio companies to stay below.

Principle Three: Affiliate and Network Liability Reaches the Capital Layer. The prohibition must reach the entity that finances, directs, and profits from surveillance — not only the entity that technically conducts it. PE firms and institutional holders that construct or finance



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

surveillance networks across multiple entities are jointly and severally liable for the aggregate activity of those networks, to the same extent as if they had conducted the surveillance directly.

Principle Four: Anti-Fragmentation. Deliberately splitting surveillance operations across multiple legal entities to avoid a prohibition is itself a violation — independent of the underlying surveillance. Surveillance fragmentation is treated with the same legal seriousness as financial structuring to evade anti-money laundering law.

Principle Five: The Right to an Unmanipulated Mind Is Non-Waivable. No terms of service, user agreement, or consent form may authorize psychological manipulation, engineered emotional states, information environment control, or exploitation of psychological vulnerabilities. The right of American civilians to autonomous belief formation and an unmanipulated information environment cannot be contracted away.

Principle Six: Consent Is Not a Form Agreement. No terms of service constitutes meaningful consent to mass surveillance or behavioral manipulation. Informed consent requires specific plain-language disclosure, voluntary agreement not conditioned on service access, and the right to revoke at any time.

Principle Seven: Loopholes Are Violations. Government agencies acquiring surveillance data through private intermediaries to circumvent constitutional requirements are committing constitutional violations dressed in commercial clothing. The Cordova administration treats them as such.

Principle Eight: No New Executive Agencies. New executive branch agencies can be captured, defunded, or weaponized against the states and the public by future administrations. The Constitutional People's Counsel is an officer of Congress — not an executive agency — that no President can remove, redirect, or defund unilaterally.

Principle Nine: Permanence Requires Constitutional Foundation. Executive orders can be reversed. Statutes can be repealed. Only a constitutional amendment creates protections durable across administrations and political cycles. The Cordova administration pursues all three layers.

Principle Ten: American Civilian Data Is Not a Commodity. A person's data — their location, their health, their beliefs, their relationships, their psychological vulnerabilities — is an extension of themselves, not an asset to be bought, sold, and resold through a supply chain they never consented to and cannot see. The commercial sale of American civilian data without specific, transaction-level consent is a violation of the same fundamental character as an unreasonable search. The American people have said so clearly. This framework answers them.



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

2.2 Executive Action — Day One

The President signs the **Executive Order on Corporate Surveillance, Psychological Manipulation, and Behavioral Control**:

- Closes the public-private surveillance loophole with immediate effect
- Prohibits all covered federal agencies from contracting with, purchasing data from, or otherwise enabling private surveillance or behavioral manipulation contractors
- Prohibits mass civilian surveillance and psychological manipulation with **no size or contract threshold** — the prohibition applies to every entity
- Establishes **affiliate and network liability**: PE firms and institutional holders are liable for the aggregate surveillance and manipulation conducted by entities within their control
- Establishes the **anti-fragmentation clause**: deliberate structuring of surveillance across entities to evade prohibition is an independent violation
- Prohibits AI-driven psychological manipulation including engineered emotional states, information environment control, exploitation of psychological vulnerabilities, manufactured social division, and synthetic deceptive content
- **Immediately prohibits the sale of psychological vulnerability data** — grief indicators, fear profiles, addiction vulnerability scores, financial desperation markers, and manipulation susceptibility assessments — as a commercial product, with no exceptions and no consent workaround, effective day one
- Prohibits the sale of sensitive category data without express written transaction-specific consent
- Prohibits federal agencies from purchasing commercially sold data that was sold in violation of these prohibitions
- Calls on Congress to establish the National Do Not Sell Registry and National Data Transaction Registry
- Rejects creation of a new executive enforcement agency; distributes interim enforcement across FTC, DOJ, State Attorneys General, and Inspectors General
- Calls on Congress to establish the Constitutional People's Counsel
- Directs DNI review of all Intelligence Community arrangements within 90 days
- Directs OMB to identify and terminate all violating contracts within 60 days

2.3 Legislative Action — 90 Days

The administration submits to Congress the **American Civilian Sovereignty Act**:

Title I — Definitions: Informed consent defined with six mandatory requirements; no consent framework may authorize psychological manipulation.



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

Title II — Prohibitions:

- Mass civilian surveillance prohibited at **any scale, with no threshold**
- **Affiliate and network liability**: PE firms and institutional holders jointly and severally liable for portfolio surveillance activity; 5% equity or board appointment rights triggers presumptive liability
- **Anti-fragmentation**: structuring surveillance across entities to evade prohibition is an independent violation; DOJ and People's Counsel develop joint prosecution guidance within 180 days
- Public-private surveillance loophole closed by statute
- **Psychological and information manipulation prohibited** as a standalone section, covering: engineered emotional states, filter bubbles, exploitation of psychological vulnerabilities, manufactured social division, AI-generated deceptive content; these prohibitions are not waivable by contract
- AI-driven population profiling prohibited
- Targeting of protected political, religious, and civic activities prohibited
- Data export to foreign entities prohibited where it circumvents domestic prohibitions
- Foreign entity surveillance of American civilians prohibited

Section 210 — Data Commodification Prohibition *(responding directly to what 84% of Americans have asked for)*:

- General prohibition on data sale without **specific transaction-level consent** — original consent does not travel with the data
- **Absolute prohibition on bulk sale** of aggregated behavioral profiles regardless of individual consent
- **Absolute prohibition on sale of psychological vulnerability data** — grief indicators, fear profiles, addiction vulnerability scores, financial desperation markers, manipulation susceptibility assessments — no exceptions, no consent workaround, no commercial justification. A person's psychological vulnerabilities are not a product.
- **Sensitive category prohibition** — location at health clinics, places of worship, political events; health and biometric data; religious beliefs; political beliefs; sexual orientation; immigration status; children's data — express written transaction-specific consent required, not conditioned on service access
- **Recursive resale liability** — liability travels with data through every transaction; every reseller jointly and severally liable; no prior seller warranty defense
- **National Do Not Sell Registry** — free, permanent, one registration stops all sales everywhere; FTC maintains; interoperable with all state mechanisms including California Delete Act



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

- **National Data Transaction Registry** — any American can view every transaction involving their data, who purchased it, what was paid, what purpose was stated; fully public and searchable
- Right to complete transaction history on request within 30 days at no cost, going back 7 years
- Prohibition on government purchase of commercially sold data that violates these prohibitions

Title III — Enforcement: Civil penalties of \$10,000 per affected individual per violation with no aggregate cap; criminal penalties up to 15 years for knowing violations; private right of action with no arbitration escape; distributed enforcement across People's Counsel, FTC, DOJ, and State Attorneys General.

Title IV — Structural Reforms: Mandatory data broker registration; institutional holder disclosure; government procurement reform; AI system transparency requirements.

Title V — The Constitutional People's Counsel: Established as a permanent Article I officer of Congress; appointed by joint resolution for a single 7-year term; removable only by impeachment; funded by mandatory appropriation not subject to executive reduction; independent standing to litigate against any entity in any federal court; cross-branch accountability authority; prohibited from being used as instrument against the states; mandatory fully public quarterly reporting.

Title VI — Rights of Civilians: Right to know, right to delete, right to opt out of AI profiling — none waivable by service agreement.

2.4 Constitutional Action — Year One

The administration calls on Congress to propose the **American Civilian Sovereignty Amendment:**

- **Section 1:** Right against surveillance applies to every entity at any scale — no population threshold, no minimum size
- **Section 2:** Right against psychological and behavioral manipulation is a fundamental constitutional right; enumerated prohibitions on engineered emotional states, information environment control, exploitation of psychological vulnerabilities, manufactured social division, and synthetic deceptive content; **the right to an unmanipulated mind is non-waivable by any contract or terms of service**



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

- **Section 3:** Bill of Rights protections apply to all corporate actors at any scale; aggregate activity of affiliated entities treated as activity of one entity; PE firms and institutional holders bear constitutional responsibility for surveillance and manipulation conducted within their portfolios; **no fragmentation or offshore escape at the constitutional level**
- **Section 4:** Public-private surveillance loophole permanently closed — domestic and foreign
- **Section 5:** Population control systems prohibited
- **Section 5A: American Civilian Data Is Not a Commodity** — permanently established as a constitutional principle; absolute prohibition on sale of psychological vulnerability data enshrined at constitutional level; National Do Not Sell Registry and National Data Transaction Registry mandated as permanent federal institutions; right to know, right to delete, and right to prohibit sale established as constitutional rights; recursive resale liability established at constitutional level
- **Section 6:** Constitutional People's Counsel permanently established — cannot be removed by President, cannot be defunded unilaterally, has self-executing litigation standing, prohibited from use against states
- **Section 7:** Private right of action — no arbitration waiver enforceable
- **Section 8:** Congressional enforcement authority

2.5 The Constitutional People's Counsel: Design and Purpose

The Constitutional People's Counsel is the enforcement innovation that makes this entire framework durable and honest.

What it is: An independent officer of Congress — not an executive agency — serving as the permanent public advocate for the constitutional rights of the American people against all concentrations of unaccountable power, governmental or corporate.

Structure:

Feature	Executive Agency	Constitutional People's Counsel
Removable by President	Yes	No
Budget controlled by executive	Yes	No — mandatory appropriation
Appointed by President	Yes	Joint resolution of Congress
Can sue federal government	Rarely	Yes — independently
Can be weaponized against states	Yes	Prohibited by mandate
Survives hostile administration	No	Yes
Reports classified by executive	Possible	No — reports are fully public



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

Authority: Independent standing to sue any entity — corporate, federal, state — in any federal court without authorization from any branch. Subpoena power. Complaint intake from any American civilian. Concurrent enforcement referral to FTC, DOJ, and State Attorneys General while retaining independent litigation authority. Mandatory fully public quarterly reporting to Congress that cannot be classified or suppressed.

What it is not: A rulemaking body. A new bureaucracy. A presidential appointment. An executive instrument. It is a public defender for the Constitution — structured like the GAO or CBO: institutionally durable, politically insulated, belonging entirely to the people it serves.

2.6 Structural Reforms

Data Broker Industry Mandatory registration and public disclosure of all data categories, all government clients, and all institutional holders above 5% ownership. Prohibition on government data sales without court order. Mandatory affirmative consent architecture. Mandatory deletion after defined retention periods.

Institutional Holder Accountability Mandatory quarterly disclosure of surveillance economy holdings. Prohibition on governance coordination across portfolio surveillance companies. FTC review authority for anticompetitive behavior. Elimination of carried interest tax treatment for PE investments in surveillance infrastructure.

Government Procurement Complete prohibition on procurement of civilian surveillance data. Mandatory contractor certification. Permanent debarment for violations. Public registry of all technology contractors and their data-handling practices.

AI System Transparency Mandatory disclosure of all behavioral AI systems operating at scale. Prohibition on AI designed to produce psychological manipulation without consent. Independent audit requirements. Mandatory labeling of AI-generated content distributed at scale.

PART III — IMPLEMENTATION TIMELINE

Action	Timeline
Executive Order signed	Day 1
Public-private loophole closure effective	Day 1
No-threshold prohibition effective	Day 1



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

Affiliate liability and anti-fragmentation effective	Day 1
Anti-manipulation prohibition effective	Day 1
DNI review of Intelligence Community arrangements	30 days
OMB identification of violating contracts	30 days
Contract terminations	60 days
FAR amendment rulemaking initiated	60 days
Data broker registration requirement effective	90 days
American Civilian Sovereignty Act submitted to Congress	90 days
People's Counsel appointment process begins	90 days
Joint DOJ/People's Counsel anti-fragmentation guidance	180 days
People's Counsel fully operational	180 days
Constitutional Amendment proposed to Congress	Year 1
All violating federal contracts terminated	Year 1

PART IV — ANTICIPATED OBJECTIONS AND RESPONSES

"This will harm innovation and the technology sector."

The surveillance economy is not innovation. It is extraction. Collecting behavioral data on three hundred million people without consent, selling it to any buyer, and using AI to engineer their emotional states and manipulate their beliefs is a civil rights violation that has been monetized. The legitimate technology sector — software, hardware, AI research, communications infrastructure that actually serves human needs — does not depend on mass civilian surveillance or psychological manipulation to function. This framework targets those specific functions. It does not restrict technology development.

"National security requires these capabilities."

No legitimate national security function requires the warrantless purchase of mass civilian surveillance data from private brokers or the psychological manipulation of the domestic civilian population. The Fourth Amendment already provides a mechanism for targeted national security surveillance where it is genuinely required: a warrant supported by probable cause. The argument that national security requires circumventing the Fourth Amendment is an argument that national security requires eliminating constitutional rights. The Cordova administration rejects it categorically.



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

"The fragmentation rule will penalize normal corporate structures."

The anti-fragmentation clause targets deliberate structuring of surveillance operations across entities for the purpose or effect of evading a prohibition — not ordinary corporate structure. A corporation with subsidiaries that do not engage in mass civilian surveillance is not affected. A PE firm that deliberately spreads a surveillance operation across twelve shell companies to keep each one below a threshold is exactly what the clause is designed to catch. The distinction is the same one prosecutors draw in financial structuring cases: structure that serves a legitimate business purpose versus structure designed solely to evade legal prohibition.

"People consented to these terms of service."

No one meaningfully consents to mass surveillance by clicking through a forty-page terms of service agreement as a condition of accessing a smartphone. The doctrine that voluntary provision of data to a private party constitutes a waiver of constitutional rights was developed before the surveillance economy existed at population scale. The Cordova framework establishes what informed consent actually means and explicitly provides that no consent framework may authorize psychological manipulation — that right is non-waivable.

"Won't the People's Counsel become politicized?"

The People's Counsel is specifically designed to resist politicization. A 7-year term with removal only by impeachment, mandatory funding that cannot be cut by the executive, appointment by joint resolution rather than presidential nomination, and a strict nonpartisanship requirement are structural safeguards modeled on the most durable independent offices in the federal government. The goal is an institution that outlasts any administration and answers to no one except the public and Congress.

"Doesn't this just expand federal power?"

The opposite. The Constitutional People's Counsel's mandate explicitly includes protecting the states from federal overreach, and its litigation authority covers actions against federal agencies. Enforcement is distributed across the People's Counsel, FTC, DOJ, and State Attorneys General — no single actor controls the mechanism. And the constitutional amendment itself closes the loophole by which the federal government has used private intermediaries to surveil the population it is constitutionally prohibited from surveilling directly. This framework reduces federal surveillance power while creating an independent check on all power.



Cordova for President

Moving Forward Together



www.vincentcordova.com | info@cordova2028.com | (350) 229-1046 | MANTECA, CA 95336

PART V — CONCLUSION

The Cordova administration's civilian sovereignty framework closes every gap that has allowed the surveillance economy to operate without legal constraint — and responds directly to what the American people have been asking for:

- No threshold means no floor for PE firms to engineer around
- Affiliate liability means the capital behind surveillance cannot hide behind portfolio company structure
- Anti-fragmentation means deliberate evasion is itself a crime
- Anti-manipulation means psychological engineering of the American civilian population is prohibited regardless of commercial justification or any purported consent
- **Data commodification prohibition** means American civilian data is not a product — it cannot be sold, resold, or traded without specific transaction-level consent, and psychological vulnerability data cannot be sold under any circumstances
- **National Do Not Sell Registry** means any American can permanently stop the sale of their data with a single free registration
- **National Data Transaction Registry** means the supply chain that has profited in the dark operates in the light — every American can see every transaction involving their data
- The Constitutional People's Counsel means enforcement belongs to the public — not to whichever party controls the White House

84% of Americans support stricter federal data privacy laws. 73% say they lack adequate control over their data. 80% say the government needs a warrant before purchasing their location information. They have been saying this for years. This framework is the answer.

The American people are not a population to be managed. Not by their government. Not by a corporation. Not by a private equity firm. Not by an algorithm. Not by any concentration of power — however it is organized, however it is financed, however it is branded. And their most private and vulnerable selves — their grief, their fears, their psychological wounds — are not products to be packaged and sold to the highest bidder.

This framework makes that principle enforceable law. Permanently.

Cordova 2028 Presidential Campaign cordova2028.com | info@cordova2028.com