

Already Illegal:

Flock Safety and the Six Bodies of Existing Law Nobody Is Applying

Travis Gilly* 🦋 August 2026 (v2)

Abstract

Automated license plate reader networks are debated as a privacy problem awaiting a privacy statute. That debate has obscured a simpler fact: at least six bodies of existing law already reach the conduct, and none of them is a privacy statute. Antidiscrimination law reaches the procurement decision, because a municipality that closes its own mobility program to a disability-defined class through a facially neutral administrative choice violates Title II and Section 504. State criminal surveillance law reaches the conduct, because observing a person in a private place without the consent of all persons observed is a felony in Georgia and in most states. Consumer protection law reaches the vendor, on a deception theory and on an unfairness theory grounded in documented security failure. Contract and delegated authority reach the access, because a municipality cannot license to a vendor a use that the camera owner was expressly told would not occur. Computer crime law reaches the intruder but, after *Van Buren v. United States*, not the credentialed insider, and that hole is the one real gap. National security data law reaches the location data itself, because the executive branch has already found by regulation that precise geolocation inside 736 enumerated areas is government-related data regardless of volume. This Article also reports an original empirical result bearing on the last of those. Joining the coordinates the Attorney General published for all 736 areas against 23,946 mapped readers, the author finds readers inside 74 enumerated areas, 504 of them within tightly drawn boundaries, against 11,992 within a ten kilometer approach. The densest is a 2.14 square kilometer rectangle enclosing the Pentagon, which holds eleven readers positioned on the roads in and out. The Article assembles the six bodies, identifies the statute the public reaches for and why it fails, and closes on the substitution the enacted threat model has not performed: what the assembled system does when the tracked vehicle belongs to a sitting legislator and the credentials belong to someone who can be bought.

Keywords: automated license plate readers; mass surveillance; disparate impact; methods of administration; meaningful access; unlawful eavesdropping and surveillance; continental geofence; subscription surveillance; *Van Buren v. United States*; paranoia-spectrum conditions; law enforcement insider threat; government-related data.

*Travis Gilly is Founder and Executive Director of the Real Safety AI Foundation. ORCID: 0009-0007-2954-6313. Correspondence: t.gilly@ai-literacy-labs.org. The author discloses the use of speech-to-text software (Wispr Flow) and Anthropic's Claude as assistive technology for a diagnosed neurodevelopmental condition. All legal analysis, case synthesis, theoretical framing, doctrinal arguments, and conclusions are solely the author's own.

Contents

I	Introduction	4
II	The System	5
	A Architecture and Scale	5
	B The Hotlist, and the Move from Record to Real Time.	6
	C The Security Posture	7
	D Federal Access, and What the Vendor Said About It.	8
III	The Statute Everyone Reaches For, and Why It Fails	9
	A <i>The Objection: “Including but Not Limited To”</i>	10
IV	Antidiscrimination Law Reaches the Procurement.	11
	A The Program Is Public Mobility	11
	B Campuses and School Districts.	12
	C <i>Choate</i> , and the Two Regulatory Vocabularies	12
	D The Reality-Testing Mechanism	13
	E Three Objections	14
	F <i>Sandoval, Payan</i> , and the Administrative Route	15
V	Criminal Surveillance Law Reaches the Conduct	16
	A The Georgia Statute	16
	B The Contested Element	17
	C The Exceptions, and the Circularity in the Owner Exception.	17
	D Civil Consequences	18
	E <i>The Real Obstacle Is Not Doctrinal</i>	19
VI	Consumer Protection Law Reaches the Vendor	19
	A <i>The Authority, and That It Covers Security</i>	19
	B <i>Deception</i>	20
	C <i>Unfairness</i>	20
	D <i>The Countervailing Benefits Question</i>	21
	E <i>Two Objections</i>	22
VII	Contract and Delegated Authority Reach the Access	23
	A <i>The Pattern</i>	23
	B <i>A Municipality Cannot License What It Never Held</i>	24
	C <i>Apparent Authority Does Not Rescue the Vendor</i>	24
	D <i>And the Institution Could Not Have Consented for the Occupants Anyway</i>	25
	E <i>Remedies, and the Problem That Precedes Them</i>	26
VIII	Computer Crime Law, and the One Real Gap	26
	A The Intruder	26
	B The Insider, and <i>Van Buren</i>	27
	C The Insider Is Not Hypothetical	28

IX	National Security Data Law Reaches the Location Data	29
A	The Rule	29
B	The Continental Geofence	30
C	The Empirical Question, Answered.	31
D	One Zone	32
E	The Admission	34
X	Conclusion: The Substitution	35

I. Introduction

The public argument about automated license plate reader networks has settled into a single shape. Advocates describe a surveillance apparatus of unprecedented reach. Legislators respond by drafting privacy bills. Vendors respond that the bills would impede public safety. The argument proceeds as though the conduct were presently lawful and the only question were whether to make it unlawful going forward.

That premise is wrong, and this Article is about how wrong it is.

At least six distinct bodies of enacted law already reach the deployment, the operation, or the data of these networks. None of them is a privacy statute. They are, in order of the argument below, federal disability antidiscrimination law,¹ state criminal surveillance law,² federal consumer protection law,³ the ordinary law of contract and delegated authority, federal computer crime law,⁴ and the national security regulation of sensitive location data.⁵ Each reaches a different actor and a different act. Together they cover nearly the whole of what the public objects to.

The point is not that a new privacy statute would be unwelcome. The point is that a decade of enforcement is available now, under law already on the books, to anyone willing to read past the word privacy.

Part II describes the system as its manufacturer describes it, because the capability at issue is not inferred from critics but marketed by the vendor. Part III takes up the statute that the public and the press reach for first, the Children's Online Privacy Protection Act, and explains why it fails, since a clear account of the failure is what makes the rest of the argument legible. Parts IV through IX assemble the six bodies of law that do reach. Part IX also reports an original

1. 42 U.S.C. § 12132; 29 U.S.C. § 794(a).

2. GA. CODE ANN. § 16-11-62(2) is the vehicle used here; every state criminalizes some form of nonconsensual observation.

3. 15 U.S.C. § 45(a)(1), (n).

4. 18 U.S.C. § 1030(a)(2)(C).

5. 28 C.F.R. pt. 202.

empirical result, joining the coordinates the Attorney General published for all 736 enumerated areas against 23,946 mapped readers. Part X performs the substitution that no legislature appears to have performed.

II. The System

A. Architecture and Scale

Flock Safety is the dominant vendor of municipal automated license plate reader networks in the United States. Its cameras photograph passing vehicles continuously, resolve the plate by optical character recognition, and transmit the record with a timestamp and a fixed camera location to a cloud platform its customers reach through a browser and a mobile application.⁶ Agency proposals executed with municipalities describe the same architecture in contract language, including a nationwide lookup across every camera opted into the vendor's network and a proprietary vehicle identification capability that operates on make, color, and distinguishing features when a plate is not legible.⁷ The vendor states that the platform connects more than 4,800 agencies.⁸

The scholarly literature on these systems has identified their defining institutional property as function creep, arising because the systems operate below the threshold of public attention and are configured incrementally to user-specific demands rather than by design at the outset.⁹ That property is the through line of this Article. Each Part below concerns a use the purchasing public was not told about.

6. Flock Safety, *Flock Safety Platform*, <https://www.flocksafety.com/products/flock-safety-platform> (last visited Aug. 9, 2026) (describing license plate recognition, alerts, and cross-jurisdictional search on a single platform).

7. Flock Grp. Inc., *Proposal to Lafayette, Ind. Police Dep't* 1–3, <https://www.lafayette.in.gov/AgendaCenter/ViewFile/Item/19567?fileID=61909> (last visited Aug. 9, 2026) [hereinafter *Lafayette Proposal*] (defining “Hotlist” and describing nationwide network lookup and Vehicle Fingerprint search).

8. Flock Safety, *extisupra* note 6.

9. Gabriel Pereira & Christoph Raetzsch, *From Banal Surveillance to Function Creep: Automated License Plate Recognition (ALPR) in Denmark*, 20 SURVEILLANCE & SOC'Y 265 (2022).

Two features of that architecture matter for every Part that follows. First, the record is not local. A plate photographed in one municipality is searchable by agencies in other states through the shared network, so the analytically relevant unit is not the camera or the city but the network.¹⁰ Second, the record is retained. The system is a continuously updated archive of vehicle movement rather than a set of momentary observations.

B. The Hotlist, and the Move from Record to Real Time

The capability that distinguishes this system from a conventional camera is the hotlist. A hotlist is a list of plates against which every passing vehicle is checked. Some entries derive from the National Crime Information Center and carry a defined source. The vendor also permits an agency to build its own list, described in adopting agencies' own policies as a permission-based feature allowing users to create alerts for vehicles that would not otherwise alert through traditional hotlist sources.¹¹ No judicial officer reviews a custom entry. Nothing in the described mechanism causes an entry to expire.

The alert is not a report generated after the fact. The vendor's mobile application advertises real-time hotlist alerts delivered with images of the vehicle and its plate, filtered by a radius the officer selects, available on a phone or a wrist-worn device.¹² Integration partners describe hotlist notifications flowing into real-time crime center environments used by analysts and command staff.¹³

The vendor's own promotional material assembles these pieces into the sequence that matters here. An operator identifies a plate, adds it to a hotlist, the readers flag the vehicle,

10. extitLafayette Proposal, extitsupra note 7, at 2 (describing lookup "on all cameras opted in to the nationwide Flock network").

11. See DeFlock, *Flock Hotlists: How the Cameras Flag Drivers Automatically*, <https://deflockilm.org/flock-hotlists-pattern-flags/> (last visited Aug. 9, 2026) (quoting adopting agencies' policies and reporting that no judicial officer reviews a custom entry and that entries do not expire).

12. Flock Safety, *Flock Safety* (mobile application description), <https://apps.apple.com/us/app/flock-safety/id1667653638> (last visited Aug. 9, 2026) ("Real-Time Hot List Alerts," "Notifications by Radius," and license plate lookup).

13. Coreforce, *Flock Safety and Coreforce Announce Integration Partnership* (Jan. 7, 2026), <https://www.coreforcetech.com/resources/flock-safety-and-coreforce-announce-integration-partnership-to-enhance-real> (last visited Aug. 9, 2026).

officers receive updates on its movements, and units coordinate to converge on it.¹⁴ That sequence is the product. It is demonstrated, not alleged.

A custom hotlist entry is therefore something more than a query. A query answers where a vehicle has been. An entry is a standing instruction to report where the vehicle is, from now until someone removes it. This Article uses *subscription surveillance* for that distinction, because the legal analysis in Parts VIII and X turns on it: the marginal cost of continuing surveillance, once an entry exists, is zero.

C. The Security Posture

Independent security research has established that the network’s perimeter is not what its customers were led to believe. In December 2025, journalists located more than sixty production cameras streaming live video to the open internet without authentication or encryption, with archived footage viewable in a browser.¹⁵ In January 2026, a security researcher reported finding sixty-seven live camera feeds and debug web interfaces exposed without authentication.¹⁶

Researchers further demonstrated that a button sequence on a camera’s exposed rear panel opens a diagnostic wireless access point protected by a default password, from which root access follows through a standard developer tool in under thirty seconds.¹⁷ The cameras are mounted on public poles.

14. Flock Safety, *In Critical Moments, Every Second Shapes the Outcome*, <https://www.flocksafety.com/video/real-time-policing-in-action> (last visited Aug. 9, 2026) (describing plate identification, hotlist addition, flagging by readers, movement updates to officers, and coordinated convergence).

15. See Jaron Schneider, *Big Brother Left the Door Open: Flock’s AI Surveillance Cameras Exposed to the Internet*, PETAPIXEL (Dec. 29, 2025), <https://petapixel.com/2025/12/29/big-brother-left-the-door-open-flocks-ai-surveillance-cameras-exposed-to-the-internet/> (last visited Aug. 9, 2026) (reporting the exposure and the vendor’s characterization of it as a limited misconfiguration rather than a compromise).

16. Jon Gaines, *Finding 67 Flock Safety Live PTZ Camera/LPR Feeds and Debug Web Interfaces Accidentally Exposed Without Authentication to the Internet*, GAINSEC (Jan. 9, 2026), <https://gainsec.com/2026/01/09/bird-hunting-season-finding-67-live-camera-feeds-and-debug-web-interfaces-accidentally-exposed-by-flock/> (last visited Aug. 9, 2026).

17. See *Flock Safety’s Camera Network Is Not Secure*, GADGET REV., <https://www.gadgetreview.com/flock-safety-s-camera-network-is-not-secure-how-physical-hotspot-sequences-allow-anyone-to-hijack-flock> (last visited Aug. 9, 2026) (reporting the demonstration by researchers Jon Gaines and Benn Jordan). The vendor’s response, that exploitation requires physical access and knowledge of internal hardware, is addressed *infra* Part VI.

Access to the platform is likewise weaker than its function implies. A congressional letter to the Federal Trade Commission documented the absence of any mandatory multifactor authentication requirement for law enforcement customers, thirty-five customer accounts with credentials stolen, and vendor logins offered for sale on Russian cybercrime forums.¹⁸

D. Federal Access, and What the Vendor Said About It

The vendor publicly maintains that it has no contract with United States Immigration and Customs Enforcement.¹⁹ On the same page it discloses a series of federal pilot projects, including a Customs and Border Protection pilot running from May 9 to August 24, 2025, and a Homeland Security Investigations pilot running from March 3 to May 1, 2025.²⁰

Three access paths are documented in the public record. Local officers ran more than four thousand immigration-related lookups on behalf of federal agents between June 2024 and May 2025, including in jurisdictions whose own law forbade it.²¹ A university human rights center found apparent back door federal access to at least ten Washington agencies that had never authorized it.²² An audit by the Illinois Secretary of State concluded that the resulting sharing violated Illinois law.²³

The vendor's chief executive had told the press that federal data sharing was not an issue because the company held no federal contracts, a representation the company was later required

18. *See Flock Safety Cameras Exposed*, STATE OF SURVEILLANCE (Jan. 25, 2026), <https://stateofsurveillance.org/news/flock-safety-cameras-exposed-no-password-2026/> (last visited Aug. 9, 2026) (summarizing the November 3, 2025 letter from Senator Ron Wyden and Representative Raja Krishnamoorthi to the Chair of the Federal Trade Commission).

19. Flock Safety, *Does Flock Share Data With ICE?*, <https://www.flocksafety.com/blog/does-flock-share-data-with-ice> (last visited Aug. 9, 2026).

20. *Id.*

21. *See* Jason Koebler, *Illinois Cops Gave ICE Access to More Than 5,000 Surveillance Cameras Nationwide*, 404 MEDIA (May 27, 2025), <https://www.yahoo.com/news/illinois-cops-gave-ice-access-171603853.html> (last visited Aug. 9, 2026).

22. Univ. of Wash. Ctr. for Human Rights, *LEAVING THE DOOR WIDE OPEN: FLOCK SURVEILLANCE SYSTEMS EXPOSE WASHINGTON DATA TO IMMIGRATION ENFORCEMENT* (Oct. 21, 2025), <https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/> (last visited Aug. 9, 2026).

23. Press Release, Ill. Sec'y of State, *Giannoulis' Audit Finds License Plate Reader Company in Violation of State Law* (Aug. 25, 2025), <https://www.ilsos.gov/news/2025/august-25-2025-giannoulis-audit-finds-license-plate-reader-company-in-violation-of-state-law.html> (last visited Aug. 9, 2026).

to correct.²⁴ His statement afterward was that the company had communicated poorly.²⁵ That sequence matters to Part VI, where the representations themselves become the violation.

III. The Statute Everyone Reaches For, and Why It Fails

When children appear in the frame of a surveillance story, the reflex is to reach for the Children’s Online Privacy Protection Act. The reflex is understandable and it is wrong, and understanding why is the cleanest way to see what the statute is.

COPPA prohibits an operator of a website or online service directed to children, or an operator with actual knowledge that it is collecting personal information from a child, from doing so without notice to parents and verifiable parental consent.²⁶ The Commission’s amended Rule now includes within personal information a biometric identifier that can be used for automated or semi-automated recognition, and has since 2013 included a photograph, video, or audio file containing a child’s image or voice.²⁷ Full compliance with the amended Rule has been required since April 22, 2026.²⁸

Two definitional walls stop the statute at the curb.

The first is the phrase “collected online.” Personal information under the Rule is individually identifiable information about an individual collected online, and collection means the gathering of personal information from a child by any means, illustrated by three examples: requesting or prompting a child to submit information online, enabling a child to make information publicly available, and passive tracking of a child online.²⁹ A camera

24. ACLU, *Flock Safety Credibility Lost as It Repeatedly Lies to City Councils, Police Departments, and Public Across the Country* (July 2, 2026), <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flock-safety-credibility-lost-as-it-repeatedly-lies-to-city-councils-police-depa> (last visited Aug. 9, 2026).

25. *Flock Safety License Plate Camera Company Stops Cooperating with Federal Agencies over Investigation Concerns*, CBS CHICAGO (Aug. 26, 2025), <https://www.cbsnews.com/chicago/news/flock-safety-license-plate-company-federal-agencies-cooperation/> (last visited Aug. 9, 2026).

26. 15 U.S.C. § 6502(a)(1), (b)(1)(A).

27. 16 C.F.R. § 312.2 (2026) (defining “personal information”).

28. Children’s Online Privacy Protection Rule, 90 Fed. Reg. 16918 (Apr. 22, 2025) (final rule).

29. 16 C.F.R. § 312.2 (defining “collects or collection” and “personal information”). The illustrative list is introduced by “including but not limited to,” so it does not by its terms foreclose other means.

photographing a body in physical space gathers information about a child rather than from one, and no enforcement action has extended the definition to ambient third-party capture.

The second is the phrase “directed to children.” The Rule’s audience-composition inquiry weighs subject matter and visual content, but it also weighs the age of users on comparable services, and a service is deemed directed to children when it collects from users of another child-directed service.³⁰ The users of an automated license plate reader network are police agencies. A camera pointed at a playground is aimed at children; it is not directed to them in the Rule’s sense.

A. The Objection: “Including but Not Limited To”

The strongest reply is textual. Collection is defined as the gathering of personal information from a child by any means, and the three examples are introduced by “including but not limited to.” A non-exhaustive list does not by its terms exclude ambient capture, and the amended Rule’s inclusion of biometric identifiers shows the Commission is willing to reach data a child never typed.

Two answers hold the line. First, the chapeau still requires gathering from a child, and every enumerated example describes a child as the source of the transfer, which is the natural reading of a list that supplies the meaning of the general phrase preceding it. Second, and independently, the “collected online” limitation in the definition of personal information is a separate requirement that the non-exhaustive collection list does not touch. An operator seeking to enforce the Rule against a physical camera network must satisfy both, and no enforcement action has done so.

There is a further practical answer that matters more than either. Even if the definitional argument succeeded, the remedy COPPA supplies is notice and verifiable parental consent. Applied to a camera on a public pole, that remedy is not merely difficult; it has no addressee.

30. *Id.* (defining “Web site or online service directed to children”).

There is no moment at which a parent could be asked. A statute whose sole remedial mechanism cannot be performed is not a statute that reaches the conduct.

The failure is structural, and it is instructive. COPPA is not a privacy right. It is a transactional gate enforced through the Commission's unfair and deceptive practices authority, conditioning collection on prior notice and consent and restricting onward disclosure.³¹ A gate requires a transaction to stand in front of. Ambient capture supplies none. The very feature that makes these networks objectionable, that a person need do nothing at all to be recorded, is the feature that places them outside the statute the public instinctively invokes.

That is the clarifying lesson of Part III, and the rest of this Article follows from it. Stop looking for a consent statute. Look for the bodies of law that regulate what an actor may do, rather than what a data subject may agree to.

IV. Antidiscrimination Law Reaches the Procurement

A. The Program Is Public Mobility

Title II of the Americans with Disabilities Act forbids a public entity to exclude a qualified individual with a disability from participation in, or deny that individual the benefits of, the services, programs, or activities of the entity.³² That the public right of way is such a program is settled. The Ninth Circuit held that maintaining public sidewalks is a service, program, or activity of a city, so that a failure to make them accessible states a Title II claim.³³ The Fifth Circuit, sitting en banc, reached the same conclusion for the building and altering of sidewalks under both Title II and Section 504.³⁴ The claim to use the city's network of streets and rights of way stands on the same statutory ground as the claim to enter the courthouse.³⁵

31. 15 U.S.C. § 6502(c) (treating a violation as an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act).

32. 42 U.S.C. § 12132.

33. *Barden v. City of Sacramento*, 292 F.3d 1073, 1076 (9th Cir. 2002).

34. *Frame v. City of Arlington*, 657 F.3d 215, 225–26 (5th Cir. 2011) (en banc).

35. *Cf. Tennessee v. Lane*, 541 U.S. 509, 533–34 (2004) (Title II validly enforces the right of access to the courts).

Where the equipment was purchased or operated with federal financial assistance, and a substantial share of municipal camera and plate reader deployments are grant funded through Department of Justice and Department of Homeland Security programs, Section 504 of the Rehabilitation Act supplies a parallel and substantively coextensive claim against the recipient.³⁶

Critically, the public entity cannot launder the program through its vendor. The Title II regulations reach discrimination carried out “directly or through contractual, licensing, or other arrangements.”³⁷ The entity that owes the class meaningful access to the mobility program is the same entity that procured, sited, and publicized the network. The vendor’s identity is evidence. It does not complicate the choice of defendant.

B. Campuses and School Districts

The Section 504 overlay is at its strongest where the recipient is an educational institution. A school district or public university that accepts federal financial assistance and installs plate readers on its own grounds is a recipient administering a program, and the Department of Education’s Section 504 regulation adopts the procedural provisions of its Title VI regulation for enforcement purposes.³⁸ The population is not incidental. Students with individualized education programs and Section 504 plans for psychiatric conditions attend the campuses on which the cameras sit, and the therapeutic environment the plan presupposes is the environment the network alters.

C. Choate, and the Two Regulatory Vocabularies

Alexander v. Choate governs and supplies both the standard and its principal limit. Section 504 reaches at least some conduct neutral on its face but discriminatory in effect, and the benchmark is meaningful access to the benefit the grantee offers.³⁹ *Choate* at the same time declined to

36. 29 U.S.C. § 794(a).

37. 28 C.F.R. § 35.130(b)(1).

38. 34 C.F.R. § 104.61 (adopting the procedural provisions of the Department’s Title VI regulation for purposes of Part 104).

39. *Alexander v. Choate*, 469 U.S. 287, 301 (1985).

read the statute as a freestanding regime under which every neutral policy with uneven effects is presumptively unlawful.⁴⁰ The consequence for pleading is precise. The claim is not bare statistical impact. It is framed in the two regulatory vocabularies the Department of Justice supplied, both of which *Choate* left intact.

The first is the reasonable modification mandate: a public entity must make reasonable modifications in policies, practices, or procedures where necessary to avoid discrimination, unless the modification would fundamentally alter the nature of the service.⁴¹ The modifications available here are operating parameters and never abolition: retention limits converting a permanent archive into a short rolling buffer; audit and purge obligations; buffer zones around clinical facilities, supportive housing, and peer support centers; query logging and access restriction; and expiration requirements on custom hotlist entries. Each modifies how the network operates. None removes a camera.

The second is the methods of administration regulation, which forbids criteria or methods of administration that have the effect of subjecting qualified individuals with disabilities to discrimination or that defeat or substantially impair accomplishment of the program's objectives for them.⁴² Indefinite retention, regional network sharing, and saturation publicity are methods of administering the program, selected by the entity and changeable by it. Their effect, for a class whose condition is defined in part by beliefs about being watched, is to close the mobility program the entity is obliged to keep open.

D. The Reality-Testing Mechanism

The mechanism is clinical and it is specific. Persecutory delusions are understood in the dominant cognitive account as threat beliefs maintained by safety-seeking strategies, so that treatment proceeds by relearning safety through entry into the feared situation.⁴³ The controlled

40. *Id.* at 298–99.

41. 28 C.F.R. § 35.130(b)(7)(i).

42. 28 C.F.R. § 35.130(b)(3).

43. Daniel Freeman, *Persecutory Delusions: A Cognitive Perspective on Understanding and Treatment*, 3 LANCET PSYCHIATRY 685 (2016).

evidence is that disconfirmation is what does the work: patients who tested threat predictions and dropped safety behaviours showed large reductions in delusional conviction, while exposure alone produced substantially less.⁴⁴ A standard therapeutic intervention for persecutory belief accordingly invites the patient to test the belief against the world. Where the belief is that one's movements are recorded and retrievable by strangers, and the municipality has installed a network that records and retrieves movements for strangers, the intervention has no purchase. The clinician cannot help the patient correct a belief that is accurate.

The security posture described in Part II.C converts what remained of the distortion into description. Before December 2025, the belief that an unauthorized stranger might be watching through a municipal camera was the kind of thought a clinician would treat. After sixty-seven feeds were found open to anyone with a browser, it was a report.⁴⁵

E. Three Objections

The first objection is that the relevant program is public safety, not mobility, and that a public entity does not deny access to its streets by placing a camera beside them. The answer is that the entity does not choose which of its programs the plaintiff invokes. The sidewalk and street cases establish the mobility program independently of anything the entity does with cameras, and the regulation asks whether a method of administering the entity's activities has the effect of impairing the program's objectives for the class.⁴⁶ Two programs are administered on the same right of way, and the second closes the first.

The second objection is that the harm is idiosyncratic and therefore not cognizable. This misreads the class. The claim is not that surveillance is unpleasant for sensitive people. It is that a protected class loses a specific therapeutic pathway that depends on a belief remaining falsifiable,

44. Daniel Freeman et al., *Virtual Reality in the Treatment of Persecutory Delusions: Randomised Controlled Experimental Study Testing How to Reduce Delusional Conviction*, 209 BRIT. J. PSYCHIATRY 62 (2016) (reporting a 22.0 percent reduction in delusional conviction for cognitive therapy against exposure alone, Cohen's $d = 1.3$); see also Tania M. Lincoln & Emmanuelle Peters, *A Systematic Review and Discussion of Symptom Specific Cognitive Behavioural Approaches to Delusions and Hallucinations*, 203 SCHIZOPHRENIA RSCH. 66 (2019).

45. Gaines, *extisupra* note 16. The clinical significance of the shift is that the falsifiability of the belief, not merely its content, is what the intervention depends on.

46. 28 C.F.R. § 35.130(b)(3).

and the controlled evidence identifies disconfirmation rather than habituation as the operative mechanism.⁴⁷ The general population loses comfort. The class loses treatment.

The third objection is standing, and it is the most serious. A claim that meaningful access has been denied to a class, with no identified member, is the generalized grievance the doctrine rejects.⁴⁸ What the claim requires is at least one injured person in fact, whose injury is concrete because it is diagnosable and documented, and who need not appear in the caption where an organization with members satisfies the associational requirements.⁴⁹

F. Sandoval, Payan, and the Administrative Route

Private enforcement of disparate impact regulations promulgated under Title VI was foreclosed in *Alexander v. Sandoval*.⁵⁰ Whether that reasoning reaches Section 504 and Title II disparate impact claims has divided courts; the Ninth Circuit has held that it does not.⁵¹

Two points follow. First, whatever the answer for private plaintiffs, it does not constrain the agency. The effects regulation is the agency's own, and the authority to enforce it administratively is what *Sandoval* left standing.⁵² An administrative complaint to the relevant grant-making agency therefore does not wait on the circuit split.

Second, the disparate impact theory need not carry the case alone. Failure to accommodate is an independent theory that the *Sandoval* debate does not touch, and it attaches on notice: once a public entity is told, in writing and with clinical support, that its administrative choices close the mobility program to a class, a refusal to consider any modification is the refusal the regulation addresses.

47. Freeman et al., *extisupra* note 44.

48. *Cf. Lujan v. Defs. of Wildlife*, 504 U.S. 555, 573–74 (1992).

49. *See Hunt v. Wash. State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977).

50. *Alexander v. Sandoval*, 532 U.S. 275, 293 (2001).

51. *Payan v. L.A. Cmty. Coll. Dist. (Payan I)*, 11 F.4th 729, 737–38 (9th Cir. 2021) (holding a private right of action exists to enforce disparate impact regulations under Title II and Section 504, and identifying disparate treatment, disparate impact, and failure to accommodate as the three available theories).

52. *Sandoval*, 532 U.S. at 289 (describing the agency's power to enforce its regulations by terminating funding or by other means authorized by law).

On remedy, the landscape is now more favorable than it was. The Ninth Circuit has extended *Cummings v. Premier Rehab Keller, P.L.L.C.*⁵³ to bar emotional distress damages under Title II, while expressly preserving compensatory damages for lost opportunities as economic harm.⁵⁴ A claim built on foregone employment, foregone medical appointments, and foregone education, rather than on distress, survives that limitation. And injunctive relief, which is the relief that matters for a network, is unaffected by it.

V. Criminal Surveillance Law Reaches the Conduct

A. *The Georgia Statute*

Every state criminalizes some form of nonconsensual surveillance. Georgia’s provision is representative and, because the vendor is headquartered in Atlanta and the incident discussed below occurred in a Georgia municipality, it is the natural vehicle.

It is unlawful for any person, through the use of any device, without the consent of all persons observed, to observe, photograph, or record the activities of another which occur in any private place and out of public view.⁵⁵ A violation of any provision of that Part is a felony punishable by imprisonment for one to five years, a fine up to \$10,000, or both.⁵⁶ Evidence obtained in violation of the Part is inadmissible in the courts of the state.⁵⁷

Three elements deserve emphasis. The verb “observe” completes the offense; no recording, retention, or distribution is required. The consent required is that of all persons observed, not that of the owner or occupier of the premises. And a separate paragraph makes it unlawful to sell, give, or distribute, without legal authority, a photograph or record of activities in a private place and out of public view without the consent of all persons observed.⁵⁸

53. 596 U.S. 212 (2022).

54. *Payan v. L.A. Cmty. Coll. Dist. (Payan II)*, 169 F.4th 971, 977–79 (9th Cir. 2026) (barring emotional distress damages and preserving compensatory damages for lost educational opportunities as economic harm).

55. GA. CODE ANN. § 16-11-62(2).

56. GA. CODE ANN. § 16-11-69.

57. GA. CODE ANN. § 16-11-67.

58. GA. CODE ANN. § 16-11-62(6).

B. The Contested Element

The element that will be litigated is whether the space is a private place and out of public view. “Private place” is defined as a place where there is a reasonable expectation of privacy.⁵⁹ The Georgia Court of Appeals has held that the term refers to a physical location, out of public view, in which an individual may reasonably expect to be safe from intrusion or surveillance, and has accordingly held that the provision does not criminalize the observation or filming of a person who is in a public place.⁶⁰ The court applied the rule of lenity in reaching that result, construing the criminal statute strictly and declining to extend it by forced interpretation.⁶¹

The consequence is a room-by-room analysis rather than a facility-wide one. Interior spaces from which the public is excluded, including changing areas and adjoining rooms, satisfy the element comfortably. An open floor observed by parents, staff, and other members is a harder case, and the rule of lenity cuts against the prosecution there.

C. The Exceptions, and the Circularity in the Owner Exception

Four exceptions attach to the prohibition. Two are plainly inapplicable to a vendor: the exception for observation of incarcerated persons and the exception for the curtilage of a residence.⁶²

The third exception permits an owner or occupier of real property to use a device for security, crime prevention, or crime detection to observe persons on the property, but only in areas where there is no reasonable expectation of privacy.⁶³ The qualifier produces a useful circularity. If the space is a private place, meaning a place where there is a reasonable expectation of privacy, then the owner’s own cameras are not within the exception either. The exception does

59. GA. CODE ANN. § 16-11-60(3).

60. *Gary v. State*, 338 Ga. App. 403, 407–09 (Ga. Ct. App. 2016) (reversing a conviction for a recording made in a grocery store aisle and holding that “private place” denotes a physical location rather than a region of the body).

61. *Id.* at 406.

62. GA. CODE ANN. § 16-11-62(2)(A), (C). The continued validity of subparagraph (2)(C) as printed warrants confirmation against the session laws, because the Georgia Supreme Court has held that an earlier subparagraph (2)(C) never survived a later enactment in the same session and that publication in the Official Code plays no role in determining validity. *Rutter v. Rutter*, 294 Ga. 1, 3–5 (Ga. 2013).

63. GA. CODE ANN. § 16-11-62(2)(B).

not authorize a property owner to place a camera anywhere on the property; it authorizes cameras only where the element the statute turns on is absent.

The fourth exception permits a law enforcement officer or agent, in the lawful performance of official duties, to observe activities that occur in the presence of that officer or agent.⁶⁴ Two limits follow from its text. A commercial sales demonstration is not the lawful performance of official duties. And activities viewed through a remote feed do not occur in the officer's presence.

D. Civil Consequences

The Part is criminal and, consistent with Georgia's general rule that a penal statute does not create a private right of action, the civil route runs through the common law tort of intrusion upon seclusion rather than through the statute itself.

One qualification is owed to that statement, because the leading case rests on two independent grounds and only one of them transfers. *Somerville* relied both on the longstanding rule against implied private rights and on a 2010 enactment providing that no private right of action shall arise from any Act enacted after July 1, 2010, unless expressly provided.⁶⁵ Section 16-11-62 long predates that date, so the statutory ground does not reach it and the question resolves on the common law rule alone. The practical consequence is unchanged. The exposure is criminal, the referral goes to the district attorney, and the civil theory is the tort.⁶⁶ That is a routing question rather than a defense. The criminal exposure remains, and the referral goes to the district attorney.

64. GA. CODE ANN. § 16-11-62(2)(D).

65. GA. CODE ANN. § 9-2-8(a); *Somerville*, 337 Ga. App. at 416–17. The court expressly rested on the fact that the statute before it was enacted in 2014.

66. *Somerville v. White*, 337 Ga. App. 414, 415–17 (Ga. Ct. App. 2016) (holding that civil liability arises under a penal statute only where the General Assembly expressly provided a private right of action in the text, and reversing compensatory and punitive awards entered under GA. CODE ANN. § 16-11-90).

E. The Real Obstacle Is Not Doctrinal

The honest difficulty with this Part is not that the elements fail. It is that the enforcement decision belongs to a local prosecutor whose office works daily with the department that bought the cameras. That is a structural conflict rather than a legal defect, and it explains why a statute this old and this broad has never been applied to vendor conduct. It also identifies the audience: the argument is addressed to state attorneys general, to legislative oversight committees, and to the civil bar, none of whom depend on the cooperation of the purchasing agency.

VI. Consumer Protection Law Reaches the Vendor

A. The Authority, and That It Covers Security

Section 5 of the Federal Trade Commission Act declares unlawful unfair or deceptive acts or practices in or affecting commerce.⁶⁷ The Commission may declare an act unfair only where it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or to competition.⁶⁸

Whether that authority extends to a company's data security is settled at the appellate level. The Third Circuit held that it does, and rejected the argument that the standard is too imprecise to supply notice, reasoning that a company is not entitled to such precision as would eliminate all close calls and that fair notice is satisfied where a company can reasonably foresee that a court could construe its conduct as falling within the statute.⁶⁹ The court further described what subsection 45(n) requires as a cost-benefit inquiry weighing the probability and expected size of reasonably unavoidable consumer harms at a given level of security against the costs of investing in stronger security.⁷⁰

67. 15 U.S.C. § 45(a)(1).

68. 15 U.S.C. § 45(n).

69. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 255–56 (3d Cir. 2015).

70. *Id.* at 255.

One further holding in that decision does most of the work here. The court held that a company's conduct need not be the most proximate cause of an injury to support liability for foreseeable harms, and that criminal conduct by a third party does not break the chain where the defendant facilitated it and the harm was reasonably foreseeable.⁷¹ A vendor whose credentials were offered for sale on criminal forums, and whose cameras could be rooted in half a minute from a public pole, cannot answer the resulting harm by pointing at the person who walked through the door it left open.

B. Deception

The deception theory requires no novel doctrine. The vendor made representations to municipal purchasers and to the public about federal access and about the security of its platform. The record in Part II.D establishes that at least one category of those representations was inaccurate and was corrected only after contrary information surfaced.⁷²

Materiality is the element that decides a deception count, and it is supplied here by the identity of the audience. These representations were made to city councils weighing procurement, in public session, on the precise question the councils were deliberating. A statement about whether federal agencies can reach a city's data is not collateral to that decision. It is the decision. And a municipal purchaser could not have verified it independently, because the access logs that would have disproved it were held by the vendor and surfaced only through public records litigation by a resident.⁷³

C. Unfairness

Each element of subsection 45(n) is satisfied on the documented record.

71. *Id.* at 246.

72. ACLU, extitsupra note 24. The chief executive's own characterization afterward was that the company had communicated poorly. extscBS Chicago, extitsupra note 25.

73. *See supra* notes 19–24 and accompanying text.

The injury is substantial. It is continuous location capture, retained, searchable nationally, and demonstrably reachable by parties with no authorization of any kind.⁷⁴ Substantiality does not require that a catastrophe has already occurred; a small harm to a very large number of people satisfies the standard as readily as a large harm to a few, and this network photographs a substantial share of the driving public.

It is not reasonably avoidable. This element is ordinarily the hardest for the Commission and is the easiest here. Avoidance presupposes a choice, and the person photographed has none. Camera locations are not disclosed, the capture requires no interaction, and there is no notice at the moment of collection and no mechanism to decline afterward. A driver cannot know that a given feed is open to the internet, and could not act on the knowledge if she had it, short of not driving.

The countervailing benefits are the contested element, and it is where the vendor will make its stand.

D. The Countervailing Benefits Question

The vendor's answer to any unfairness theory is public safety, and the answer has to be met on evidence rather than on assertion, because subsection 45(n) makes benefit a term of the test rather than a defense outside it.

Three categories of record bear on it. The first is efficacy. Municipal oversight bodies that have measured outcomes rather than argued about them have reported that a substantial share of stops prompted by system alerts ended in release because of data problems, and at least one board concluded it had seen no evidence that the cameras had contributed to the outcomes claimed for them.⁷⁵

The second is the cost side of the same ledger. Erroneous alerts have produced stops at gunpoint and settlements in the seven figures, including a reported \$1.9 million settlement arising from an incident in which four children were removed from a vehicle at gunpoint after

74. Gaines, *extitsupra* note 16; *extscGadget Rev.*, *extitsupra* note 17.

75. *See DeFlock*, *extitsupra* note 11 (collecting municipal oversight findings, including from Oak Park, Illinois).

a plate matched a stolen vehicle from another state, and a reported \$495,000 settlement where a reader misread a single digit.⁷⁶ Those payments are borne by the municipalities rather than by the vendor, which is itself a fact about how the costs of the product are distributed.

The third is that the benefit the analysis weighs is the benefit of the product as secured, not the benefit of a hypothetical version of it. Nothing in the public safety case for automated plate reading requires that the feeds be reachable without a password, that credentials be usable without multifactor authentication, or that a camera on a pole yield root access in thirty seconds. The costs of remediating each of those are ordinary engineering costs. That asymmetry, large avoidable harm against modest remediation expense, is what the cost-benefit inquiry was written to capture.

E. Two Objections

The first objection is that the person photographed is not the vendor's customer, so there is no consumer relationship to protect. Section 5 does not require one. The unfairness standard speaks to substantial injury to consumers rather than to counterparties, and the Commission has never been limited to policing the terms of completed transactions. In any event the municipal purchaser is a customer, and it was told the platform was secure.

The second objection is that the Commission's data security authority has been contested, most visibly where an order was vacated because the conduct it required was not stated with enough specificity to be enforceable.⁷⁷ That decision concerns the form of the remedy rather than the existence of the authority, and the court said so, assuming for the sake of its analysis that the underlying failure was an unfair act or practice and vacating on specificity alone.⁷⁸ It argues for a narrowly drawn order identifying particular controls rather than against proceeding at

76. *Id.*

77. *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1236 (11th Cir. 2018) (the order “does not enjoin a specific act or practice” but “mandates a complete overhaul” of the respondent's data-security program, and is therefore unenforceable).

78. *Id.* at 1236 (assuming *arguendo* that a negligent failure to maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a)); *id.* at 1235 (prohibitions in cease and desist orders and injunctions “must be specific,” governed by the same standard because the stakes for violation are the same). The decision separately requires the Commission to ground unfairness in policies expressed in the Constitution, statutes, or the common law, *id.* at 1229, which the sources assembled in Parts V and VII supply.

all. The controls here name themselves: mandatory phishing-resistant multifactor authentication, disabling of diagnostic access on deployed hardware, an authenticated default for every feed, and audit fields that cannot be satisfied by arbitrary text.

The vendor's stated defense to the physical attack, that exploitation requires physical access and knowledge of internal hardware, does not survive contact with the deployment model. The cameras are installed on public poles at a height reachable with a ladder. Physical access to public infrastructure is a design assumption, not a security control.

VII. Contract and Delegated Authority Reach the Access

A. The Pattern

The narrowest and, in a specific case, the most powerful of the six bodies is the ordinary law of authority. A municipality may share access to its own cameras. It may not license to a vendor a use of a third party's cameras that the third party was expressly told would not occur.

The pattern arises whenever a private institution is asked to contribute its cameras to a municipal network. The institution is approached by a department, declines a general grant, and receives a writing narrowing the request to a stated purpose, commonly real-time response to a critical incident. On that representation the institution agrees.⁷⁹ What the department obtained was not a camera. It was a license, and the license had terms.⁸⁰

79. The Article states this pattern generically. A documented instance exists in a metropolitan Atlanta suburb, where a police department's September 2024 writing narrowed a private community center's grant of interior camera access to real-time critical incident response, and vendor personnel later opened cameras serving children's programming during commercial demonstrations. The institution in that instance is the party whose consent was exceeded rather than a wrongdoer, and the argument here turns on the text of the limiting writing and on who may consent for whom, neither of which depends on identifying the facility. Naming a children's facility as a surveillance subject in academic literature amplifies the exposure the section is written to condemn, and the doctrinal analysis is complete without it.

80. Nothing turns on whether the arrangement is characterized as a license, a bailment of access, or a contract for services. Each carries the same limitation: the grant is measured by its stated scope.

B. A Municipality Cannot License What It Never Held

The first consequence is a matter of arithmetic rather than doctrine. A party cannot convey an interest larger than the one it holds. A department granted access for critical incident response holds access for critical incident response, and a later agreement between that department and a vendor, however broadly drafted, operates on the department's interest and not on the institution's. A demonstration agreement can no more enlarge that consent than a lease can enlarge the term of the underlying estate.⁸¹

The second consequence follows from how the consent was procured. The narrowing writing was not a recital appended to a completed bargain. It was the inducement, offered after the institution had refused the broader request, and it is therefore a term rather than a preamble. A grantor who agrees only after receiving an express limitation has agreed to the limitation, and a use outside it is a breach whether or not any document uses that word.⁸²

C. Apparent Authority Does Not Rescue the Vendor

The vendor's answer is apparent authority: it dealt with the municipality, it believed the municipality could grant what it granted, and it should be protected in that reliance.

Apparent authority is created by manifestations traceable to the principal, and it exists only where a third party reasonably believes the actor has authority and that belief is traceable to the principal's own manifestations rather than to the actor's.⁸³ The principal whose interests

81. Georgia binds a principal by the acts of its agent taken within the scope of the agent's authority, which is the same proposition stated from the other side. GA. CODE ANN. § 10-6-51. Authority conferred for a stated purpose is measured by that purpose, and where an express restriction exists the authority is not plenary. *Cf. Omni Builders Risk*, 313 Ga. App. at 360 (authority "determined by the contract... and by instructions given," and treated as plenary only "in the absence of express restrictions").

82. The limitation is the inducement for which assent was exchanged, and a communication that induces assent is a term of the resulting agreement rather than a gloss on it. Georgia treats reliance on such a communication as itself sufficient consideration. GA. CODE ANN. § 13-3-44(a); *Kemira, Inc. v. Williams Investigative & Sec. Servs., Inc.*, 215 Ga. App. 194, 198–99 (Ga. Ct. App. 1994).

83. *Omni Builders Risk, Inc. v. Bennett*, 313 Ga. App. 358, 360–61 (Ga. Ct. App. 2011) ("Apparent authority is that which the principal's conduct leads a third party reasonably to believe the agent has"; "[w]here there were no manifestations of authority by the principal to a third party, apparent authority is not in issue."). The evidence must show that the principal either intended to cause the third person to believe the agent was authorized or should have realized that its conduct was likely to create that belief. *Id.* at 361.

are in suit is the institution that supplied the cameras and received the written limitation, not the department that passed the access along. A vendor that never saw a grant from that principal, and relied instead on a representation by an intermediary, holds no apparent authority against it. Reliance may bear on how loss is allocated between the vendor and the municipality. It does not manufacture consent the camera owner never gave.

The Supreme Court has said as much in the closest analogous setting, warning that rights are not to be eroded by strained applications of the law of agency or by unrealistic doctrines of apparent authority.⁸⁴

D. And the Institution Could Not Have Consented for the Occupants Anyway

The deeper point is that even a general grant by the institution would not reach the people inside the rooms.

Stoner is the cleanest statement of it. A hotel guest's protection, the Court held, would disappear if it were left to depend upon the unfettered discretion of an employee of the hotel, and the right at stake belonged to the guest, so that it was a right which only the guest could waive by word or deed, directly or through an agent.⁸⁵ The Court then drew the line that governs this Part. A person who takes a room gives implied permission to maids, janitors, and repairmen to enter in the performance of their duties, and that permission does not extend to authorizing a search.⁸⁶

Substitute the facts. A facility grants a department access to its interior cameras for response to a critical incident. That is permission for a stated duty. It is not permission for a salesperson in another building to open the feed and look at a room of children in order to close a deal with a prospective municipal buyer. And the people in the room, who granted nothing, retain what the facility never held on their behalf.

84. *Stoner v. California*, 376 U.S. 483, 488 (1964). The apparent-authority discussion in *Stoner* has since been qualified for co-occupants who share common authority, see *Illinois v. Rodriguez*, 497 U.S. 177, 188–89 (1990), but the holding that an employee of the establishment cannot consent for the occupant is undisturbed.

85. *Stoner*, 376 U.S. at 489.

86. *Id.* at 489 (distinguishing *United States v. Jeffers*, 342 U.S. 48, 51 (1951)).

This is also why Part V’s criminal analysis and this Part converge rather than duplicate. The Georgia statute requires the consent of all persons observed, which is the same proposition stated as an element.⁸⁷ The facility’s signature is not their consent, and no agreement between the facility, the department, and the vendor can supply it.

E. Remedies, and the Problem That Precedes Them

The institution’s remedies are ordinary: breach of the access agreement, rescission of it, and an injunction against further use outside the stated purpose. Where the institution acted on a written assurance and would not otherwise have agreed, reliance supplies an independent basis.⁸⁸ And under the exclusionary provision that accompanies the criminal statute, evidence obtained in violation of the Part is inadmissible in the courts of the state, which converts the question from an abstraction into one with consequences for any prosecution that touches the footage.⁸⁹

A municipality that invokes a demonstration agreement and then cannot produce it has an additional and more mundane problem, in the law of municipal contracting and public records, that precedes every question discussed above.

VIII. Computer Crime Law, and the One Real Gap

A. The Intruder

Federal computer crime law reaches the person who compromises a camera. Intentionally accessing a protected computer without authorization and obtaining information from it violates the Computer Fraud and Abuse Act.⁹⁰ A person who opens the diagnostic access point on

87. GA. CODE ANN. § 16-11-62(2).

88. GA. CODE ANN. § 13-3-44(a) (“A promise which the promisor should reasonably expect to induce action or forbearance on the part of the promisee or a third person and which does induce such action or forbearance is binding if injustice can be avoided only by enforcement of the promise.”); *Kemira*, 215 Ga. App. at 198–99 (statute codifies promissory estoppel, under which reliance is itself sufficient consideration). That the assurance concerned future conduct and was conditional does not defeat the theory. *Id.* at 199.

89. GA. CODE ANN. § 16-11-67.

90. 18 U.S.C. § 1030(a)(2)(C) (prohibiting intentionally accessing a computer without authorization or exceeding authorized access and thereby obtaining information from any protected computer); *id.* § 1030(e)(2)(B) (defining “protected computer” to include a computer used in or affecting interstate commerce or communication).

a pole-mounted camera and takes root has no authorization at any gate, and the analysis is straightforward.

B. The Insider, and Van Buren

The credentialed officer is a different matter, and here the assembled architecture of this Article has a hole in it that honesty requires naming.

In *Van Buren v. United States*, a police officer accepted money to run a search in a law enforcement database.⁹¹ The Supreme Court held that an individual exceeds authorized access only when he accesses a computer with authorization and then obtains information located in areas of the computer that are off-limits to him.⁹² Liability under both clauses of the statute stems from what the Court called a gates-up-or-down inquiry: one either can or cannot access a system, and one either can or cannot access particular areas within it.⁹³ Improper purpose is not the test. Justice Thomas, in dissent, would have held that using a police database in circumstances where that use is expressly forbidden is a crime.⁹⁴ He did not carry the Court.

The conduct at the center of the concern in Part X therefore falls outside the federal computer crime statute. An officer with lawful access to the platform who enters a plate for a forbidden reason, including for payment, has not exceeded authorized access.

Two partial answers exist and neither is complete. Federal program bribery reaches an agent of a local agency that receives federal funds who solicits or accepts a thing of value in connection with the agency's business, and grant-funded deployments will often supply the

91. *Van Buren v. United States*, 593 U.S. 374 (2021).

92. *Id.* at 378 (“An individual ‘exceeds authorized access’ when he accesses a computer with authorization but then obtains information located in particular areas of the computer, such as files, folders, or databases, that are off-limits to him.”).

93. *Id.* at 390.

94. *Id.* at 400 (Thomas, J., dissenting).

jurisdictional predicate.⁹⁵ And many states criminalize misuse of law enforcement databases directly.

Neither answer is clean, and the reasons are worth stating. The bribery statute conditions liability on a business or transaction of the agency involving anything of value of \$5,000 or more, a threshold that attaches to the underlying transaction rather than to the payment, and a single database query is not obviously such a transaction.⁹⁶ The statute also requires a corrupt agreement rather than a reward conferred after the fact.⁹⁷ The state statutes vary in coverage and in whether they extend to a query made with valid credentials.

The federal statute written for computer misuse therefore does not reach the paradigm case of computer misuse, and that is the one place in this Article where the argument that the law already reaches must yield.

C. The Insider Is Not Hypothetical

The gap matters because the conduct is documented. A federal firearms agency analyst improperly accessed a Virginia municipality's plate reader system to aid an immigration investigation and is no longer employed by that department.⁹⁸ Texas authorities searched roughly eighty-three thousand cameras nationwide in a search connected to a suspected self-administered

95. 18 U.S.C. § 666(a)(1)(B) (agent who corruptly solicits, demands, accepts, or agrees to accept anything of value, intending to be influenced or rewarded in connection with any business or transaction of the agency involving anything of value of \$5,000 or more); *id.* § 666(b) (jurisdictional predicate: agency receives benefits in excess of \$10,000 in any one-year period under a Federal program); *id.* § 666(d)(1) (defining "agent" to include an employee of a government).

96. 18 U.S.C. § 666(a)(1)(B). The better characterization treats the agency's surveillance contract, routinely six figures, as the business in connection with which the agent was rewarded, but the point is contestable and has not been litigated on these facts.

97. *Cf. Snyder v. United States*, 603 U.S. 1 (2024) (holding that § 666 criminalizes bribes and does not criminalize gratuities).

98. *See* Immigr. Pol'y Tracking Project, *Reported: ICE Using Automated License-Plate-Reader Cameras for Immigration Enforcement via State/Local Police*, <https://immpolicytracking.org/policies/reported-ice-accessing-flock-automated-license-plate-reader-cameras-via-local-law-enforcement/> (last visited Aug. 9, 2026).

abortion, reaching into states where the procedure is lawful.⁹⁹ An Oregon department entered the string “hehehe” into the mandatory search reason field on twenty occasions.¹⁰⁰

The audit control on a nationwide real-time tracking system is a free text box, and it has already been defeated by officers acting for their own reasons, without payment.

IX. National Security Data Law Reaches the Location Data

A. The Rule

The executive branch has already found, in a binding regulation, that precise location data about federal personnel is a national security risk. Executive Order 14117 directed, and the Department of Justice implemented, the Data Security Program, effective April 8, 2025.¹⁰¹

The Program defines government-related data to include any precise geolocation data, regardless of volume, for any location within an area enumerated on a Government-Related Location Data List, on the Attorney General’s determination that such data poses a heightened risk of revealing insights about federally controlled locations, including insights about the facilities, activities, or populations there, and including the worksites of personnel who occupy national security positions.¹⁰² The List enumerates 736 geofenced locations.¹⁰³ Precise geolocation data means data identifying the physical location of an individual or device within

99. Letter from Rep. Robert Garcia & Rep. Raja Krishnamoorthi to Garrett Langley, CEO, Flock Grp. Inc. 1–2 (Aug. 6, 2025), <https://krishnamoorthi.house.gov/sites/evo-subsites/krishnamoorthi.house.gov/files/evo-media-document/2025-08-06.garcia-krishnamoorthi-to-flock-re-lpr-tech-and-tracking.pdf> (last visited Aug. 9, 2026).

100. ACLU, *extitsupra* note 24.

101. Exec. Order No. 14117, 89 Fed. Reg. 15421 (Mar. 1, 2024); Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636 (Jan. 8, 2025) (final rule) (codified at 28 C.F.R. pt. 202).

102. 28 C.F.R. § 202.222(a)(1).

103. 28 C.F.R. § 202.1401.

1,000 meters.¹⁰⁴ The countries of concern are China, including Hong Kong and Macau, Cuba, Iran, North Korea, Russia, and Venezuela.¹⁰⁵

B. The Continental Geofence

A plate photographed by a fixed pole-mounted camera is precise geolocation data by any measure the regulation supplies. The obvious objection is that a plate identifies a vehicle rather than a person. The regulation anticipates it twice over. Government-related location data need not be linked or linkable to an individual at all, because the risk the Attorney General identified is insight into the facility rather than identification of a driver.¹⁰⁶ And the empirical literature on mobility traces has established that the gap between a movement record and an identity is narrow: in a dataset of one and a half million people, four spatio-temporal points sufficed to identify ninety-five percent of individuals uniquely, and coarsening the resolution degraded that uniqueness only slowly.¹⁰⁷ A registration record closes the remaining gap in one lookup. Whether any particular camera sits inside one of the 736 enumerated areas is an empirical question worth answering, and the answer is discoverable, since the List is public and deployment locations are substantially mapped.

But the empirical question is smaller than the structural one, and the structural one exposes an under-inclusiveness in the rule that its own rationale cannot survive.

The List geofences discrete sites because the threat model behind it assumed that collection is patchy, incidental, and site-specific. Where collection is continuous across the road network, the premise inverts. An adversary does not need a camera at a sensitive site if it has cameras on every road leading to and from it. Indeed route coverage yields more than a site read does. A site read establishes that a person was somewhere once. Route coverage establishes

104. 28 C.F.R. § 202.242.

105. 28 C.F.R. §§ 202.208, 202.213, 202.229, 202.236, 202.247, 202.250–.251, 202.259 (naming each jurisdiction); *id.* § 202.601 (determination of countries of concern); *id.* § 202.209 (defining “country of concern”).

106. 28 C.F.R. § 202.222(a)(1). Contrast the bulk sensitive personal data categories, which do turn on linkage. *Id.* §§ 202.232–.233 (defining “linked” and “linkable”).

107. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REPS. 1376 (2013).

arrival times, departure times, frequency, duration, and onward destination, which is to say pattern of life. The regulation's stated concern is insight into facilities, activities, and populations. Continuous route coverage delivers that concern more completely than the enumerated geofence does.

This Article calls the resulting condition a *continental geofence*: a collection network of sufficient density and interoperability that the analytically relevant boundary is national rather than local, and site enumeration ceases to describe the risk.

C. *The Empirical Question, Answered*

Whether any automated plate reader sits inside an enumerated area is an empirical question, and it is answerable from public sources alone. The List publishes corner coordinates for all 736 areas.¹⁰⁸ Reader locations are separately mapped by a volunteer project whose records are contributed to a public geographic database under a standard tagging scheme.¹⁰⁹ Joining the two is a point-in-polygon operation.

The author performed that join against 23,946 mapped readers. Seventy-four enumerated areas contain at least one reader within the published boundary. Forty-one of the areas registering hits are drawn on a very large scale, some spanning hundreds of kilometers, and excluding those leaves fifty-five tightly drawn areas holding 504 readers inside the fence.

The ratio that matters is what happens outside it. Within two kilometers of an enumerated area there are 4,656 readers. Within five, 7,660. Within ten, 11,992. Five hundred and four readers stand inside the boundaries the Attorney General drew, and roughly twenty-four times that number stand within a ten kilometer approach. The rule geofenced the destinations. The network holds the roads.

108. 28 C.F.R. § 202.1401 tbl.1 (publishing, for each Area ID, latitude and longitude pairs forming the corners of the geofenced area).

109. Data retrieved Aug. 10, 2026 from OpenStreetMap via the Overpass application programming interface, querying nodes tagged `man_made=surveillance` with `surveillance:type=ALPR`. See DeFlock, <https://deflock.me> (last visited Aug. 10, 2026) (crowdsourced mapping project contributing to that database). Coverage is volunteer-generated and therefore incomplete, which means the analysis can establish presence and can never establish absence. Every figure below is a floor.

D. One Zone

The densest example is Area 605, and it is worth stating in full because the abstraction disappears on contact with it.

The published corners are 38.8665872170001, -77.06187689; 38.8804333410001, -77.06187689; 38.8804333410001, -77.0457741439999; and 38.8665872170001, -77.0457741439999.¹¹⁰ The enclosed area is 2.14 square kilometers, a rectangle roughly 1.5 kilometers by 1.4. Plotted on satellite imagery, it resolves to the Pentagon reservation in Arlington, Virginia, bounded by Arlington National Cemetery to the west, Interstate 395 and Washington Boulevard through the interior, and the Boundary Channel and Columbia Island Marina to the east.¹¹¹

Eleven mapped automated plate readers stand inside it, a density of 5.15 readers per square kilometer. They are not clustered in one place. Two sit at the northern approach near the Memorial Bridge interchange, two at the eastern edge near the marina and the river crossing, three along the interior arterials and ramps on the building's eastern face, and four at the southern parking areas and the interchange feeding them. That distribution is the significant fact. The readers are positioned on the roads by which the site is entered and left.

The regulation drew this boundary for the express reason that precise location data generated inside it poses a heightened risk of revealing insights about the facility, the activities conducted there, and the personnel who work there, including personnel occupying national security positions.¹¹² The same regulation attaches no bulk threshold to such data, precisely because a single reading can carry that insight.¹¹³

Area 605 is one of fifty-five. The point of setting it out is not that this rectangle is the worst case, though it is difficult to nominate a better candidate. It is that the government

110. 28 C.F.R. § 202.1401 tbl.1 (Area ID 605).

111. Boundary coordinates from 28 C.F.R. § 202.1401 tbl.1 (Area ID 605), rendered over Google Earth imagery. The Attorney General's List publishes coordinates without naming the facilities they enclose; the identification here is made by inspection of the imagery within the published boundary.

112. 28 C.F.R. § 202.222(a)(1).

113. *Id.* (government-related data status attaches "regardless of volume").



Figure 1: Geofenced Area 605, published at 28 C.F.R. § 202.1401 tbl.1, rendered over Google Earth imagery, with the eleven automated plate readers mapped inside its boundary. Boundary drawn from the coordinates published in the rule. Reader positions from OpenStreetMap, retrieved August 10, 2026.

identified this rectangle, by coordinate, as a place where location data is a national security concern, and a commercial network selling subscription access to location data operates eleven readers inside it, on the roads in and out. Nothing in the Program’s structure prevented that, because the Program regulates transfers to foreign adversaries rather than domestic collection, and no privacy statute prevented it either.

E. The Admission

The value of the Program to the argument is not primarily as a cause of action. Its prohibitions attach to covered data transactions, meaning data brokerage, vendor, employment, and investment arrangements with countries of concern or covered persons, and credentials stolen and resold by criminals may not constitute a transaction within that definition.¹¹⁴

That statement understates the rule, and the definition of data brokerage is why. Data brokerage means the sale of data, the licensing of access to data, or a similar commercial transaction transferring data from a provider to a recipient where the recipient did not collect the data directly from the individuals linked or linkable to it.¹¹⁵ The Department’s own illustration is an organization that maintains a database and sells annual memberships conferring a license to access it.¹¹⁶ That is the subscription model described in Part II. An agency pays for access to a network of cameras it did not install, and reads plates its own officers never collected.

Three predicates follow, and each is a question of fact rather than of doctrine. The first is a prohibited data-brokerage transaction, which requires a country of concern or covered person on the receiving end, and a covered person includes any individual primarily resident in a country of concern.¹¹⁷ The second requires no country of concern at all. Where a transaction involves access by any foreign person to government-related data and involves data brokerage,

114. 28 C.F.R. § 202.210 (defining “covered data transaction”); *id.* § 202.211 (defining “covered person”); *id.* § 202.214 (data brokerage); *id.* § 202.258 (vendor agreement); *id.* §§ 202.301–.305 (prohibited transactions, including prohibited evasions and knowingly directing prohibited transactions); *id.* § 202.1301 (penalties).

115. 28 C.F.R. § 202.214(a).

116. *Id.* § 202.214(b)(3).

117. *Id.* § 202.301(a); *id.* § 202.211(a)(4).

the operator must contractually bar onward brokerage to a country of concern and must report known or suspected violations of that term within fourteen days.¹¹⁸ The third is the vendor path: any agreement under which a covered person provides goods or services, including cloud computing, with access to such data is a restricted transaction, permitted only on satisfaction of the Program's security requirements.¹¹⁹ An operator whose platform lacked mandatory multifactor authentication would have difficulty establishing the third.

What the rule does not reach is theft. The Department's own example holds that a domestic company does not violate the Program merely because a foreign vendor employs individuals resident in a country of concern, absent evasion or knowing direction.¹²⁰ Credentials stolen and resold on a criminal forum are not a transaction, and no amount of foreseeability converts them into one. The gap between what the rule prohibits and what the security record shows is therefore real, and it is the gap a legislature could close.

Its remaining value is evidentiary. The United States has determined, and written into the Code of Federal Regulations, that precise location data concerning federal personnel is a national security risk regardless of volume when a foreign adversary can reach it. Having made that determination, the same government funded and deployed a domestic network that generates precisely that data class, secured it with an unenforced authentication policy, and watched its credentials appear for sale on Russian cybercrime forums.¹²¹ The threat model is not contested. It is the government's own, and the government built the collection system after writing it down.

X. Conclusion: The Substitution

Assemble the pieces the vendor sells and the researchers found.

118. *Id.* § 202.302(a)–(b).

119. *Id.* § 202.258(a) (defining vendor agreement); *id.* § 202.401 (authorization to conduct restricted transactions); *id.* § 202.248 (security requirements).

120. *Id.* § 202.230(b)(1).

121. extscState of Surveillance, extitsupra note 18.

A plate can be resolved to a vehicle. A vehicle can be entered on a custom hotlist by a credentialed user, without judicial review and without expiration. Every camera in a nationwide network then checks every passing vehicle against that entry, and an alert reaches a handheld device in real time, with an image and a location, filtered to a radius the subscriber chooses. Successive alerts yield heading. The vendor markets this sequence, including the final step in which units coordinate to converge on the vehicle.

Now change one field. Let the vehicle belong to a state legislator, a member of Congress, a federal judge, or a protective detail. Nothing about the system changes, because the system has no concept of a protected principal. The entry is made the same way, the alerts arrive the same way, and the convergence is coordinated the same way. The only difference is who is converging, and why.

The access required is one credentialed account in one department among nearly five thousand. It need not be a sophisticated intrusion. Officers have already run queries in this system for their own private reasons, in jurisdictions whose law forbade it, and have defeated the audit control by typing nonsense into a text field. After *Van Buren*, an officer paid to make such an entry has not committed a federal computer crime.

What is being purchased in that transaction is not a lookup. A lookup is a single answer about the past. A hotlist entry is a standing subscription to a person's movements, and its marginal cost after purchase is zero. A third product exists that will not occur to most readers, which is non-entry: payment to ensure that a particular plate never alerts. That is counter-surveillance, and to some buyers it is worth more than tracking.

None of this requires a new statute to be unlawful. The procurement is reachable under Title II and Section 504. The observation of persons in private spaces is a felony in Georgia and its analogues. The vendor's representations and security posture are reachable under Section 5. The access exceeding the scope of the camera owner's consent is reachable in contract and in the law of delegated authority. The intruder is reachable under the Computer Fraud and Abuse Act.

And the location data itself is already classified by the executive branch, in a binding regulation, as a category of national security concern.

None of these six is free of obstacles, and this Article has named them rather than routed around them: the *Choate* limit and the circuit split on private enforcement, the private place element and the rule of lenity, the contested shape of administrative data security authority, apparent authority, the transaction threshold in the bribery statute, and the covered transaction limit in the Data Security Program. Every one of those is an argument a court has the tools to resolve. None of them requires a legislature.

Six bodies of law, none of them enacted for this purpose, none of them a privacy statute, all of them presently in force. Legislatures debating a seventh should be told what the first six already do, and should be asked why the one real gap, the bought insider, is the gap nobody is drafting to close.

The last observation is the one that ought to move an audience that has never cared about any of this. The legislators who will decide whether this infrastructure continues are inside its coverage. The tool cannot tell them apart from anyone else. It was not built to.

References

- Alexander v. Choate, 469 U.S. 287 (1985).
- Alexander v. Sandoval, 532 U.S. 275 (2001).
- American Civil Liberties Union. (2026). *Flock Safety credibility lost as it repeatedly lies to city councils, police departments, and public across the country*. <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flock-safety-credibility-lost-as-it-repeatedly-lies-to-city-councils-police-departments->
- Americans with Disabilities Act of 1990, 42 U.S.C. §§12101–12213.
- Barden v. City of Sacramento, 292 F.3d 1073 (9th Cir. 2002).
- Bribery concerning programs receiving Federal funds, 18 U.S.C. §666.
- Children’s Online Privacy Protection Act, 15 U.S.C. §§6501–6506.
- Children’s Online Privacy Protection Rule, 16 C.F.R. pt. 312.
- Computer Fraud and Abuse Act, 18 U.S.C. §1030.
- Cummings v. Premier Rehab Keller, P.L.L.C., 596 U.S. 212 (2022).
- de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports*, 3, 1376.
- Executive Order No. 14117, 89 Fed. Reg. 15421 (2024).
- Federal Trade Commission Act, 15 U.S.C. §45.
- Flock Safety. (n.d.). *Does Flock share data with ICE?* <https://www.flocksafety.com/blog/does-flock-share-data-with-ice>.
- Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
- Frame v. City of Arlington, 657 F.3d 215 (5th Cir. 2011) (en banc).
- Freeman, D. (2016). Persecutory delusions: A cognitive perspective on understanding and treatment. *Lancet Psychiatry*, 3, 685.
- Freeman, D., Bradley, J., Antley, A., Bourke, E., DeWeever, N., Evans, N., . . . Clark, D. M. (2016). Virtual reality in the treatment of persecutory delusions. *British Journal of Psychiatry*, 209, 62.
- Gaines, J. (2026). *Finding 67 Flock Safety live PTZ camera/LPR feeds and debug web interfaces accidentally exposed without authentication to the internet*. GainSec. <https://gainsec.com/2026/01/09/bird-hunting-season-finding-67-live-camera-feeds-and-debug-web-interfaces-accidentally-e>
- Gary v. State, 338 Ga. App. 403 (Ga. Ct. App. 2016).
- Hunt v. Washington State Apple Advertising Commission, 432 U.S. 333 (1977).
- Illinois v. Rodriguez, 497 U.S. 177 (1990).
- LabMD, Inc. v. Federal Trade Commission, 894 F.3d 1221 (11th Cir. 2018).
- Georgia Code Annotated §§16-11-60 to 16-11-69.
- Koebler, J. (2025). Illinois cops gave ICE access to more than 5,000 surveillance cameras nationwide. *404 Media*.

- Lincoln, T. M., & Peters, E. (2019). A systematic review and discussion of symptom specific cognitive behavioural approaches to delusions and hallucinations. *Schizophrenia Research*, 203, 66.
- Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).
- Payan v. Los Angeles Community College District (Payan I), 11 F.4th 729 (9th Cir. 2021).
- Pereira, G., & Raetzsch, C. (2022). From banal surveillance to function creep: Automated license plate recognition (ALPR) in Denmark. *Surveillance & Society*, 20(3), 265.
- Payan v. Los Angeles Community College District (Payan II), 169 F.4th 971 (9th Cir. 2026).
- Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 28 C.F.R. pt. 202.
- Rehabilitation Act of 1973, Section 504, 29 U.S.C. §794.
- Kemira, Inc. v. Williams Investigative & Security Services, Inc., 215 Ga. App. 194 (Ga. Ct. App. 1994).
- Omni Builders Risk, Inc. v. Bennett, 313 Ga. App. 358 (Ga. Ct. App. 2011).
- Rutter v. Rutter, 294 Ga. 1 (Ga. 2013).
- Snyder v. United States, 603 U.S. 1 (2024).
- Schneider, J. (2025). Big Brother left the door open: Flock's AI surveillance cameras exposed to the internet. *PetaPixel*.
- Somerville v. White, 337 Ga. App. 414 (Ga. Ct. App. 2016).
- Stoner v. California, 376 U.S. 483 (1964).
- Tennessee v. Lane, 541 U.S. 509 (2004).
- University of Washington Center for Human Rights. (2025). *Leaving the door wide open: Flock surveillance systems expose Washington data to immigration enforcement*. <https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/>.
- Van Buren v. United States, 593 U.S. 374 (2021).