

COMPARATIVE STATE LAW ANALYSIS

Digital Rights, Government Technology, and Surveillance

Executive Summary

A review of selected state statutes shows that the principal safeguards proposed in the South Carolina Digital Liberty and Government Technology Accountability Act are not without state-law analogues. States already regulate discrete components of governmental technology through warrant requirements for digital information, limits on automated license plate readers (“ALPRs”), human review of governmental artificial-intelligence decisions, impact assessments for high-risk automated systems, access logging, data minimization, retention limits, vendor restrictions, public reporting, suppression remedies, and private enforcement.

What appears comparatively distinctive about the proposed South Carolina framework is not primarily the existence of those individual safeguards, but their consolidation into a single technology-neutral statute governing governmental power by function and effect. The proposed Act applies common constitutional-accountability principles across protected digital information, surveillance technology, artificial intelligence, biometrics, automated decision systems, contractors, shared systems, and other high-consequence governmental technologies.

Six states provide particularly useful enacted-law comparators: Virginia, Maine, Vermont, Montana, Colorado, and California. Washington is additionally useful as a legislative comparator because several proposals illustrate approaches to algorithmic impact assessment and governmental automated-decision-system accountability, but those proposals should not be characterized as enacted Washington law.

The comparison suggests four principal findings:

First, South Carolina would not be legislating in an unexplored field. Virginia and Maine impose detailed statutory restrictions on ALPRs; Maine and Vermont require warrants for categories of electronic information; Montana requires human review of governmental AI recommendations affecting legal rights or privileges; Colorado regulates high-risk AI through impact assessments and disclosure; California requires ALPR access logging and provides private remedies.

Second, existing state statutes are generally technology-specific or subject-specific. ALPR rules govern ALPRs, drone rules govern drones, electronic-communications statutes govern specified electronic information, and AI statutes govern AI. South Carolina's proposed Act instead establishes baseline rules capable of applying when the underlying technology changes.

Third, several of the strongest provisions in the South Carolina proposal closely parallel safeguards already enacted elsewhere. Human review, audit trails, limited retention, vendor accountability, warrant requirements, minimization, transparency, and meaningful remedies all have identifiable state-law precedents.

Fourth, several South Carolina provisions appear comparatively more integrated or structurally distinctive, particularly government acquisition by proxy, aggregation of surveillance across systems and time, independent verifiability of high-consequence outputs, the prohibition against contracting away governmental oversight, treatment of material supply-chain and remote-control dependencies, and affirmative authorization for new categories of local surveillance technology.

I. Virginia — ALPR Accountability as a Detailed Statutory Model

Virginia enacted a comprehensive statewide law governing law-enforcement ALPR systems in 2025, effective July 1, 2025. The law is one of the strongest direct comparators to the surveillance, auditability, procurement, retention, vendor-accountability, and remedy provisions of the proposed South Carolina Act.

Virginia requires approved ALPR systems to be capable of purging system data after 21 days, while retaining audit-trail data for two years. Vendor certifications must address data sharing, deletion capability, audit trails, database updating, and state information-security standards. Agency contracts must establish agency ownership of the data and require vendor notification when third parties seek the records.

The statute also sharply limits permissible uses. Law enforcement may query ALPR data only for enumerated investigative and public-safety purposes. Every query must contain the information needed to create an audit trail, including the user, date and time, query information, purpose, offense type where applicable, and associated case or call number. Agencies must conduct internal audits at least every 30 days.

Virginia additionally requires agency ALPR policies, annual agency reporting, statewide aggregated reporting, public posting of policies and reports, data-security procedures, limits on interstate and commercial sharing, and measures promoting public awareness before or when a local system is implemented.

Its remedy structure is notable. Willful unauthorized querying or sharing is a Class 1 misdemeanor, and evidence obtained through specified statutory violations is inadmissible when offered by the Commonwealth. A system-generated notification also does not by itself constitute reasonable suspicion for a vehicle stop; an officer must independently develop reasonable suspicion or confirm the relevant vehicle information.

Comparison to South Carolina. Virginia supplies strong enacted precedent for several elements of proposed Sections [--90], [--100], [--130], [--140], and [--160]: detailed audit records, vendor obligations, retention/destruction, public transparency, security, and meaningful enforcement. South Carolina differs by making those accountability principles applicable to a much broader class of governmental technologies rather than only ALPR systems. The proposed South Carolina Act's audit provision, for example, reaches user identity, purpose/legal basis, queries, outputs, disclosures, administrative access, configuration changes, software/firmware changes, remote access, security events, and human reviewers.

II. Maine — Warrant Requirements, ALPR Limits, and Technology-Specific Digital Privacy

Maine provides an important comparator for the proposed South Carolina principle that governmental access to protected digital information should not escape constitutional process merely because the information resides with a third party.

Maine law generally prohibits a governmental entity from obtaining electronic-device location information without a valid search warrant, subject to defined exceptions. The statute covers current and prior location information generated, derived from, or obtained through operation of an electronic device.

Maine separately requires a warrant when government obtains electronic-device content information from electronic-communication or remote-computing providers, again subject to statutory exceptions.

The location statute also contains a notice regime: absent judicially authorized delay, government generally must notify an identifiable owner or user that location information was obtained and identify the nature of the inquiry, information obtained, and third-party provider from whom it was obtained.

Maine's ALPR statute is unusually restrictive. It begins with a general prohibition on ALPR use and then creates specified exceptions, including authorized law-enforcement uses. Law-enforcement ALPR use must be tied to official and legitimate purposes, and certain inputs must rest on specific and articulable facts, court orders, NCIC records, or official law-enforcement bulletins. Ordinary ALPR data that do not qualify as investigative/intelligence records generally may not be stored for more than 21 days. Violation is a Class E crime.

Comparison to South Carolina. Maine demonstrates enacted state-law precedent for treating electronic information held by intermediaries as subject to affirmative legal-process rules and for pairing surveillance authority with short retention periods and statutory penalties. South Carolina's proposed [--20] is broader in formulation: it applies whenever substantially equivalent direct governmental acquisition would require constitutional process, regardless of whether access is purchased, licensed, donated, shared, or provided by another governmental or private entity.

That makes the South Carolina proposal particularly significant in the commercial-data/data-broker context. Maine's statutes regulate identified categories and provider relationships; South Carolina's proposed rule would operate by constitutional equivalence rather than by enumerating each commercial source.

III. Vermont — Electronic Privacy, Surveillance Minimization, Drones, and Reporting

Vermont provides another useful example of multiple technology-specific safeguards operating alongside one another.

Under the Vermont Electronic Communication Privacy Act, law enforcement generally may not compel production of or access to protected user information from a service provider except pursuant to a warrant, recognized warrant exception, specific consent, qualifying emergency, and other enumerated circumstances.

Vermont's drone statute illustrates data minimization by design. When law enforcement lawfully uses a drone, it must operate the drone in a manner intended to collect data only about the surveillance target and avoid collection concerning other persons, homes, or areas. Facial-recognition or other biometric-matching technology may not be applied to data concerning non-target persons, homes, or areas. Evidence gathered in violation of the statute is inadmissible.

Vermont also requires annual reporting of law-enforcement drone use, including the number of deployments, incident type, information collected, rationale, investigations and arrests aided, incidental collection involving non-target persons or property, program cost, and funding source. The Department of Public Safety then reports that information to legislative committees.

Vermont's ALPR regime historically included operational restrictions, training/certification, retention and judicial preservation mechanisms; its current statutory structure is undergoing a legislatively prescribed transition associated with automated-law-enforcement provisions, making effective-date distinctions important when citing Vermont ALPR law.

Comparison to South Carolina. Vermont supplies particularly strong precedent for the principles behind South Carolina's newly added minimization provision, biometric safeguards, judicial-process requirements, transparency, and remedies. South Carolina differs by placing minimization within a general protected-digital-information framework rather than limiting it to a particular surveillance technology.

IV. Montana — Government AI and Meaningful Human Review

Montana enacted one of the clearest state-law analogues to the South Carolina proposal's independent-human-review requirement in 2025.

Montana Code § 2-21-104 provides that when an AI system produces a recommendation or decision for a governmental entity or state officer that could affect a person's rights, duties, privileges, or immunities, the recommendation or decision must be reviewed and remain subject to rejection or modification by a human in an appropriate responsible position.

Montana also prohibits governmental AI from being used for cognitive behavioral manipulation, unlawful discriminatory classification, malicious purposes, or surveillance of public spaces except for specified circumstances.

Government-produced AI material not reviewed by an appropriate human must carry an AI disclosure, and governmental public interfaces using AI generally must disclose the AI use, subject to specified law-enforcement exceptions.

Comparison to South Carolina. This is a particularly direct comparator to proposed [--60]. South Carolina likewise prohibits deprivation of significant legal interests through an automated decision system without due process and independent human review. But South Carolina goes further by defining what qualifies as independent review: the reviewer must possess actual authority to approve, reject, modify, or remand the determination; have access to information needed to evaluate its material basis; and possess sufficient practical ability to exercise independent judgment. Mere approval or confirmation of the machine's output does not qualify.

Accordingly, the principle of meaningful governmental human review already has enacted state precedent. South Carolina's proposed contribution is a more detailed statutory definition designed to prevent nominal or “rubber-stamp” review.

V. Colorado — High-Risk AI, Impact Assessments, and Risk Governance

Colorado's enacted AI framework provides a useful comparator for South Carolina's treatment of high-consequence governmental digital systems, although the statutes differ significantly in scope and regulatory purpose.

Colorado enacted SB 24-205 in 2024, establishing obligations for developers and deployers of “high-risk” AI systems used in consequential decisions. The statute uses risk-management duties, disclosures, documentation, and impact assessments to address reasonably foreseeable algorithmic-discrimination risks. It gives the Attorney General exclusive enforcement authority under the Colorado Consumer Protection Act.

Colorado's framework is primarily a high-risk-AI/consumer-protection model rather than a constitutional governmental-technology statute. Nonetheless, it demonstrates legislative use of concepts that also appear in the South Carolina proposal: defining consequential automated systems, requiring documentation about system purpose and operation, assessing foreseeable risks, requiring deployer/developer information exchange, and imposing renewed obligations when systems are materially modified.

Comparison to South Carolina. Proposed [--70] requires a Digital Systems Impact Assessment before initial deployment, renewal after the transition period, or material change of a high-consequence governmental digital system. The assessment addresses legal authority, data, retention, sharing, AI functions, human review, audit and verification, remote access, cloud/subcontractor dependencies, and material foreign ownership/access/control dependencies.

South Carolina therefore borrows no single Colorado model; rather, it applies the now-established concept of a pre-deployment impact assessment to governmental constitutional accountability, cybersecurity, oversight, procurement, and system control—not merely algorithmic discrimination.

VI. California — ALPR Audit Trails, Privacy Policies, Security, and Private Remedies

California's existing ALPR statute provides another useful enacted comparator.

California Civil Code § 1798.90.52 requires ALPR operators that access or provide access to ALPR information to maintain access records identifying the date/time, query information, user and affiliated organization, and purpose of access. ALPR information may be used only for authorized purposes identified in the required usage and privacy policy.

California also provides a private civil remedy for individuals harmed by specified ALPR violations. Available relief can include actual damages subject to a statutory liquidated-damages floor, punitive damages for willful or reckless conduct, attorney's fees and costs, and equitable relief.

California is currently considering SB 1013, which as of August 27, 2026 remained pending rather than enacted. The current proposal would substantially strengthen ALPR restrictions, including archive/retention rules, warrant requirements for querying archived information, additional access-log requirements, and other controls. Those provisions are useful evidence of current legislative direction but must not be described as existing California law unless enacted.

Comparison to South Carolina. California demonstrates precedent for legislatively requiring detailed access records and creating enforceable individual remedies. South Carolina's proposed Act generalizes auditability beyond ALPRs and would permit declaratory/injunctive relief, record-preservation orders, attorney's fees, and other remedies while expressly leaving immunity and damages mechanics for Legislative Council reconciliation.

VII. Washington — Useful Legislative Comparator, but Not Enacted Law

Washington illustrates why enacted law and legislative proposals must be kept separate in this analysis.

Washington lawmakers have repeatedly considered automated-decision-system accountability legislation. HB 1951 in the 2023–24 session proposed annual impact assessments addressing system purpose, outputs, data, foreseeable discrimination risks, safeguards, human involvement, and validity/relevance testing.

Earlier SB 5116 proposed algorithmic-accountability reports for public agencies, minimum requirements for governmental development/procurement/use of automated decision systems, inventories, review, and auditing by the state's technology office.

These proposals are useful conceptual comparators to South Carolina's impact-assessment, inventory, procurement, and auditability provisions, but they should be labeled proposed legislation, not Washington statutory law.

Cross-State Comparison by Principle

Principle	Existing comparator	Relationship to proposed South Carolina framework
Government access to digital information	Maine and Vermont impose warrant/process requirements for specified electronic information.	SC proposes a technology-neutral rule based on whether equivalent direct governmental acquisition would require constitutional process.
Government acquisition by proxy/data intermediary	Existing electronic-privacy statutes regulate access through service providers.	SC's explicit anti-circumvention/proxy rule is broader and comparatively distinctive.
ALPR retention	Virginia: 21 days for ordinary system data; Maine: generally 21 days for non-investigative data.	SC uses a general necessity/proportionality and lawful-purpose framework rather than setting a single technology-specific retention period.
Auditability	Virginia requires detailed query audit trails and 30-day internal audits; California requires ALPR access records.	SC generalizes detailed auditability across high-consequence governmental systems.
Meaningful human review	Montana expressly requires human review with authority to reject or modify AI	SC defines independent human review more comprehensively and applies

	recommendations affecting rights or privileges.	it to automated governmental decisions affecting substantial legal interests.
Impact assessment	Colorado enacted high-risk-AI impact-assessment obligations; Washington has considered broader ADS assessments.	SC's assessment uniquely combines legal authority, data, human review, verification, cybersecurity, remote access, vendors and foreign dependencies.
Data minimization	Vermont drone law requires collection to be directed at the surveillance target and avoidance of incidental collection.	SC establishes a general minimization/retention principle for protected digital information.
Biometrics	Vermont limits biometric matching of incidentally collected drone data; Montana limits AI surveillance of public spaces.	SC incorporates biometrics into the general digital-rights/high-consequence framework.
Vendor accountability	Virginia imposes vendor certifications, deletion capability, security requirements, data-ownership terms and third-party-request notification.	SC generalizes contractor responsibility and adds supply-chain, remote-management, COTS, cloud and foreign-dependency review.
Transparency/public reporting	Virginia requires public ALPR policies/reports; Vermont requires legislative drone reporting; Montana requires governmental AI disclosures.	SC combines inventories, impact assessments, governing policies and lawful oversight across technology categories.
Remedies	Virginia provides criminal penalties and suppression; Vermont provides suppression for unlawful drone evidence; California provides private ALPR remedies.	SC proposes a general equitable-remedy/fees framework while reserving immunity and damages mechanics for Legislative Council.

Areas in Which the South Carolina Proposal Appears Comparatively Distinctive

The comparative research supports describing several features as distinctive in combination, while avoiding the stronger claim that no other state has enacted anything similar.

Government-by-proxy. Proposed [--40] expressly prevents government from using private persons, vendors, contractors, purchased services, or intermediaries to accomplish acquisition, surveillance, analysis, or processing that would require constitutional or statutory process if government performed it directly. The surveyed statutes generally regulate particular provider relationships or technologies rather than articulate this as a cross-technology rule.

Aggregation doctrine. Proposed [--30] directs attention to surveillance in the aggregate—including duration, precision, persistence, retrospective capability and aggregation across sources—and prevents constitutional requirements from being avoided by dividing surveillance among devices, databases, entities, contractors, or time periods. That systems-level treatment is broader than the technology-specific surveillance statutes surveyed.

Independent verifiability. Proposed [--80] provides that a high-consequence governmental system cannot serve as the sole nonverifiable authoritative evidence of the correctness of its own material output, and requires verification sufficiently independent of the failure mode being examined. Certification, accreditation, procurement acceptance, or technical-standard compliance does not itself establish the correctness of a particular governmental outcome. This is one of the proposal's more unusual features; the surveyed AI laws focus more commonly on risk, discrimination, disclosure, or human review.

Oversight that cannot be contracted away. Proposed [--110] prevents contracts, licenses, NDAs, and hosting arrangements from blocking courts, legislative committees, the Attorney General, auditors, inspectors general, or other authorized oversight bodies from obtaining information necessary to determine compliance. Virginia's ALPR vendor provisions demonstrate the underlying concern in a narrower technology-specific setting, but South Carolina would establish the principle generally.

Supply-chain and operational-control accountability. Proposed [--100] reaches hardware, software, firmware, communications, wireless access, remote management, update authority, cloud services, subcontractors, data storage, material COTS components, country-of-origin information when reasonably ascertainable, and foreign access/control/operational dependencies—while expressly stating that a foreign-manufactured component alone does not

prove compromise or unreliability. This is broader than the principal civil-liberties and AI statutes identified in this survey.

Judiciary Takeaway

The comparative record supports a careful characterization of the proposed South Carolina Act:

South Carolina would not be creating the underlying concepts from whole cloth. Other states have already enacted warrants for digital information, ALPR retention limits, audit trails, governmental AI human review, impact assessments, minimization rules, vendor requirements, public reporting, suppression, civil remedies, and other technology-accountability safeguards.

What South Carolina's proposal does differently is organize many of those principles into a unified constitutional-governance framework. Instead of requiring the General Assembly to legislate separately every time a new camera, algorithm, database, biometric technique, AI system, commercial-data source, or vendor architecture emerges, the proposed Act establishes baseline rules governing governmental acquisition, consequential decision-making, verification, auditability, contracting, retention, oversight, and remedies according to the function and effect of governmental power.

That distinction is important. The comparative state-law record suggests that technology-specific legislation can provide strong protections—Virginia's 2025 ALPR statute is an especially clear example—but it also produces a patchwork in which different technologies are governed by different statutes enacted at different times. South Carolina's proposed framework attempts to establish the common accountability layer beneath those technology-specific rules while allowing the General Assembly to enact additional safeguards for particular technologies when warranted.

For legislative drafting purposes, the strongest enacted comparators are therefore Virginia for ALPR auditability/vendor accountability/remedies; Maine for warrants and retention; Vermont for minimization, surveillance process, and reporting; Montana for meaningful governmental human review; Colorado for high-risk-system impact assessment; and California for access logging and private enforcement.

Virginia ALPR statute — Va. Code § 2.2-5517

Maine ALPR statute — 29-A M.R.S. § 2117-A

Maine electronic-location warrant statute — 16 M.R.S. § 648

Vermont Electronic Communication Privacy Act

Vermont law-enforcement drone statute

Montana Government Use of Artificial Intelligence statutes

Colorado SB 24-205 — Consumer Protections for Artificial Intelligence

California ALPR access-log statute — Civil Code § 1798.90.52

NCSL Artificial Intelligence Legislation Database — updated September 1, 2026

Status note: This draft distinguishes enacted statutes from pending proposals based on sources checked through September 23, 2026. California SB 1013 and the Washington measures discussed above are included only as legislative comparators and are not represented as enacted law.