

LEGISLATIVE INITIATIVES

Implementation Priorities

These initiatives translate the legislator-circulated South Carolina Digital Bill of Rights framework into practical legislative work while keeping the vehicle focused on digital rights and governmental technology accountability.

1. Technology-Neutral Digital Rights Framework

Create a technology-neutral statutory framework governing protected digital information, governmental surveillance, automated decisions, high-consequence governmental digital systems, auditability, procurement, oversight, records, security, and remedies.

Constitutional protections should neither expand nor diminish solely because technology evolves. Implementing legislation should be capable of governing existing technologies and technologies not yet developed.

2. Government Acquisition by Proxy / Commercial Data

Prevent government from purchasing, licensing, querying, requesting, or receiving protected digital information through data brokers, vendors, contractors, shared systems or other intermediaries where substantially equivalent direct governmental acquisition would require constitutional or statutory process.

Covered information should include, as appropriate under implementing legislation, location and movement history, license plate history, communications information, biometric information, consumer profiles, advertising identifiers, behavioral analytics, data-broker information, and other protected digital information.

Government should not accomplish indirectly through private companies, contractors, vendors, artificial intelligence systems, surveillance networks, data brokers, or other intermediaries what it is prohibited or constitutionally restricted from doing directly.

3. Surveillance Authorization and Public Accountability

Require affirmative authorization, governing policies, access controls, retention rules, audit logs, public inventories, and periodic review for designated surveillance technologies, while

preserving express and narrowly defined investigative, emergency, and security exceptions consistent with constitutional requirements.

Evaluate appropriate aggregate public reporting concerning surveillance-system use, including, where feasible and consistent with legitimate investigative and security protections:

- categories of surveillance technology in use;
- vendor contracts and material data-sharing arrangements;
- categories of information collected;
- retention periods;
- audit procedures;
- aggregate search or query activity;
- aggregate warrant or judicial-process activity; and
- aggregate use of surveillance information in investigations.

Transparency requirements should protect legitimate investigative methods, security-sensitive information, legally protected information, and individual privacy while providing meaningful public accountability.

4. Digital Search and Constitutional Process Standards

Establish clear statutory standards for governmental access to protected digital information where constitutional or statutory process is required.

Address historical and aggregated information capable of revealing movement, location, travel patterns, communications, biometric characteristics, associations, or other sensitive aspects of a person's life while preserving constitutionally recognized exceptions, including lawful emergency authorities.

Third-party possession, commercial availability, contractual access, or technical capability should not, standing alone, extinguish the constitutional inquiry or create governmental authority that otherwise does not exist.

5. Data Minimization, Retention, and Disposition

Establish appropriate statutory standards governing governmental collection, retention, use, sharing, anonymization, and disposition of protected digital information.

Retention should be connected to lawful governmental purpose, legal requirements, evidentiary obligations, and legitimate operational needs.

Implementing legislation should consider reasonable limits on retaining information concerning individuals who are not connected to an investigation or other lawful governmental purpose, while preserving records required by law, litigation holds, evidentiary obligations, public-record requirements, and other legitimate governmental needs.

6. Individual Access, Accuracy, and Correction

Establish meaningful procedures, where consistent with legitimate law-enforcement needs and other legal protections, through which individuals may determine what covered governmental information is maintained about them and obtain appropriate information concerning its source, access, use, or sharing.

Provide procedures for individuals to challenge demonstrably inaccurate information and seek timely correction.

Where materially inaccurate information has been propagated to downstream governmental systems or recipients, establish appropriate correction or notification procedures while preserving independent legal record-retention requirements.

7. Biometric Information Protection

Establish enhanced statutory safeguards governing governmental collection, retention, use, sharing, analysis, and disclosure of biometric information.

Address facial geometry, fingerprints, palmprints, iris or retinal patterns, DNA profiles, voiceprints, gait, behavioral biometrics, biometric templates, embeddings, vectors, and other biometric identifiers as appropriate.

Biometric safeguards should account for the persistent nature of many biometric characteristics and the difficulty or impossibility of changing them after compromise.

8. High-Consequence System Integrity and Independent Verification

Apply function-based integrity standards to governmental digital systems that materially affect constitutional rights, liberty or property, law-enforcement action, taxation or financial obligations, benefits or services, licensing, governmental identification, civic participation, or other substantial legal interests.

Require material governmental outcomes to remain independently verifiable where required, without exclusive dependence upon the system, component, vendor, manufacturer, testing process, or certifying authority responsible for producing or validating the outcome.

Certification, testing, accreditation, procurement approval, or compliance with a technical standard should not, standing alone, substitute for independent verification or create a conclusive presumption of correctness, integrity, security, lawful operation, or compliance.

9. Automated Decisions and Due Process

Require independent human review, notice, explanation, correction, and meaningful challenge procedures when automated systems materially contribute to adverse governmental determinations affecting protected rights or substantial legal interests.

Government should not rely solely upon artificial intelligence or automated decision-making to make consequential governmental determinations affecting liberty, property, legal status, licenses, benefits, governmental services, or constitutional rights where meaningful human review is required.

Human review should be substantive rather than ceremonial and should permit an identified decision-maker with appropriate authority and information to independently evaluate, reject, correct, modify, or remand a material automated determination.

10. Government Technology Impact Assessments

Require appropriate impact assessment before deployment of designated high-consequence governmental digital systems or surveillance technologies and upon material change or other triggering events established by law.

Assessments should address, as applicable:

- legal authority;
- constitutional and privacy implications;
- categories and sources of data;
- automated or artificial-intelligence functions;
- human-review mechanisms;
- independent-verification mechanisms;
- cybersecurity risks;
- remote-access capabilities;
- cloud and subcontractor dependencies;
- material foreign ownership, access, control, or operational dependencies;
- expected governmental purpose and effectiveness; and
- reasonable alternative approaches where appropriate.

11.Auditability, Records, and Incident Accountability

Require reconstructable audit records, appropriate preservation requirements, protections against unauthorized alteration, deletion, concealment, or destruction, anti-spoilation rules, anti-spoilation rules, downstream correction where materially inaccurate information has been propagated, and timely incident response for covered systems.

Audit evidence should be sufficient, where applicable, to reconstruct material system activity, including administrative access, configuration changes, software or firmware versions and updates, data transfers, remote access, automated actions, errors, security events, and material human review.

12.Procurement, Vendor Accountability, Supply Chain, and Sovereignty

Require covered contracts and procurement processes to preserve audit and oversight access, identify material hardware, software, firmware, commercial off-the-shelf components, remote-access capabilities, update authority, cloud and subcontractor dependencies; address cybersecurity and data disposition; and evaluate material foreign ownership, access, control, or operational dependencies without treating foreign manufacture alone as proof of compromise.

Government contracts involving protected information or covered governmental systems should contain appropriate requirements addressing cybersecurity, unauthorized disclosure or resale, auditability, incident notification, lawful oversight, and disposition of information upon termination when appropriate.

Certification, testing, accreditation, procurement approval, or compliance with a technical standard should not, standing alone, substitute for independent verification or create a conclusive presumption of compliance.

Procurement authority should not be treated as substantive authority to exercise every capability of a purchased or licensed technology.

13. Children's Digital Rights

Evaluate enhanced protections for minors concerning governmental collection, retention, use, commercialization, sharing, and disclosure of children's protected digital information.

Implementing legislation should account for parental authority, lawful governmental responsibilities, education and child-protection requirements, legitimate public interests, and circumstances in which collection or disclosure is otherwise authorized by law.

Special consideration should be given to persistent identifiers, biometric information, profiling, automated decision-making, and other digital practices capable of creating long-term records concerning children.

14.Existing-Code Modernization

Review relevant South Carolina Code provisions governing electronic communications, privacy and public records, procurement, governmental data practices, criminal procedure, and related authorities to determine which provisions should be preserved, strengthened, modernized, amended, or conformed to the Digital Bill of Rights framework and South Carolina's constitutional protections.

15.ALPR and Future Surveillance Gaps

Address gaps in South Carolina law governing automated license plate readers and persistent surveillance while accounting for ALPR-specific legislation already under consideration.

Establish broader, technology-neutral rules capable of governing present and future persistent surveillance systems rather than relying exclusively upon statutes written around a particular technology, product, or vendor.

16.Open Fields and Private-Land Surveillance Reform

Review S.C. Code §50-3-420 and other relevant law governing governmental investigative entry onto privately owned land beyond curtilage and technology-assisted surveillance of private land.

Distinguish physical entry from technology-assisted surveillance; define the roles of warrants, owner consent, emergencies, and other lawful authority; and establish technology-neutral protections applicable to cameras, audio devices, unmanned aircraft, remote sensors, and future surveillance methods.

17.Image, Voice, and Likeness / Photo-Consent Reconciliation

Review H.3404 and related law to preserve the distinction between ownership of an expressive work and legal interests in a person's name, photograph, voice, likeness, biometric information, or information derived from that work.

Address commercial exploitation, unauthorized synthetic or biometric uses, minors, consent, news and public-interest uses, expressive activity, and First Amendment protections without

converting ordinary photography or recording into an automatic transfer of ownership or a blanket consent requirement.

Legislative Approach

The goal is not to prohibit useful technology or prevent government from carrying out legitimate and lawful functions.

The goal is to ensure that governmental power remains traceable to lawful authority, subject to constitutional process, independently verifiable where required, auditable, reviewable, and accountable regardless of the technology, component, vendor, contractor, or intermediary involved.

Implementation may occur through a comprehensive statutory framework, targeted companion legislation, modernization of existing Code provisions, or a combination of these approaches where appropriate.

Technology changes. Rights do not.