DIGITAL LIBERTY AND GOVERNMENT TECHNOLOGY ACCOUNTABILITY ACT

Purpose

To establish a technology-neutral statutory framework governing governmental acquisition and use of protected digital information, surveillance technology, automated decision systems, biometrics, and other high-consequence governmental digital systems, while preserving the independent force of the United States Constitution and the South Carolina Constitution.

Core Judiciary Questions

- Does government possess lawful authority for the technological use at issue?
- Would the same acquisition require constitutional process if government obtained the information directly?
- Can a consequential governmental output be independently verified rather than accepted solely because a machine produced it?
- Is an accountable human decision-maker available when automation materially affects a person's rights or legal interests?
- Can courts and lawful oversight bodies obtain the records necessary to determine compliance?
- Was a new category of systematic surveillance affirmatively authorized rather than merely purchased or placed in a budget?

Policy Scope

The Act is intentionally vendor-neutral and technology-neutral. It applies the same constitutional accountability principles to covered surveillance systems, data-broker acquisitions, artificial intelligence, biometric systems, digital identity systems, and other high-consequence governmental technologies.

A BILL

TO AMEND THE SOUTH CAROLINA CODE OF LAWS BY ADDING A NEW CHAPTER, AT A CODE LOCATION TO BE DESIGNATED BY LEGISLATIVE COUNCIL, SO AS TO ENACT THE "SOUTH CAROLINA DIGITAL LIBERTY AND GOVERNMENT TECHNOLOGY ACCOUNTABILITY ACT"; TO ESTABLISH REQUIREMENTS GOVERNING GOVERNMENTAL ACQUISITION AND USE OF PROTECTED DIGITAL INFORMATION, SURVEILLANCE TECHNOLOGY, AUTOMATED DECISION SYSTEMS,

BIOMETRIC INFORMATION, AND HIGH-CONSEQUENCE GOVERNMENTAL DIGITAL SYSTEMS; TO PROHIBIT CIRCUMVENTION OF CONSTITUTIONAL REQUIREMENTS THROUGH THIRD PARTIES; TO PROVIDE FOR HUMAN REVIEW, INDEPENDENT VERIFIABILITY, AUDITABILITY, RECORD PRESERVATION, PROCUREMENT AND SUPPLY-CHAIN DISCLOSURES, PUBLIC TRANSPARENCY, AND AFFIRMATIVE AUTHORIZATION FOR CERTAIN TECHNOLOGIES; TO PROVIDE REMEDIES AND RULES OF CONSTRUCTION; AND FOR OTHER PURPOSES.

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. Short title.

This act may be cited as the "South Carolina Digital Liberty and Government Technology Accountability Act."

SECTION 2. Legislative findings and purpose.

The General Assembly finds that:

(1) the liberties secured by the Constitution of the United States and the Constitution of the State of South Carolina do not diminish because technology evolves;

(2) Article I, Section 10 of the Constitution of South Carolina expressly protects the people against unreasonable searches and seizures and unreasonable invasions of privacy and requires particularity concerning the information to be obtained;

(3) technological capability does not itself create governmental authority;

(4) governmental use of private contractors, technology vendors, data brokers, artificial intelligence providers, or other intermediaries must not be used to circumvent constitutional limitations;

(5) governmental systems materially affecting constitutional rights or substantial legal interests must remain subject to independent human review, independent verification, auditability, and lawful oversight; and

(6) procurement, possession, or technical capability of a technology does not, standing alone, constitute authorization for every governmental use of that technology.

This act must be construed to preserve constitutional liberty. Exceptions affecting rights protected by this act must be expressly stated and narrowly construed.

SECTION 3. The South Carolina Code is amended by adding a chapter, at a location to be designated by Legislative Council, to read:

"CHAPTER [--]

Digital Liberty and Government Technology Accountability

DRAFTING NOTE: Code placement and section numbering are provisional. Legislative Council should assign this Act to an appropriate available chapter of the South Carolina Code and conform all internal cross-references accordingly.

Section [--10]. Definitions

(1) "Automated decision system" means a computational process, including artificial intelligence, machine learning, statistical modeling, or another data-processing technique, that makes, recommends, ranks, scores, classifies, predicts, authenticates, or materially assists a governmental determination.

(2) "Biometric information" means data generated from biological, physiological, or behavioral characteristics for identification or persistent recognition, including facial geometry, fingerprints, palmprints, iris or retinal patterns, DNA profiles, voiceprints, gait, behavioral biometrics, keystroke patterns, device-interaction patterns, physiological identifiers, templates, embeddings, or vectors.

(3) "Governmental entity" means the State, an agency, department, board, commission, authority, political subdivision, county, municipality, school district, special purpose district, law enforcement agency, or other public body, and a person or entity acting on behalf of one of them in performing a covered governmental function.

(4) "High-consequence governmental digital system" means an automated, algorithmic, electronic, computational, or digital system that makes, records, calculates, authenticates, determines, recommends, transmits, certifies, or materially influences an official governmental action or determination affecting a constitutional right, liberty or property, legal status, law-enforcement action, taxation or financial obligation, eligibility for public benefits or essential governmental services, professional or occupational licensing, governmental identification, civic participation, or another substantial legal interest designated by law.

(5) "Independent human review" means review by an identified natural person who has actual authority to approve, reject, modify, or remand a proposed governmental determination; access to information reasonably necessary to evaluate the material basis of the automated output; and training reasonably appropriate to the nature of the determination and sufficient time and practical ability to exercise independent judgment before final action. Mere approval, acknowledgment, transmission, execution, or confirmation of an automated output does not constitute independent human review.

Legislative Council note: Evaluate whether the training language should remain an element of the definition or instead become an implementation requirement.

(6) "Material change" means a substantial change in a covered system's capability or effect, including a substantial change in data categories, analytical functions, interoperability, retention, sharing, surveillance reach, decision-making use, remote administration, software or firmware

authority, update authority, authentication or cryptographic trust, material component architecture, material vendor or subprocessor arrangements, or material foreign operational dependency.

Routine maintenance, security patches, and updates that do not substantially alter capability or effect or materially alter system control, trust, or security dependencies are not material changes.

(7) "Protected digital information" means digital information generated by, derived from, or uniquely linked to an individual's identity, body, communications, precise or historical location, associations, private activities, biometric characteristics, authentication information, financial or medical information, browsing or search activity, behavioral information, or an aggregated profile, inference, score, prediction, or dossier substantially derived from such information. The term includes a transformed, tokenized, pseudonymized, embedded, scored, classified, predicted, or inferred representation when it remains reasonably linkable to a person or materially reveals substantially equivalent protected facts.

(8) "Surveillance technology" means hardware, software, or a service principally capable of monitoring, identifying, locating, tracking, recognizing, profiling, predicting, or reconstructing the movements, associations, communications, characteristics, or activities of a person or group.

Section [--20]. Constitutional process for protected digital information.

(A) A governmental entity may not search, seize, compel, acquire, purchase, license, query, access, request, receive, retrieve, or otherwise obtain protected digital information when substantially equivalent direct governmental acquisition would require a warrant or other judicial process unless the governmental entity first obtains the constitutionally required process or the acquisition falls within a constitutionally recognized exception.

(B) Subsection (A) applies without regard to whether access is paid or unpaid, purchased, licensed, donated, provided through a trial or demonstration, obtained through a shared account, or supplied by another governmental or private entity.

(C) Third-party possession, commercial availability, contractual access, or consent of a custodian does not independently establish governmental authority to obtain information otherwise protected by the Constitution of the United States or the Constitution of the State of South Carolina.

(D) A contract, procurement action, possession of technology, or technical capability does not create substantive governmental authority that the Constitution or laws of this State do not otherwise provide.

Section [--30]. Aggregated surveillance.

(A) A governmental entity may not avoid a constitutional or statutory requirement by dividing substantially continuous, aggregated, historical, retrospective, or persistent surveillance among separate observations, searches, queries, devices, databases, governmental entities, contractors, or periods of collection.

(B) In determining whether surveillance implicates a constitutional or statutory protection, a court may consider the surveillance activity and resulting information in the aggregate, including duration, precision, continuity, persistence, retrospective capability, aggregation across sources, and the extent to which the resulting information reveals or reconstructs a person's movements, associations, activities, habits, or private life.

Section [--40]. Government acquisition by proxy.

A governmental entity may not employ, direct, request, contract with, purchase from, license from, query through, receive from, or otherwise use a private person or entity to accomplish governmental acquisition, surveillance, analysis, or processing that would be subject to constitutional or statutory process if conducted directly.

Section [--50]. Shared, federated, and intergovernmental systems.

(A) Constitutional and statutory requirements apply to covered governmental access through shared, federated, regional, interstate, intergovernmental, or privately operated systems to the same extent they would apply to substantially equivalent direct access.

(B) A governmental entity may not avoid a requirement of this chapter by requesting or causing another governmental entity, contractor, vendor, or intermediary to conduct a search, query, acquisition, or analysis on its behalf.

Section [--60]. Automated governmental decisions.

(A) A governmental entity may not deprive a person of life, liberty, property, employment, a license, public benefit, constitutional right, legal protection, or another substantial legal interest through an automated decision system without due process of law and independent human review.

(B) When an automated decision system materially contributes to an adverse governmental determination, the affected person must receive appropriate notice and a reasonable opportunity to challenge material factual or computational error, subject to an exception expressly provided by law.

(C) A human reviewer may not be required by policy, procedure, technical design, performance metric, or directive to accept an automated output without independent evaluation of its material basis.

Section [--70]. High-consequence systems; impact assessment and continuing review.

(A) Before first deploying, renewing after the applicable transition period, or materially changing a high-consequence governmental digital system, a governmental entity shall complete and retain a Digital Systems Impact Assessment.

(B) The assessment must identify, to the extent applicable: governmental purpose; legal authority; vendor or provider; categories of data collected, derived, or generated; retention and sharing practices; material automated or artificial-intelligence functions; independent-human-review process; audit and verification mechanisms; remote-access and network capabilities; material cloud or subcontractor dependencies; and material foreign ownership, access, control, or operational dependencies relevant to security or accountability.

(C) Security-sensitive information may be withheld from public disclosure to the extent otherwise authorized by law, but must remain available to a court or governmental oversight authority lawfully entitled to review it.

Section [--80]. Independent verifiability.

(A) A high-consequence governmental digital system may not constitute the sole nonverifiable authoritative evidence of the correctness of its own material output.

(B) When independent verification is required, the verifying evidence or method must be sufficiently independent of the material failure mode under examination to permit detection of a material error, fault, compromise, or unauthorized alteration.

(C) Where reasonably practicable, the governmental entity shall maintain evidence independent of the system sufficient to verify a material governmental outcome without exclusive dependence on the software, algorithm, device, manufacturer, vendor, contractor, network, or digital system under examination.

(D) Certification, testing, accreditation, approval, procurement acceptance, or compliance with a technical standard does not, standing alone, constitute independent verification of a material governmental outcome or create a conclusive presumption of the correctness, integrity, security, or lawful operation of a system or component.

Section [--90]. Auditability and record integrity.

(A) A covered high-consequence system must create and preserve sufficient contemporaneous audit evidence to permit lawful review of material governmental access, use, and administration.

(B) Audit evidence must include, as applicable, the identity or accountable role of a user; date and time; documented purpose or legal basis; material query or input; material output or action; disclosure or export; privileged and administrative access; configuration changes; software or firmware versions and material modifications; material data imports, transfers, and deletions; network and remote-access events; errors and exceptions; material security events; and the identity of a required human reviewer.

(C) Required audit records must be protected against unauthorized alteration, deletion, concealment, or destruction and retained for the period required by applicable law or a retention schedule sufficient to support statutory and constitutional review.

(D) A governmental entity may not rely on the absence of a vendor- created log or system configuration as a defense to a statutory duty to create or preserve audit evidence.

Section [--100]. Procurement, contractors, and supply-chain accountability.

(A) Delegation of a governmental technological function to a contractor, vendor, manufacturer, cloud provider, or other third party does not diminish governmental responsibility for constitutional or statutory compliance.

(B) Before acquiring or materially changing a designated high-consequence governmental digital system, a governmental entity shall obtain information reasonably sufficient to understand material hardware, software, firmware, communications, wireless, remote-management, update, cloud, subcontractor, data-storage, and foreign access, control, or operational dependencies relevant to security or accountability.

(C) Procurement requirements may include a software bill of materials, hardware or component inventory, including identification of material commercial off-the-shelf components, country-of-origin information when reasonably ascertainable, and substantially equivalent supply-chain documentation.

(D) The presence of a foreign-manufactured component, standing alone, does not establish compromise, unlawful conduct, or system unreliability.

Section [--110]. Oversight may not be contracted away.

(A) A governmental entity may not enter a contract, license, nondisclosure agreement, hosting arrangement, or other agreement that prevents a court, the General Assembly or an authorized committee, the Attorney General, the State Auditor, the State Inspector General when otherwise within jurisdiction, or another governmental oversight authority lawfully entitled to review information from obtaining information reasonably necessary to determine constitutional or statutory compliance.

(B) A contract for a covered system must preserve governmental access to compliance records reasonably necessary for lawful audits, investigations, litigation holds, public-record obligations, and constitutional or statutory review.

(C) Legitimate trade-secret and security-sensitive information may be protected from unnecessary public disclosure without restricting lawful oversight access.

Section [--120]. Authorization of new surveillance technology.

DRAFTING NOTE: Evaluate whether an analogous affirmative-authorization mechanism should apply to State agencies deploying a new category of surveillance technology. Any State-level mechanism should reflect the different governance structure of State agencies rather than mechanically applying the political-subdivision public-meeting process.

(A) A political subdivision may not deploy a new category of surveillance technology, or materially change an existing category into a substantially new use, without affirmative approval by its governing body at a public meeting.

(B) Before approval, publicly available materials must identify the category and purpose of the technology, vendor or provider, anticipated cost, categories of information collected or generated, retention and sharing rules, governing policy, and proposed duration or renewal term.

(C) Inclusion of an expenditure in an annual budget, standing alone, does not satisfy this section unless the technology and proposed governmental use are specifically identified in publicly available budget materials.

(D) An emergency exception must be expressly authorized by law, based on objective criteria, and narrowly limited by necessity, scope, and duration. Use under an emergency exception must be documented and subject to retrospective review as provided by law.

Section [--130]. Public technology inventory.

Each governmental entity operating a high-consequence governmental digital system or surveillance technology subject to Section [--120] shall maintain a publicly accessible inventory identifying, to the extent disclosure is not otherwise lawfully restricted, the technology category, vendor, purpose, legal authority, acquisition or subscription cost, categories of data, retention period, sharing policy, governing policy, and date of approval.

Section [--140]. Data minimization, retention, security, correction, and preservation.

(A) A governmental entity entrusted with protected digital information shall employ reasonable administrative, technical, and physical safeguards against unauthorized disclosure, access, alteration, destruction, or misuse.

(B) A person must receive timely notice when protected personal information concerning that person is materially compromised through a governmental data breach, except when a temporary delay is authorized by law for a legitimate investigative or security purpose.

(C) Records required for constitutional review, statutory compliance, audit, verification, litigation, investigation, or public oversight may not be destroyed, altered, concealed, or permitted to expire contrary to an applicable preservation requirement.

(D) A governmental entity shall limit the collection, generation, retention, use, and dissemination of protected digital information to that reasonably necessary and proportionate to a lawful governmental purpose. Protected digital information may not be retained longer than reasonably necessary for that purpose unless retention is required or authorized by law, court order, applicable records-retention schedule, litigation hold, evidentiary obligation, audit or oversight requirement, or another lawful preservation requirement. When protected digital information is no longer reasonably necessary for a lawful governmental purpose and no independent legal duty requires its preservation, the governmental entity shall securely delete, destroy, anonymize, or otherwise dispose of the information in accordance with applicable law.

(E) Where required by law or ordered as equitable relief, a governmental entity must provide a practicable process for correction, deletion, restriction, or downstream notice concerning unlawfully maintained or disseminated protected digital information, subject to independent record-preservation duties.

Section [--150]. Anti-circumvention.

A governmental entity may not accomplish indirectly, through technological configuration, contractual arrangement, intermediary, contractor, shared system, derived information, division of governmental functions, or substantially equivalent means, what this chapter prohibits or conditions when accomplished directly.

Section [--160]. Remedies.

(A) A person aggrieved by a material violation of this chapter may seek declaratory or injunctive relief in a court of competent jurisdiction.

(B) A court may order preservation of relevant records and other equitable relief necessary to prevent or remedy an ongoing violation.

(C) A prevailing plaintiff may be awarded reasonable attorney's fees and litigation costs as determined by the court.

(D) A person challenging failure to comply with an affirmative procedural requirement concerning authorization, transparency, auditability, preservation, security, procurement, independent human review, or independent verification need not first prove that the underlying technology produced an erroneous substantive outcome.

(E) For a knowing or willful substantive violation, the court may award actual damages and any statutory damages expressly provided by law.

DRAFTING NOTE: Legislative Council should evaluate whether the final legislation should specify a unit of violation and appropriate limitations necessary to avoid unintended multiplication of liability.

(F) A cure period may be provided by law for designated non-willful administrative defects but may not excuse ongoing unlawful acquisition, access, use, disclosure, deliberate concealment, destruction of required evidence, or continued substantive conduct after notice.

(G) When another provision of law authorizes damages, suppression, exclusion, administrative relief, or another remedy, nothing in this chapter limits that remedy.

(H) Any reliance or good-faith defense created by law must rest on objectively reasonable reliance on valid legal authority; vendor representations, procurement approval, administrative custom, or technical capability alone are insufficient.

[(I) REMEDIES/IMMUNITY PROVISION TO BE CONFORMED BY LEGISLATIVE COUNCIL: The final provision should preserve the express remedies authorized by this section while addressing applicable sovereign, governmental, and official immunity law and avoiding unintended personal liability for ordinary employees acting within the lawful scope of assigned duties.]

DRAFTING NOTE: Legislative Council should reconcile standing, declaratory and injunctive relief, attorney's fees and costs, damages, sovereign/governmental/official immunity, and existing statutory remedies so that the remedies expressly enacted by the General Assembly are legally effective without creating unintended personal liability.

Section [--170]. Construction.

(A) This chapter does not authorize conduct that would otherwise violate the Constitution of the United States or the Constitution of the State of South Carolina.

(B) Compliance with a minimum safeguard established by this chapter does not establish the constitutionality of conduct otherwise prohibited by law.

(C) No exception to a right protected by this chapter may be implied solely from technological capability, commercial availability, private ownership of infrastructure, contractual consent by another person, third-party possession, automation, administrative convenience, or technological novelty.

(D) An exception created by implementing legislation must be expressly stated, narrowly tailored, and no broader than constitutionally permissible for the purpose it serves.

(E) This chapter establishes minimum protections and does not preempt a political subdivision from adopting greater protections when otherwise authorized by law.

(F) Nothing in this chapter may be construed to require conduct prohibited by federal law or to supersede federal law to the extent federal law preempts state law.

SECTION 4. Severability.

If a provision of this act or its application to a person or circumstance is held invalid, the invalidity does not affect another provision or application that can be given effect without the invalid provision or application, and to this end the provisions of this act are severable.

SECTION 5. Effective date.

This act takes effect one hundred eighty days after approval by the Governor. A governmental entity operating a covered system on the effective date has twelve months from the effective date to complete an initial inventory and impact assessment required by this act, unless a shorter period is required by other law. The additional period provided for completion of an initial inventory or impact assessment does not delay the applicability of another substantive requirement of this act unless expressly provided by law.