PUBLIC POWER THROUGH PRIVATE INFRASTRUCTURE ACT

Deep research report and model federal statute

A focused legislative proposal governing private surveillance infrastructure intentionally designed for governmental investigative use

Prepared as Volume II-A of the Private Infrastructure, Public Power project

Research current through July 19, 2026

This report is a policy and legislative research document, not legal advice. It distinguishes existing constitutional holdings from proposed protections that would operate above the constitutional floor.

Executive Summary

The problem addressed by this report is not simply that private companies collect data. It is that a growing class of companies deliberately builds, markets, and operates infrastructure to extend governmental identification, tracking, searching, and investigative capability. The government may thereby obtain persistent surveillance capacity without owning the sensors, creating the database, or directly employing the people who operate the system.

Existing constitutional doctrine does not provide a reliable answer. The Fourth Amendment governs government searches, but private collection may occur before government acquisition. State-action doctrine reaches private conduct only through narrow tests such as government compulsion, joint action, entwinement, or performance of a function traditionally and exclusively reserved to the State. The Supreme Court has repeatedly emphasized that merely serving the public or contracting with government does not ordinarily transform a private entity into a state actor.

At the same time, the Supreme Court's digital-search decisions establish a critical substantive principle: scale, persistence, aggregation, and retrospective search can make digital surveillance qualitatively different from isolated observation. United States v. Jones, Riley v. California, Carpenter v. United States, and Chatrie v. United States all reinforce, in different ways, that digital systems can expose a comprehensive record of movement, association, and private life.

The recommended solution is therefore statutory rather than doctrinal. Congress should create a defined category of Covered Government Surveillance Infrastructure Provider and regulate both the provider and the government customer's use of the provider's system. The Act should not declare every covered vendor a state actor, and it should not prohibit legitimate investigative technology. It should instead impose market-entry, procurement, audit, accuracy, disclosure, and use restrictions proportionate to the public power exercised through the infrastructure.

The recommended enactment is a new standalone federal statute, supplemented by targeted amendments to federal procurement law, the Stored Communications Act, the Privacy Act, and grant conditions. A standalone act is preferable because the regulated object is neither merely a government record nor merely an electronic communication. It is an integrated public-private capability: sensors, databases, identity resolution, cross-jurisdiction access, algorithmic search, and government action.

Core legislative design:

- Define coverage by function and government-facing commercial purpose, not by brand or device type.
- Require registration, public system descriptions, customer disclosure, audit logs, use policies, security testing, and independent compliance assessments.
- Prohibit unrestricted nationwide or cross-jurisdiction searching without documented legal authority and purpose.
- Require corroboration before coercive action based on probabilistic or automated matches.
- Create correction, notice, and redress mechanisms when covered data materially contributes to an adverse governmental action.
- Use federal procurement, interstate-commerce regulation, grant conditions, and FTC enforcement as complementary implementation mechanisms.
- Preserve narrow emergency exceptions, judicially supervised sealing, and national-security accommodations without creating a blanket exemption.

Principal Recommendation

Congress should enact the Public Power Through Private Infrastructure Act as a new federal regulatory framework. The Act should be administered jointly by the Department of Justice and the Federal Trade Commission, with procurement implementation by the Office of Management and Budget and the Federal Acquisition Regulatory Council. States should remain free to enact stronger protections.

What This Report Does Not Cover

This report intentionally excludes the separate Government Data Lifecycle Accountability Act, which governs retention, replication, transmission, secondary use, and deletion after governmental acquisition. It also excludes the broader project concerning private-law systems that practically suppress civic or constitutional freedoms. Those are separate reports.

1. Continuity with the Problem Brief

The earlier problem brief identified a public-private surveillance pipeline: private collection, centralized aggregation, governmental access, algorithmic inference, coercive action, and fragmented accountability. It documented how automated license-plate readers, commercial facial recognition, location-data brokers, residential camera networks, telecommunications intermediaries, and cloud evidence systems can distribute responsibility among multiple actors while preserving the practical effect of governmental surveillance.

Statute 1 targets the front half of that pipeline. It asks when a private company ceases to be an ordinary vendor and becomes a supplier of persistent public investigative power. Its purpose is to regulate the creation and governmental availability of the capability itself. Statute 2 separately governs what government may do with information after acquisition.

Problem identified	Existing legal gap	Statutory response
Private sensor networks become searchable government infrastructure	Constitution generally binds government, not upstream private collection	Create a regulated provider category and government procurement conditions
Cross-jurisdiction search converts local cameras into national tracking	Local procurement and policy do not control remote downstream users	Purpose limitation, jurisdiction rules, audit logs, and approval requirements
Commercial data purchase can bypass ordinary compulsory process	Access rules vary by data type and acquisition method	No-purchase circumvention rule and legal-process parity
Automated matches produce coercive consequences	Vendor accuracy and police corroboration rules are fragmented	Accuracy testing, disclosure, and independent corroboration
Responsibility is distributed among vendor, agency, and data contributor	No unified duty to preserve logs and identify decision provenance	Mandatory auditability and joint recordkeeping

2. The Legal Architecture of the Gap

2.1 The Fourth Amendment regulates governmental searches, not an entire commercial supply chain

The Fourth Amendment prohibits unreasonable governmental searches and seizures. Its protections are often triggered when government acquires or searches information, not when a private party initially creates or stores it for independent purposes. The private-search doctrine can also allow government to repeat or use aspects of a genuinely private search without converting the original private act into government conduct, although governmental instigation or participation can alter the analysis.

This creates an upstream gap. A commercial provider may build a nationwide database before any particular police query occurs. The later query may implicate the Fourth Amendment, but the architecture, default sharing, retention, customer permissions, and algorithmic features may already have been fixed by private contract.

The Act should therefore regulate commercial conduct and procurement directly rather than depend on case-by-case suppression litigation after an investigation.

2.2 Digital aggregation changes constitutional significance

United States v. Jones restored a property-based Fourth Amendment analysis for physical GPS installation, while five Justices separately emphasized the privacy significance of prolonged monitoring. Riley v. California required warrants for cell-phone searches incident to arrest because digital devices differ quantitatively and qualitatively from ordinary physical containers. Carpenter v. United States held that government acquisition of seven days of historical cell-site location information was a search and declined to apply the third-party doctrine mechanically to a detailed chronicle of physical movements.

In Chatrie v. United States, decided June 29, 2026, the Supreme Court addressed geofence data and clarified Carpenter's application to reverse identification from provider-held location records. Whatever the precise boundary in future cases, the decision confirms that reverse searching and aggregated provider databases remain central Fourth Amendment questions rather than ordinary subpoenas for isolated business records.

The legislative lesson is broader than the holdings: Congress can regulate systems according to persistence, scale, sensitivity, and retrospective search capability without waiting for a categorical constitutional rule covering every technology.

2.3 State-action doctrine is an unreliable regulatory trigger

Under Lugar v. Edmondson Oil Co., private conduct may be attributable to the State when the deprivation results from a state-created rule and the private actor is fairly treated as a state actor. Brentwood Academy v. Tennessee Secondary School Athletic Association recognized entwinement as a basis for attribution. But Blum v. Yaretsky, Rendell-Baker v. Kohn, Jackson v. Metropolitan Edison Co., and Manhattan Community Access Corp. v. Halleck sharply limit the public-function and nexus theories.

Halleck states the modern rule bluntly: a private entity is ordinarily not constrained by the First Amendment, and the public-function exception generally applies only when government has delegated a function traditionally and exclusively performed by government. Operating surveillance technology, selling information, or contracting with police will not automatically satisfy that test.

That is precisely why a statute is necessary. Congress need not redefine state action to regulate interstate surveillance commerce, federal purchasing, or recipients of federal law-enforcement funds.

2.4 Existing remedies are fragmented and reactive

42 U.S.C. § 1983 supplies a cause of action against persons acting under color of state law, but the threshold state-action inquiry remains. The exclusionary rule may suppress evidence in criminal

cases, but it does not comprehensively regulate vendor design or provide relief to all non-defendant subjects. The Federal Trade Commission may challenge unfair or deceptive commercial practices, yet Section 5 of the FTC Act does not create a complete government-surveillance code. Procurement rules address contract integrity, cybersecurity, and prohibited equipment, but not a general constitutional-impact review for surveillance products.

3. Existing Statutory Models

No existing federal statute is a complete fit. Several statutes nevertheless supply reusable legislative modules.

Model	Reusable mechanism	Application to proposed Act
Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.	Permissible purposes, accuracy procedures, disclosure, dispute and correction, user duties, civil liability	Limit surveillance queries to authorized purposes; require accuracy, access and correction when data contributes to adverse action
Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725	Default prohibition with enumerated permissible uses; redisclosure rules; civil remedies	Use an enumerated-purpose architecture for government access and onward sharing
Stored Communications Act, 18 U.S.C. §§ 2701-2713	Provider-government access rules keyed to process and data category	Apply legal-process parity where government buys or queries data functionally equivalent to compelled records
Privacy Act of 1974, 5 U.S.C. § 552a	System notices, purpose limitation, access, amendment, accounting of disclosures	Require system descriptions, audit accounting, notice and correction for federal use
FTC Act § 5, 15 U.S.C. § 45	Unfairness and deception enforcement	Authorize FTC civil enforcement against misrepresentation, undisclosed sharing and unfair surveillance commerce
Federal Acquisition Regulation	Mandatory clauses, certifications, audit and debarment	Make compliance a condition of federal procurement and flow duties to subcontractors
Section 889 procurement restrictions, 41 U.S.C. § 3901 note / FAR 52.204-25	Categorical restrictions on covered technology and supplier representations	Demonstrates Congress can restrict acquisition based on systemic technology risk

3.1 Fair Credit Reporting Act analogy

The FCRA is the strongest structural analogy because it regulates a private information industry whose records materially affect governmental and private decisions. Congress found that inaccurate reports impair economic systems and public confidence. The statute limits permissible purposes, requires reasonable procedures for maximum possible accuracy, gives consumers access and dispute rights, regulates furnishers and users, and creates civil remedies.

Surveillance databases similarly convert dispersed records into identity-linked reports that may produce stops, questioning, watchlisting, immigration consequences, or investigation. The analogy does not mean surveillance records are consumer reports under current law. It shows that Congress can regulate an information intermediary by assigning duties to the database operator, data furnisher, and end user.

3.2 Driver's Privacy Protection Act analogy

The DPPA establishes a default prohibition on disclosure of personal information from motor-vehicle records, followed by enumerated permissible uses. It also restricts resale and redisclosure and creates a private civil action. This architecture is well suited to public-private surveillance: default prohibition, specified governmental purposes, documented authorization, controlled redisclosure, and damages for knowing violations.

3.3 Stored Communications Act and the anti-circumvention principle

The Stored Communications Act specifies when providers may disclose communications and records to government. Yet modern agencies may purchase access to commercial datasets rather than compel them. The proposed Act should adopt a parity rule: government may not avoid legal process by purchasing, licensing, or remotely querying information that would require legal process if compelled directly from a provider.

This principle aligns with legislative efforts commonly described as the Fourth Amendment Is Not For Sale Act, although the proposed Act is broader because it also regulates network architecture, cross-jurisdiction access, and vendor obligations.

3.4 Privacy Act and procurement analogies

The Privacy Act applies to federal agency systems of records and includes notice, access, correction, purpose limitation, and disclosure-accounting mechanisms. It does not comprehensively reach contractor-controlled shared surveillance systems or all inferred data. Federal procurement law, however, can impose contractual clauses, certifications, audit rights, and suspension or debarment. The best design combines substantive statutory duties with mandatory contract clauses.

4. Evidence Supporting Legislative Action

4.1 Non-federal facial-recognition systems

The Government Accountability Office reported in 2021 that 20 of 42 surveyed federal law-enforcement agencies owned or used facial-recognition systems and 15 used non-federal systems. GAO found that 13 agencies lacked mechanisms to track employee use of non-federal systems and recommended both tracking and privacy/accuracy risk assessment. Later GAO updates documented agency-specific implementation but also showed how decentralized vendor access can escape ordinary system inventory.

This is a direct empirical justification for provider registration, user logging, agency approval, and system-risk assessment.

4.2 Commercial location data sold for public-sector use

The FTC's 2024 action against Gravy Analytics and Venntel alleged unfair sale and use of sensitive location data and stated that Venntel sold information and analytical tools to public-sector customers. The FTC alleged that the data could reveal visits to sensitive locations and was associated with persistent identifiers, timestamps, IP addresses, and source applications.

The case shows why a general consumer-consent framework is insufficient. The government's use of a commercial surveillance product creates public-law consequences for people who never contracted with the government-facing vendor.

4.3 Automated license-plate systems

California's Civil Code §§ 1798.90.5-1798.90.55 regulates automated license-plate recognition operators and end users through security requirements, usage and privacy policies, access controls, and civil remedies. It supplies a concrete state-law precedent for regulating both operators and users rather than relying exclusively on constitutional litigation.

The federal Act should build upon this dual-actor structure while addressing interstate networks, cross-jurisdiction access, governmental purpose, accuracy, and procurement.

4.4 Why federal legislation is justified

- The services and datasets routinely cross state lines and are sold through interstate commerce.
- A local camera may contribute records to a network searchable by remote agencies.
- Federal agencies and federally funded state and local agencies use non-federal systems.
- Different state retention and access rules cannot fully govern a nationally shared platform.
- A federal baseline can preserve stronger state protections while reducing vendor forum shopping.

5. Legislative Design Choices

5.1 Coverage should be functional, not brand-specific

The statute should avoid naming Flock, Ring, Clearview, or any current vendor. Coverage should turn on whether the entity offers a system whose substantial commercial purpose is enabling governmental identification, tracking, reverse search, biometric comparison, association analysis, or persistent observation.

A 'primary purpose' test alone is too easy to evade through mixed-use marketing. The recommended trigger is a substantial-purpose test combined with objective indicators: government-specific product tiers, law-enforcement integration, government customer revenue, restricted investigative interfaces, cross-jurisdiction query capability, or contractual commitments to support investigations.

5.2 Distinguish providers, contributors, and government users

The Act should separately define: (1) the infrastructure provider; (2) a private data contributor such as a business or homeowner association; and (3) a government user. Duties should reflect control. Providers control architecture and permissions. Contributors control sensor placement and initial participation. Government users control investigative purpose and coercive action.

5.3 Regulate capability without outlawing all observation

The strongest constitutional and practical case is not a blanket ban on cameras viewing public space. Courts have long recognized reduced privacy in what is knowingly exposed to public observation. The distinctive concern is the transformation of isolated observations into persistent, searchable, identity-linked, cross-jurisdiction infrastructure.

Accordingly, the model Act does not prohibit an ordinary business security camera that incidentally captures a sidewalk. It applies when the system is integrated into a government-facing network, supports systematic identification or retrospective search, or routinely transmits data for governmental investigative use.

5.4 Require legal-process parity and purpose limitation

Government should not be able to evade a warrant, court order, or subpoena requirement by substituting a commercial license for compulsory process. The parity clause should require the same or greater legal process when information is bought, remotely queried, obtained through a trial account, or requested from a private contributor.

Separately, every query should identify an authorized purpose, case or incident number, requesting official, jurisdictional basis, and applicable legal authority. 'Training,' 'general intelligence,' and curiosity searches should be prohibited unless independently authorized and audited.

5.5 Build in corroboration and provenance

Automated license-plate and facial-recognition matches are investigative leads, not adjudicated facts. The Act should prohibit arrest, high-risk stop, search, seizure, immigration hold, or adverse administrative action based solely on an automated match. It should require independent corroboration and preservation of the query, candidate list, confidence information, data source, and human review.

5.6 Remedies must be calibrated

A private right of action is appropriate for knowing or reckless violations that cause concrete harm, unauthorized disclosure, or material adverse governmental action. Technical violations that cause no material risk may be addressed through agency enforcement and cure periods. Suppression should remain governed by existing constitutional and statutory doctrine unless Congress expressly provides otherwise.

6. Recommended Federal Structure

The report recommends a standalone act with four coordinated enforcement channels:

- FTC jurisdiction over covered providers and unfair or deceptive surveillance commerce.
- DOJ rulemaking and enforcement for government investigative use, audit standards, and civil-rights compliance.
- Federal procurement clauses, certifications, suspension, and debarment.
- Conditions on federal law-enforcement grants to state, tribal, territorial, and local agencies.

This structure avoids relying on a single agency and matches authority to institutional competence.

7. Model Statutory Text

PUBLIC POWER THROUGH PRIVATE INFRASTRUCTURE ACT OF 2026

A BILL

To regulate commercial surveillance infrastructure intentionally used to extend governmental investigative or coercive capability; to establish transparency, authorization, audit, accuracy, procurement, and redress requirements; and for other purposes.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Public Power Through Private Infrastructure Act of 2026."

SEC. 2. FINDINGS.

Congress finds that—

(1) private entities increasingly develop and operate systems that enable governmental identification, tracking, reverse search, biometric comparison, association analysis, and persistent observation;

(2) such systems may combine records contributed by governmental and private sensors across multiple jurisdictions;

(3) aggregated and retrospective digital surveillance may reveal substantially more than an isolated observation;

(4) governmental access to commercial surveillance infrastructure may occur through purchase, license, remote query, voluntary disclosure, or integration rather than compulsory legal process;

(5) federal agencies have used non-federal facial-recognition systems without complete tracking or risk assessment, as documented by the Government Accountability Office;

(6) commercial location-data markets have supplied analytical products to public-sector customers and can reveal visits to sensitive locations;

(7) existing constitutional, consumer-protection, procurement, and privacy rules regulate only portions of this activity; and

(8) a uniform federal baseline is necessary to protect constitutional interests, public safety, interstate commerce, and public confidence.

SEC. 3. PURPOSES.

The purposes of this Act are—

(1) to preserve legitimate public-safety and investigative uses of advanced technology;

(2) to prevent private infrastructure from becoming an unaccountable channel of governmental power;

(3) to require authorization, transparency, auditability, accuracy, and redress proportional to the capability supplied;

(4) to prevent government from circumventing legal-process requirements through commercial acquisition;

(5) to preserve stronger protections provided by State law; and

(6) to promote accountable innovation in surveillance technology.

SEC. 4. DEFINITIONS.

In this Act:

(1) COVERED GOVERNMENT SURVEILLANCE INFRASTRUCTURE PROVIDER.—The term means a person that, in or affecting interstate commerce, develops, markets, licenses, operates, or materially maintains a system for which a substantial commercial purpose is to enable a governmental entity to identify, locate, track, compare, infer, reverse search, or investigate a natural person through persistent observational data.

(2) COVERED SYSTEM.—The term means the hardware, software, database, model, network, interface, or integrated service supplied by a covered provider.

(3) PERSISTENT OBSERVATIONAL DATA.—The term means records derived from observation of persons, devices, vehicles, faces, voices, movements, associations, searches, or presence that are retained, aggregated, linked, or made retrospectively searchable.

(4) REVERSE SEARCH.—The term means a search that begins with a place, time, characteristic, image, plate fragment, keyword, behavior, or other attribute and returns one or more persons, devices, vehicles, accounts, or identities not previously specified.

(5) GOVERNMENTAL ENTITY.—The term includes a Federal, State, tribal, territorial, or local department, agency, instrumentality, prosecutor, law-enforcement body, intelligence body, or contractor acting on its behalf.

(6) PRIVATE DATA CONTRIBUTOR.—The term means a nongovernmental person that supplies sensor data or records to a covered system.

(7) MATERIAL ADVERSE GOVERNMENTAL ACTION.—The term includes arrest, detention, search, seizure, immigration action, watchlisting, denial of a license or benefit, or another action materially affecting liberty, property, or legal status.

(8) SENSITIVE LOCATION.—The term includes a place of worship, health-care facility, reproductive-health facility, shelter, school, union hall, political gathering, legal-services office, or other location designated by rule because observation would create comparable risk.

(9) AUTOMATED MATCH.—The term means a probabilistic or algorithmic output asserting or ranking a possible correspondence between data and a person, vehicle, device, or identity.

SEC. 5. REGISTRATION.

(a) A covered provider may not offer a covered system to a governmental entity unless registered with the Federal Trade Commission.

(b) Registration shall identify ownership, controlling persons, covered products, governmental customer categories, data sources, private-contributor programs, subprocessors, jurisdictions in which the system operates, and material algorithmic functions.

(c) The Commission shall maintain a public registry, except for narrowly classified information submitted under section 17.

SEC. 6. PUBLIC SYSTEM DESCRIPTION AND IMPACT ASSESSMENT.

(a) Before first governmental deployment, a covered provider and the governmental customer shall publish a system description and surveillance impact assessment.

(b) The assessment shall describe purpose, geographic scope, data sources, query types, legal authority, sharing, accuracy, known limitations, security, retention categories, civil-rights risks, and procedures for complaint and correction.

(c) Classified or operationally sensitive details may be summarized or withheld only to the minimum extent authorized by law, with an unclassified statement of the withheld category and legal basis.

SEC. 7. PERMISSIBLE GOVERNMENTAL PURPOSES.

(a) A covered system may be queried by a governmental entity only for—

(1) investigation of a specified criminal offense;

(2) locating a missing, endangered, or abducted person;

(3) identifying an imminent threat of death or serious bodily injury;

(4) execution of a judicial warrant or court order;

(5) another purpose expressly authorized by Federal or State statute and designated by rule.

(b) A query may not be conducted solely to identify or monitor persons based on First Amendment activity, race, religion, national origin, disability, sex, or lawful reproductive or medical activity.

(c) Each query shall include a case or incident identifier, authorized purpose, requesting user, time, jurisdictional basis, and legal authority.

SEC. 8. LEGAL-PROCESS PARITY; PROHIBITION ON PURCHASED CIRCUMVENTION.

A governmental entity may not purchase, license, remotely query, receive, or direct a private person to obtain information through a covered system if compulsory acquisition of materially equivalent information from the provider or source would require a warrant, court order, subpoena, or other legal process, unless the governmental entity first obtains that process or a recognized emergency exception applies.

SEC. 9. CROSS-JURISDICTION ACCESS.

(a) A governmental entity may not provide unrestricted access to a covered system to an outside jurisdiction.

(b) Cross-jurisdiction access requires a written agreement specifying authorized purposes, applicable law, user eligibility, audit access, redisclosure limits, and suspension procedures.

(c) A query directed at conduct lawful in the jurisdiction where it occurred may not be executed solely to enforce the law of another jurisdiction, except for an offense involving death, serious bodily injury, trafficking, abduction, or another category specifically authorized by Congress.

(d) Originating agencies and providers shall technically enforce jurisdictional restrictions.

SEC. 10. PRIVATE DATA CONTRIBUTORS.

(a) A covered provider shall give a private data contributor clear notice of governmental access, network scope, data categories, retention category, and ability to suspend participation.

(b) A contributor may not authorize collection from a location in which the contributor lacks lawful authority to place or operate the sensor.

(c) A provider may not represent that contributor consent supplies independent legal authority for government to conduct a search that otherwise requires legal process.

(d) A contributor program that systematically captures public streets, sidewalks, residences, places of worship, or other nonparticipant activity shall be disclosed in the public system description.

SEC. 11. AUDIT LOGS AND USER CONTROLS.

(a) A covered provider shall maintain immutable logs of every governmental query, export, alert, match, permission change, and cross-jurisdiction disclosure.

(b) Logs shall record user, date, time, purpose code, legal authority, query parameters, records returned, downstream export, and supervisory approval where required.

(c) Providers shall implement role-based access, multifactor authentication, periodic access review, anomaly detection, and immediate account suspension capability.

(d) Logs shall be available to authorized inspectors general, courts, oversight bodies, and the Commission, subject to lawful protections.

SEC. 12. ACCURACY, TESTING, AND CORROBORATION.

(a) A covered provider shall use reasonable procedures to assure accuracy, document known error modes, and conduct independent testing appropriate to the technology.

(b) A provider shall disclose confidence scores, candidate-list behavior, input quality limitations, and demographic or environmental performance differences where technically applicable.

(c) No governmental entity may take a material adverse governmental action based solely on an automated match.

(d) Before such action, a trained official shall obtain independent corroboration and document the corroborating evidence.

(e) A provider shall preserve the input, output, candidate list, model or version identifier, and human-review record relevant to the action.

SEC. 13. NOTICE, ACCESS, AND CORRECTION.

(a) When covered-system data materially contributes to a material adverse governmental action, the affected person shall receive notice of that fact and the provider category, unless delayed by a court upon a showing that notice would create a substantial risk to an investigation, person, or national security.

(b) After the need for delay ends, the person may obtain the data materially relied upon, an accounting of relevant queries and disclosures, and a description of automated processing, subject to protective orders.

(c) A person may dispute inaccurate identity, plate, device, location, or association information. The provider and governmental user shall conduct a reasonable reinvestigation and correct, annotate, or delete information that is inaccurate, incomplete, or unverifiable.

(d) Correction shall be propagated to recipients that received the disputed information within the period established by rule.

SEC. 14. TRANSPARENCY REPORTS.

Each covered provider shall publish at least annually—

(1) the number and categories of governmental customers;

(2) aggregate query counts by purpose and jurisdiction;

(3) cross-jurisdiction query counts;

(4) emergency requests;

(5) rejected or suspended queries;

(6) security incidents;

(7) correction requests and outcomes;

(8) government demands for secrecy;

(9) material changes in system capability; and

(10) independent audit findings, with lawful redactions.

SEC. 15. GOVERNMENT PROCUREMENT AND GRANT CONDITIONS.

(a) No Federal agency may acquire or renew a covered system unless the solicitation and contract contain clauses implementing this Act.

(b) The Federal Acquisition Regulatory Council shall issue clauses requiring certification, audit access, subcontractor flow-down, breach reporting, data portability, termination assistance, and deletion or return upon contract end.

(c) Material or repeated violation is grounds for suspension, debarment, contract termination, and recovery of funds.

(d) As a condition of specified Federal law-enforcement grants, recipients shall certify compliance with sections 6 through 14.

SEC. 16. ENFORCEMENT.

(a) A violation by a covered provider constitutes an unfair or deceptive act or practice enforceable by the Federal Trade Commission under section 5 of the Federal Trade Commission Act.

(b) The Attorney General may bring a civil action for declaratory, injunctive, or monetary relief.

(c) A State attorney general may bring a civil action on behalf of residents after notice to the Attorney General and the Commission.

(d) The Commission may assess civil penalties for knowing violations and order deletion, access suspension, corrective notice, compliance monitoring, or consumer redress.

(e) Nothing in this Act limits other Federal or State remedies.

SEC. 17. PRIVATE CIVIL ACTION.

(a) A person aggrieved by a knowing or reckless violation of sections 7, 8, 9, 11, 12(c), 13, or 18 may bring an action against the covered provider or governmental entity responsible for the violation.

(b) Relief may include actual damages, statutory damages of not less than $1,000 for a material violation, punitive damages for willful misconduct, equitable relief, and reasonable attorney's fees.

(c) A governmental entity retains only those immunities expressly preserved by applicable Federal law; acceptance of Federal funds conditioned on compliance constitutes consent to appropriate prospective relief.

(d) A claim shall be brought within two years after discovery, but not more than five years after the violation, except in cases of fraudulent concealment.

SEC. 18. PROHIBITED PRACTICES.

A covered provider or governmental entity may not—

(1) falsify or materially omit an audit log;

(2) create a shared account intended to defeat user attribution;

(3) knowingly permit access by an unauthorized person;

(4) sell or disclose sensitive-location tracking for a prohibited purpose;

(5) use covered data to identify persons engaged solely in protected speech, assembly, worship, journalism, or legal representation;

(6) retaliate against a person for filing a complaint or correction request;

(7) materially misrepresent system accuracy, geographic coverage, legal authority, or government access; or

(8) use contract terms to prevent a governmental customer from complying with public-records, audit, or oversight law.

SEC. 19. EMERGENCY AND NATIONAL-SECURITY PROCEDURES.

(a) An emergency query may be conducted without otherwise required process when an authorized official reasonably believes immediate access is necessary to prevent imminent death or serious bodily injury.

(b) The official shall document the facts, scope, and results and seek judicial review within 48 hours where process would otherwise have been required.

(c) National-security activities remain subject to the Foreign Intelligence Surveillance Act and other applicable law. The Attorney General may issue narrowly tailored rules for classified programs, but may not exempt commercial systems from registration, audit preservation, or inspector-general review to the extent consistent with national security.

SEC. 20. RULEMAKING AND TECHNICAL STANDARDS.

Within 18 months, the Commission, the Attorney General, the Director of the Office of Management and Budget, and the National Institute of Standards and Technology shall issue coordinated rules and standards. Rulemaking shall address coverage thresholds, testing, audit-log integrity, impact assessments, correction, transparency, and small-provider compliance.

SEC. 21. PREEMPTION.

This Act establishes a floor and does not preempt a State or local law that provides greater protection, stricter procurement standards, shorter retention, broader notice, or additional remedies. A State may not authorize conduct prohibited by this Act.

SEC. 22. SEVERABILITY.

If any provision or application of this Act is held invalid, the remainder of the Act and its application to other persons and circumstances shall not be affected.

SEC. 23. EFFECTIVE DATE.

(a) Registration and rulemaking provisions take effect on enactment.

(b) Procurement requirements take effect 24 months after enactment.

(c) Existing contracts shall be brought into compliance at renewal or within 36 months, whichever occurs first.

(d) The Commission may grant a limited extension upon a public finding of substantial technical necessity.

8. Section-by-Section Commentary

Sections 1-3

Establish the Act's identity, factual predicate, and purpose. Findings should be supported during the legislative process with hearings on vendor networks, federal use of non-federal systems, data-broker sales, error cases, and cross-jurisdiction access.

Section 4

Uses a technology-neutral substantial-purpose test. It targets government-facing capability while excluding general-purpose cloud services and ordinary cameras unless integrated into a covered system.

Sections 5-6

Registration and impact assessment solve the inventory problem documented by GAO. They also mirror privacy-impact and system-notice concepts without assuming that the existing Privacy Act reaches every contractor platform.

Sections 7-8

Purpose limitation draws from the FCRA and DPPA. Legal-process parity prevents acquisition method from determining constitutional protection.

Section 9

Cross-jurisdiction controls address the core network effect: a sensor locally approved for one purpose can become available to a distant jurisdiction enforcing different laws.

Section 10

Recognizes private contributors without treating their consent as consent on behalf of passersby or as a substitute for government legal authority.

Sections 11-12

Auditability and corroboration are central operational safeguards. They convert vendor promises into enforceable obligations and preserve provenance for courts and oversight.

Section 13

Adapts FCRA dispute procedures and Privacy Act access principles to data that materially contributes to government action, while allowing delayed notice under judicial supervision.

Sections 14-15

Use public reporting, contract clauses, and federal grants to create scalable compliance. Federal procurement provides a direct constitutional basis for federal purchasing rules.

Sections 16-17

Combine public enforcement with a bounded private action. The draft avoids automatic liability for harmless technical mistakes while preserving meaningful redress for knowing or reckless violations.

Sections 18-19

Specify practices too central to leave solely to rulemaking and create an emergency path that is documented and reviewable rather than informal.

Sections 20-23

Delegate technical detail, preserve stronger state law, protect the remainder of the Act if one provision falls, and phase implementation.

9. Constitutional Authority and Litigation Risk

9.1 Commerce Clause

Covered providers operate in interstate data and technology markets, contract across state lines, and enable cross-jurisdiction searches. Congress has a strong basis to regulate the commercial providers directly. The legislative record should document interstate data flows, national customer networks, and the impossibility of confining the covered services to a single State.

9.2 Federal procurement and Spending Clause

Congress and the Executive possess broad authority to define the terms on which the Federal Government buys technology. Congress may also condition federal grants on clear, related, prospective requirements. Grant conditions should identify the affected programs and give recipients meaningful notice, thereby reducing anti-commandeering risk.

9.3 First Amendment

Providers may argue that data collection, database outputs, rankings, or customer disclosures are speech. The Act should be defended primarily as regulation of commercial conduct, government procurement, access control, and the operational use of surveillance systems. Disclosure provisions should be factual and reasonably related to preventing deception and protecting public accountability. Restrictions on identifying protected activity should be framed as limits on governmental investigative use, not viewpoint-based regulation of private expression.

9.4 Due Process and vagueness

Coverage definitions must be objective. The substantial-purpose test should be supported by listed indicators and a pre-enforcement advisory process. Civil penalties should require knowledge or recklessness for ambiguous boundary violations, while registration and corrective orders may operate under a lower standard.

9.5 Takings and compelled access

The Act does not appropriate vendor property for public use. It conditions participation in a regulated interstate and government market and requires records necessary for accountability. Contract termination and data portability clauses should be prospective and compensated through ordinary contracting.

9.6 Federalism and anti-commandeering

The direct provider rules regulate private interstate commerce. State and local agency duties should attach through valid federal statutes, federal preemption where necessary, and voluntary federal grant conditions. The Act should not simply command state legislatures to enact or administer a federal program.

9.7 Sovereign and qualified immunity

A private damages action against governmental entities requires careful drafting. Congress has stronger authority over federal agencies than over States. The model therefore emphasizes prospective relief, grant conditions, individual-capacity liability where existing law permits, and provider liability. Final legislative counsel should separately analyze abrogation authority for any damages remedy against States.

10. Alternatives Considered

Alternative	Strength	Why insufficient alone
Treat all covered vendors as state actors	Direct constitutional framing	Conflicts with narrow Supreme Court doctrine; fact-specific and overbroad
Amend only the Privacy Act	Uses established federal records framework	Does not adequately cover state/local users, private contributors, or shared vendor architecture
Amend only the Stored Communications Act	Addresses government-provider access	Coverage is tied to communications and existing provider categories; does not regulate sensors, ALPR, facial recognition, or audit architecture
FTC enforcement only	Flexible commercial enforcement	Case-by-case unfairness law lacks comprehensive public-law safeguards and government-user duties
Procurement rules only	Fast implementation for government contracts	Misses non-federal customers and can be changed administratively; weak individual remedies
Technology-specific bans	Simple and politically legible	Rapid obsolescence, loopholes, and inability to address convergence
Standalone Act plus conforming amendments	Unified, technology-neutral, enforceable	Requires substantial implementation and interagency coordination

11. Recommended Conforming Amendments

- Privacy Act: clarify that a contractor-operated covered system used substantially for a federal agency function is subject to system-of-records notice, access, amendment, and disclosure accounting to the extent records are under agency control.
- Stored Communications Act: add legal-process parity for purchased or licensed access to covered provider records that are materially equivalent to records obtainable under 18 U.S.C. § 2703.
- Federal Acquisition Regulation: create a mandatory clause for covered systems, including registration, audit logs, independent testing, incident reporting, subcontractor flow-down, and termination assistance.
- DOJ grant statutes and annual appropriations: condition specified technology grants on compliance and annual certification.
- FTC Act: expressly confirm Commission jurisdiction over covered providers, including common-carrier activities to the extent Congress chooses to close existing jurisdictional gaps.

12. Implementation Plan

Period	Action
0-6 months	Interagency implementation office; stakeholder hearings; interim provider inventory; preserve existing logs
6-18 months	Joint rulemaking; NIST audit and testing standards; draft FAR clause; pilot registry
18-24 months	Registration opens; federal solicitations use new clauses; agency user training
24-36 months	Full federal procurement compliance; grant conditions; first transparency reports
36 months onward	Independent audits; public evaluation; statutory review of coverage and remedies

13. Evaluation Metrics

- Percentage of covered providers registered and independently audited.
- Percentage of governmental queries containing complete purpose and legal-authority fields.
- Rate of unauthorized, anomalous, or suspended queries.
- Number and resolution time of correction requests.
- Frequency of coercive actions based on automated matches and proportion with documented corroboration.
- Cross-jurisdiction query volume and compliance with written agreements.
- Security incidents, log-integrity failures, and remedial actions.
- Public-safety outcomes reported with safeguards against unsupported causal claims.

14. Conclusion

The central legal mismatch is now clear. Constitutional doctrine asks whether a particular private actor is fairly attributable to the State and whether a particular government acquisition is a search. Modern surveillance markets operate at a different level: they create a standing, commercialized capability that can be queried by many agencies across time and jurisdiction.

The law should not wait until every vendor is judicially classified as a state actor. Nor should it prohibit technology merely because it can assist government. The appropriate response is a specialized statutory regime that recognizes the public consequences of the market while preserving legitimate investigation.

The Public Power Through Private Infrastructure Act supplies that regime. It treats government-facing surveillance infrastructure as a regulated category; uses familiar mechanisms from the FCRA, DPPA, Privacy Act, FTC Act, and federal procurement law; and requires safeguards proportional to persistence, aggregation, cross-jurisdiction reach, and coercive consequence.

Its organizing principle is narrow but consequential: private ownership should not create an accountability vacuum when the product being sold is durable public investigative power.

Authorities and References

Primary legal authorities and official government materials are listed first. Web addresses were verified during preparation. Pinpoint propositions in the report are supported by the cited authority; the proposed statutory language is original policy drafting.

1. U.S. CONST. amend. IV.

2. 42 U.S.C. § 1983.

3. 5 U.S.C. § 552a (Privacy Act of 1974), https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title5-section552a.

4. 15 U.S.C. § 45 (Federal Trade Commission Act § 5), https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title15-section45.

5. 15 U.S.C. § 1681 et seq. (Fair Credit Reporting Act), https://uscode.house.gov/view.xhtml?edition=prelim&req=granuleid:USC-prelim-title15-chapter41-subchapter3.

6. 15 U.S.C. § 1681b (permissible purposes), https://uscode.house.gov/view.xhtml?req=(title:15 section:1681b edition:prelim).

7. 15 U.S.C. § 1681i (disputed accuracy), https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid:USC-prelim-title15-section1681i.

8. 18 U.S.C. §§ 2701-2713 (Stored Communications Act), https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121.

9. 18 U.S.C. §§ 2721-2725 (Driver's Privacy Protection Act), https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter123.

10. California Civil Code §§ 1798.90.5-1798.90.55 (automated license plate recognition systems), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.90.5.

11. Federal Acquisition Regulation, 48 C.F.R. pts. 4, 42, 52, https://www.ecfr.gov/current/title-48/chapter-1.

12. 48 C.F.R. § 52.204-25 (prohibition on contracting for certain covered telecommunications equipment or services), https://www.ecfr.gov/current/title-48/chapter-1/subchapter-H/part-52/subpart-52.2/section-52.204-25.

13. United States v. Jones, 565 U.S. 400 (2012).

14. Riley v. California, 573 U.S. 373 (2014).

15. Carpenter v. United States, 585 U.S. 296 (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

16. Chatrie v. United States, No. 25-112 (U.S. June 29, 2026), https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf.

17. Lugar v. Edmondson Oil Co., 457 U.S. 922 (1982).

18. Blum v. Yaretsky, 457 U.S. 991 (1982).

19. Rendell-Baker v. Kohn, 457 U.S. 830 (1982).

20. Jackson v. Metropolitan Edison Co., 419 U.S. 345 (1974).

21. Brentwood Academy v. Tennessee Secondary School Athletic Ass'n, 531 U.S. 288 (2001).

22. Manhattan Community Access Corp. v. Halleck, 587 U.S. 802 (2019), https://www.law.cornell.edu/supremecourt/text/17-1702.

23. Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989).

24. United States v. Jacobsen, 466 U.S. 109 (1984).

25. Burrows v. Purchasing Power, LLC, 718 F.3d 1139 (9th Cir. 2013) (DPPA remedies and statutory construction context).

26. Reno v. Condon, 528 U.S. 141 (2000) (upholding DPPA as regulation of States as owners of databases and participants in interstate market).

27. South Dakota v. Dole, 483 U.S. 203 (1987) (Spending Clause conditions).

28. Murphy v. NCAA, 584 U.S. 453 (2018) (anti-commandeering).

29. Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks of Facial Recognition, GAO-21-518 (June 2021), https://www.gao.gov/products/gao-21-518.

30. Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections, GAO-22-106100 (June 2022), https://www.gao.gov/products/gao-22-106100.

31. Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data (Dec. 3, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers.

32. Federal Trade Commission, Gravy Analytics/Venntel final complaint and order materials, FTC Matter No. 2123035, https://www.ftc.gov/system/files/ftc_gov/pdf/212_3035_-_gravy_analytics_final_consent_package_without_signatures.pdf.

33. Federal Trade Commission, FTC Order Prohibits X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data.

34. U.S. Constitution Annotated, State Action Doctrine, https://constitution.congress.gov/browse/essay/amdt14-S1-8-1/ALDE_00000810/.

35. National Institute of Standards and Technology, Face Recognition Vendor Test program, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

36. Private Infrastructure, Public Power: A Problem Brief on Constitutional Values, Privatized Data Systems, Networked Surveillance, and the Shrinking Practical Space for Civic Agency (July 19, 2026) (project foundation document).