

Policy Brief on AI Video Surveillance Systems

Dan Jacobellis

Dept. of Electrical and Computer Engineering

The University of Texas at Austin

Austin, TX 78712, USA

danjacobellis@utexas.edu

Abstract—Networked camera systems that automatically identify vehicles and persons — license plate readers being the most widely deployed example — differ from human observation in that they record everyone, retain what they record, and permit the retrospective reconstruction of any individual’s movements. This memorandum first enumerates the rights of citizens that such systems implicate, organized into four categories: substantive privacy rights, including anonymity of movement in public and informational self-determination; political liberties, including freedom of association and freedom from chilling effects on protected expression; procedural and adjudicative rights, including individualized suspicion, confrontation of automated evidence, and access to exculpatory records; and structural or democratic rights, including public knowledge of the surveillance apparatus, equal protection in its deployment, and non-conscription of private infrastructure. It then translates these rights into the draft text of a proposed amendment to Article I of the Texas Constitution. The draft regulates the capabilities from which the identified injuries arise — retention, derivation, aggregation, and retrospective query — rather than particular technologies, and it is self-executing, with express provisions for exclusion, standing, waiver of immunity, and damages.

I. CITIZENS’ RIGHTS RELATED TO SURVEILLANCE

Automated camera networks, of which license plate reader systems are the most widely deployed example, implicate a set of rights that differ in origin and in the manner of their injury. Some are privacy rights in the strict sense; others are older political and procedural rights that surveillance erodes indirectly; still others concern the capacity of a self-governing public to supervise the surveillance apparatus itself. This section organizes the relevant rights into four categories: substantive privacy rights, political liberties, procedural and adjudicative rights, and structural or democratic rights. Legal protections such as retention limits, audit records, and oversight bodies are deliberately excluded from the enumeration: they are instruments for securing the rights described here rather than rights in themselves.

A. Substantive Privacy Rights

Anonymity of movement in public. The [Fourth Amendment](#) protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” [1], and since [Katz v. United States](#) its protections have extended to matters in which a person

holds a reasonable expectation of privacy [2]. In [United States v. Knotts](#), the Supreme Court held that a motorist has no reasonable expectation of privacy in individual movements on public roads, while expressly reserving judgment on “dragnet-type law enforcement practices” [3]. The subsequent cases addressing prolonged, automated location tracking have treated aggregation as the decisive fact. In [United States v. Jones](#), five concurring Justices concluded that long-term monitoring of a vehicle’s movements infringes expectations of privacy even though each individual movement is publicly observable [4]. In [Carpenter v. United States](#), the Court held that acquisition of historical cell-site location records is a search, emphasizing that such records are “detailed, encyclopedic, and effortlessly compiled” and that their retrospective character gives police access to information otherwise unknowable [5]. The Court had earlier recognized, in the freedom-of-information context, a cognate interest in the “practical obscurity” of information that is nominally public but costly to compile [6]. Courts have begun to apply this reasoning to camera networks specifically: the Supreme Judicial Court of Massachusetts held that a sufficiently extensive license plate reader network would constitute a search under the Fourth Amendment and the state constitution, though the four fixed cameras at issue fell short of that threshold [7], and the Fourth Circuit, sitting en banc, held that Baltimore’s aerial photographic surveillance program violated the Fourth Amendment because it enabled retrospective reconstruction of individuals’ movements [8]. The right at issue is accordingly not a right against being observed in public, which no authority supports, but a right against the systematic recording and retrospective reconstruction of one’s public movements.

The home and its curtilage. The home occupies a privileged position in the constitutional text and in the case law construing it. In [Kyllo v. United States](#), the Court held that the use of sense-enhancing technology to obtain information about the interior of a home that could not otherwise be obtained without physical intrusion is a search, at least where the technology is not in general public use [9], and [Florida v. Jardines](#) extended the home’s protection to its curtilage [10]. Camera networks implicate this right both directly, when fields of view encompass residential property, and inferentially: location records disclose visits to medical facilities, places of worship, and counsel, and thereby reveal what Justice Sotomayor described in [Jones](#) as a person’s “familial, political, professional, religious, and sexual associations” [4].

Informational privacy and self-determination. Warren and Brandeis grounded the common-law right to privacy in the individual's control over the disclosure of personal information [11], and Brandeis later characterized "the right to be let alone" as "the most comprehensive of rights and the right most valued by civilized men" [12]. The Supreme Court has recognized an individual interest in avoiding disclosure of personal matters [13], and Westin's influential account defines privacy as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others [14]. The German Federal Constitutional Court's census decision of 1983, which articulated a right of "informational self-determination," remains the most developed judicial statement of this principle [15]. In the American doctrine, the principal obstacle to such a right is the third-party doctrine of *Smith v. Maryland* [16]; *Carpenter* declined to extend that doctrine to comprehensive location records, reasoning that their disclosure to a third party is not meaningfully voluntary [5]. The sale or repurposing of surveillance data collected by either public or private camera systems falls squarely within this category.

B. Political Liberties

Freedom of association. In *NAACP v. Alabama ex rel. Patterson*, the Supreme Court recognized the "vital relationship between freedom to associate and privacy in one's associations," holding that compelled disclosure of an organization's membership would abridge the freedom itself, not merely expose members to reprisal [17]. A networked camera system is an instrument for reconstructing associations: it records which vehicles appear at a meeting place, which depart together, and which are later found at common addresses. The injury identified in *NAACP* does not depend on any subsequent prosecution; the disclosure of the association is itself the abridgment.

Anonymous expression and freedom from chilling effects. The *First Amendment* protects anonymous political expression; *McIntyre v. Ohio Elections Commission* described anonymity as "a shield from the tyranny of the majority" [18]. The distinctive injury of pervasive surveillance is prospective: the knowledge that attendance at a protest, a place of worship, or a political meeting will be recorded deters the protected conduct without any enforcement action. In *Laird v. Tatum* the Supreme Court confronted a claim of chilling arising from military surveillance of domestic political activity; although the Court found the plaintiffs' allegations of subjective chill insufficient for standing, the decision frames the continuing doctrinal question of when surveillance itself works a *First Amendment* injury [19]. The theoretical basis of the concern is older than the case law: Bentham designed the Panopticon precisely on the premise that the possibility of unobserved observation disciplines conduct [20], an analysis Foucault extended to modern institutions [21]. Solove's critique of the "nothing to hide" argument addresses the contention that such chilling concerns only the culpable [22].

C. Procedural and Adjudicative Rights

Individualized suspicion and particularity. The Warrant Clause requires that warrants issue only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" [1]. The clause is a direct response to the *general warrant* and the *writ of assistance*: *Entick v. Carrington* condemned general warrants at common law [23], James Otis's 1761 argument against the writs was described by John Adams as the moment "the child Independence was born" [24], and *Boyd v. United States* treated both authorities as fixing the meaning of the Fourth Amendment [25]. Indiscriminate collection inverts the principle of individualized suspicion: the population at large is recorded in advance so that any member of it may later be investigated. A database query that reconstructs a particular person's movements is, in substance, a general search conducted retrospectively, and the particularity requirement supplies the appropriate standard for it.

Confrontation of automated evidence. The *Sixth Amendment* guarantees the accused the right "to be confronted with the witnesses against him" [1]. *Crawford v. Washington* restored the requirement that testimonial statements be subject to cross-examination [26], and *Melendez-Diaz v. Massachusetts* applied it to forensic laboratory reports, rejecting the contention that scientific evidence is immune from confrontation by virtue of its ostensible neutrality [27]. Automated plate reads and vehicle identifications are machine-generated accusations with nontrivial error rates; the confrontation principle requires that a defendant be able to examine the provenance, error characteristics, and operating conditions of the system whose output is offered against him.

Access to exculpatory evidence. *Brady v. Maryland* obliges the prosecution to disclose evidence favorable to the accused [28], and the *Compulsory Process Clause* secures the defendant's right to obtain evidence in his favor [1]. When the government's evidentiary environment is a camera network, these guarantees entail a right of access to the same records for exculpatory purposes. A regime in which investigators may query a plate database freely while a citizen cannot obtain records pertinent to his own defense is difficult to reconcile with these principles.

Notice and remedy. *Marbury v. Madison* states the premise: "[t]he very essence of civil liberty certainly consists in the right of every individual to claim the protection of the laws, whenever he receives an injury" [29]. Where surveillance-derived action injures a person erroneously or unlawfully, *due process* [1] requires notice adequate to discover the error and a forum in which to correct it, and *Mapp v. Ohio* supplies the traditional remedy for evidence unlawfully obtained [30]. Rights in this category are parasitic on the others in a precise sense: without notice and remedy, the preceding guarantees cannot be enforced by the persons they protect.

D. Structural and Democratic Rights

Public knowledge of the surveillance apparatus. A surveillance system whose existence or scope is concealed from the public is insulated from the democratic processes that are

supposed to authorize it. The First Amendment’s press and petition guarantees [1] presuppose the public’s capacity to learn of and contest government conduct, and the courts of appeals have recognized a First Amendment right to record police officers performing their duties in public, subject to reasonable time, place, and manner restrictions [31], [32]. The asymmetry runs in a definite direction: the surveillance powers of the state are legitimate only insofar as they are visible to the public that authorizes them.

Equal protection in deployment and use. Camera placement and query practices are discretionary, and discretion concentrates. *Yick Wo v. Hopkins* establishes that a facially neutral system administered “with an evil eye and an unequal hand” violates the [Equal Protection Clause](#) [1], [33]. Where collection density or search frequency differs materially across communities without justification, the surveillance regime itself becomes an instrument of selective enforcement.

Non-conscription of private infrastructure. No controlling authority yet addresses whether the state may enroll privately owned cameras into a government-searchable network without the owner’s knowing consent. Structural analogies exist: the anti-commandeering principle of *Printz v. United States* forbids the federal government to conscript state officers into administering federal programs [34], and the [Third Amendment](#)’s prohibition on the quartering of soldiers reflects a broader principle against compelled private participation in state operations [1]. *Carpenter*’s refusal to treat records held by third parties as automatically available to the government [5] supplies partial protection on the data side. Two distinct interests require separation: the owner’s interest in not having his property deputized, and the interests of third parties recorded by that property, which the owner’s consent cannot waive.

II. A SURVEILLANCE BILL OF RIGHTS FOR TEXAS

This section translates the rights enumerated in [Section I](#) into the draft text of a constitutional amendment. The [Texas Constitution](#) is amenable to such an addition: amendments are proposed by a two-thirds vote of each house and ratified by a majority of the voters [35], Article I already contains a search-and-seizure guarantee parallel to the Fourth Amendment [35], and state constitutions may extend protections beyond the federal floor, as the Massachusetts court did in applying its own Declaration of Rights to license plate readers [7]. The draft is written so that a court asked whether a statute, program, or individual act violates it can answer by applying familiar judicial materials: defined terms, warrant requirements, bright-line periods, and express remedies, rather than open-ended balancing.

A. Drafting Principles

Five judgments, each drawn from the analysis of [Section I](#), govern the draft.

Rights are defined at the level of capability. The lesson of *Carpenter* and the concurrences in *Jones* is that the injury of automated surveillance arises from aggregation: no single observation infringes any right, while the accumulated

record infringes several [4], [5]. A provision that regulates individual observations therefore misdescribes the harm. The draft instead regulates retention, derivation, aggregation, and query — the operations that convert innocuous observations into a reconstructable history.

Derived representations are data. Modern systems extract from each frame a machine-readable abstraction — a biometric template, a vehicle signature, a feature encoding — that supports search and re-identification after the original recording is destroyed. A guarantee that reaches only recordings would be satisfied by deleting video while retaining everything of investigative value. The draft’s definition of surveillance data therefore includes every representation derived from it.

Technology-neutral terms age better than technological ones. *Kyllo* conditioned the home’s protection on whether a sense-enhancing technology is “in general public use,” a test whose protective force diminishes as technology diffuses [9]. The draft defines its objects functionally, by what a system does, so that its coverage does not erode with the state of the art.

Architecture is the strongest form of collection limitation.

Where alert matching is performed on or near the sensing device, information about persons matching no predicate need never be transmitted or stored, and the protection does not depend on the future good behavior of a database custodian. The draft accordingly prefers, where feasible, that non-matching data never leave the device.

Remedies must be express. The Supreme Court of Texas has held that the state Bill of Rights implies no private action for damages, leaving only equitable relief [36], and the state’s exclusionary rule is statutory rather than constitutional [37]. A surveillance amendment that is silent on enforcement would therefore protect little. The draft is self-executing, constitutionalizes exclusion, waives immunity, and confers standing on those whose data is unlawfully retained or queried.

The draft is deliberately narrower than a general privacy code. In keeping with the principle that coercive regulation is justified by the prevention of harm to others [38], it restrains only government conduct that threatens the rights enumerated in [Section I](#); private recording is untouched except at the point where its products enter government hands. It also differs in kind from the [Bill of Rights of 1791](#), which restrained named practices of eighteenth-century state power — general warrants, quartering, compelled testimony — under conditions in which observation was necessarily ephemeral, selective, and costly. The provisions below regulate what could not then exist: mechanical memory, automated inference, and retrospective search.

B. Text of the Proposed Amendment

Article I, Section __. RIGHTS OF THE PEOPLE RESPECTING AUTOMATED SURVEILLANCE.

(a) Definitions. In this section: (1) “Automated surveillance system” means a device, or coordinated network of devices, that by algorithmic or machine processing captures, extracts, indexes, or classifies information concerning identifiable persons,

vehicles, or effects in places accessible to the public, without regard to the sensing or processing technology employed.

(2) “Surveillance data” means information captured by an automated surveillance system, together with every representation derived from that information, including biometric templates, vehicle and gait signatures, feature encodings, and other machine-readable abstractions, whether or not the original recording persists. (3) “Retrospective query” means an interrogation of surveillance data undertaken to identify, locate, or reconstruct the past movements or associations of an identifiable person or vehicle. (4) “Government” means this state, its political subdivisions, and every officer, agent, and contractor acting on behalf of either.

(b) Collection and retention. Government shall not retain surveillance data except: (1) data that at the time of capture matches an entry on an alert list authorized under subsection (c); (2) data preserved upon sworn application identifying a specific offense and a particular place and interval of time; and (3) data held transiently for the purpose of matching, which shall be destroyed within seventy-two hours of capture. The legislature may shorten, but not lengthen, the period in subdivision (3). Destruction under this section includes all derived representations. Where technically feasible, matching shall be performed on or near the sensing device, so that data matching no authorized entry is neither transmitted nor centrally stored.

(c) Alert lists. Each entry on an alert list shall identify a particular person, vehicle, or effect; shall rest on an individualized and articulable basis recorded in the audit record; and shall expire, absent renewal on the same conditions, within a period fixed by general law.

(d) Retrospective queries. No retrospective query shall be conducted except under a warrant issued upon probable cause, particularly describing the person or vehicle sought, the interval of time, and the offense under investigation. The interval searched shall be no broader than the showing of cause supports.

(e) Protected activity. Surveillance data shall not be collected for the purpose of, nor queried for the purpose of, identifying any person’s participation in worship, assembly, expression, petition, the practice of journalism, or the seeking of medical care or legal counsel, except under a warrant that particularly states the grounds on which the protected character of the activity does not bar the search.

(f) Biometric identification. Government shall not perform generalized biometric comparison of surveillance data against the population at large. Particularized biometric comparison is a retrospective query within subsection (d).

(g) Sale and acquisition. Surveillance data shall not be sold or exchanged for consideration. Government shall not acquire from any person, by purchase, gift, exchange, or standing arrangement, surveillance data or its substantial equivalent that this section forbids government to collect or retain; data so acquired is subject to every limitation of this section.

(h) Aggregation and sharing. Surveillance data collected in this state may be queried only in conformity with this section,

whatever the identity or jurisdiction of the party querying. Government shall not enroll such data in any network or federated system that permits queries not conforming to this section.

(i) Private systems. Government shall not compel, condition any benefit upon, or systematically solicit the enrollment of privately owned sensing devices in any surveillance network accessible to government. Standing or programmatic access to privately held recordings requires the authorization described in subsection (d); the consent of an owner does not diminish the rights of any other person whose information a recording contains. Nothing in this subsection prevents an owner from voluntarily providing particular recordings pertinent to a specific incident.

(j) Transparency, audit, and confrontation. The existence, coverage, capabilities, and declared purpose of every government automated surveillance system are public information. Every query of surveillance data shall generate a permanent audit record identifying the querying party, the subject, the time, and the legal basis of the query, and aggregate statistics of such records shall be published at least annually. A person against whom surveillance data or its products are offered in any proceeding is entitled to examine the design, error characteristics, and conditions of operation of the system that produced them, and the audit records of the queries concerned.

(k) Exculpatory access. A person accused of an offense, or reasonably anticipating accusation, may apply to a court of competent jurisdiction for the preservation of and access to surveillance data upon a showing that it may tend to exculpate. The application shall be governed by terms no less favorable than those governing the state’s own access to the same data.

(l) Enforcement. This section is self-executing. Evidence obtained in violation of this section, and evidence derived from it, shall not be admitted against the person whose rights were violated in any proceeding. A person whose surveillance data has been retained or queried in violation of this section has standing to sue without further showing of injury. Sovereign and governmental immunity to suit and liability are waived for claims under this section, and a prevailing claimant may recover actual damages, equitable relief, and reasonable attorney’s fees. The legislature may provide protections and remedies greater than, but not less than, those this section provides.

C. Relation to the Enumerated Rights

Each provision answers an injury identified in Section I. Subsections (b) through (d) secure anonymity of movement at the level of capability at which *Carpenter* and *Jones* locate the harm, and subsection (b)(2) preserves the legitimate investigative uses — the stolen vehicle, the identified suspect, the incident at a known place and time — that motivate such systems in the first place [4], [5]. Subsection (e) protects the associational and expressive interests of *NAACP v. Alabama* and *McIntyre* against both collection and query [17], [18]. Subsections (g) and (h) address informational self-determination and close the acquisition and federation routes by which local

limits are otherwise circumvented. Subsection (i) states the non-conscription principle for which *Printz* supplies the structural analogy [34]. Subsection (j) enforces the public’s knowledge of the apparatus and extends the confrontation principle of *Melendez-Diaz* to machine-generated accusations [27]; subsection (k) gives constitutional footing to the access interest illustrated by *Brady* [28]. Subsection (l) supplies what *Marbury* identifies as the essence of civil liberty and what *Bouillion* shows the Texas Bill of Rights otherwise lacks [29], [36].

[38] J. S. Mill, *On Liberty*. London: John W. Parker and Son, 1859.

REFERENCES

- [1] “Constitution of the United States,” 1791, Amendments I, III, IV, V, VI, and XIV are cited in the text.
- [2] “Katz v. United States, 389 U.S. 347,” 1967, U.S. Supreme Court.
- [3] “United States v. Knotts, 460 U.S. 276,” 1983, U.S. Supreme Court.
- [4] “United States v. Jones, 565 U.S. 400,” 2012, U.S. Supreme Court.
- [5] “Carpenter v. United States, 585 U.S. 296,” 2018, U.S. Supreme Court.
- [6] “U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749,” 1989, U.S. Supreme Court.
- [7] “Commonwealth v. McCarthy, 484 Mass. 493, 142 N.E.3d 1090,” 2020, Supreme Judicial Court of Massachusetts.
- [8] “Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330,” 2021, U.S. Court of Appeals for the Fourth Circuit, en banc.
- [9] “Kyllo v. United States, 533 U.S. 27,” 2001, U.S. Supreme Court.
- [10] “Florida v. Jardines, 569 U.S. 1,” 2013, U.S. Supreme Court.
- [11] S. D. Warren and L. D. Brandeis, “The right to privacy,” *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, 1890.
- [12] “Olmstead v. United States, 277 U.S. 438,” 1928, U.S. Supreme Court; Brandeis, J., dissenting.
- [13] “Whalen v. Roe, 429 U.S. 589,” 1977, U.S. Supreme Court.
- [14] A. F. Westin, *Privacy and Freedom*. New York: Atheneum, 1967.
- [15] “Volkszählungsurteil (Census Act decision), BVerfGE 65, 1,” 1983, German Federal Constitutional Court.
- [16] “Smith v. Maryland, 442 U.S. 735,” 1979, U.S. Supreme Court.
- [17] “NAACP v. Alabama ex rel. Patterson, 357 U.S. 449,” 1958, U.S. Supreme Court.
- [18] “McIntyre v. Ohio Elections Commission, 514 U.S. 334,” 1995, U.S. Supreme Court.
- [19] “Laird v. Tatum, 408 U.S. 1,” 1972, U.S. Supreme Court.
- [20] J. Bentham, *Panopticon; or, The Inspection-House*. London: T. Payne, 1791.
- [21] M. Foucault, *Discipline and Punish: The Birth of the Prison*. New York: Pantheon Books, 1977, Translated by Alan Sheridan; original French edition 1975.
- [22] D. J. Solove, “‘I’ve got nothing to hide’ and other misunderstandings of privacy,” *San Diego Law Review*, vol. 44, pp. 745–772, 2007.
- [23] “Entick v. Carrington, 19 How. St. Tr. 1029, 95 Eng. Rep. 807,” 1765, Court of Common Pleas, England.
- [24] J. Adams, “Letter to William Tudor, March 29, 1817,” 1817, Recounting James Otis’s 1761 argument against the writs of assistance.
- [25] “Boyd v. United States, 116 U.S. 616,” 1886, U.S. Supreme Court.
- [26] “Crawford v. Washington, 541 U.S. 36,” 2004, U.S. Supreme Court.
- [27] “Melendez-Diaz v. Massachusetts, 557 U.S. 305,” 2009, U.S. Supreme Court.
- [28] “Brady v. Maryland, 373 U.S. 83,” 1963, U.S. Supreme Court.
- [29] “Marbury v. Madison, 5 U.S. (1 Cranch) 137,” 1803, U.S. Supreme Court.
- [30] “Mapp v. Ohio, 367 U.S. 643,” 1961, U.S. Supreme Court.
- [31] “Glik v. Cunniffe, 655 F.3d 78,” 2011, U.S. Court of Appeals for the First Circuit.
- [32] “Turner v. Driver, 848 F.3d 678,” 2017, U.S. Court of Appeals for the Fifth Circuit.
- [33] “Yick Wo v. Hopkins, 118 U.S. 356,” 1886, U.S. Supreme Court.
- [34] “Printz v. United States, 521 U.S. 898,” 1997, U.S. Supreme Court.
- [35] “Constitution of the State of Texas,” 1876, Article I, Section 9 (searches and seizures) and Article XVII, Section 1 (amendment procedure) are cited in the text.
- [36] “City of Beaumont v. Bouillion, 896 S.W.2d 143,” 1995, Supreme Court of Texas.
- [37] “Texas Code of Criminal Procedure, Article 38.23,” 1965, Statutory exclusionary rule.