

# **THE SOUTH CAROLINA BILL OF DIGITAL RIGHTS**

*Complete Constitutional and Legislative Development Package*

Version 1.0

September 2026

First Publication

## **Authors**

**Brittany Farr**

**Valerie McCarthy**

*“Technology changes. Rights do not.”*

© 2026 Brittany Farr and Valerie McCarthy

Permission is granted to reproduce and distribute this work, in whole or in part, for educational, legislative, governmental, and other non-commercial purposes, provided attribution to the original authors is maintained, any modifications are clearly identified, and this notice is retained with the reproduced work.

Commercial reproduction or distribution without the authors' written permission is prohibited.

# TABLE OF CONTENTS

## *South Carolina Bill of Digital Rights* **Judiciary Implementation Packet**

---

|                                                                                                                                  |    |
|----------------------------------------------------------------------------------------------------------------------------------|----|
| <b>Legislative Executive Brief</b>                                                                                               | 2  |
| <b>South Carolina Digital Bill of Rights</b>                                                                                     | 4  |
| <b>The Case for a South Carolina Bill of Digital Rights</b><br><i>White Paper</i>                                                | 12 |
| <b>Legislative Initiatives</b>                                                                                                   | 20 |
| <b>Digital Liberty and Government Technology Accountability Act</b><br><i>Draft for Legislative Council and Judiciary Review</i> | 27 |
| <b>Section-by-Section Judiciary Summary</b>                                                                                      | 38 |
| <b>Existing Law &amp; Pending Legislation Review</b><br><i>Implementation and Reconciliation Memorandum</i>                      | 40 |
| <b>Legislative Counsel and Judiciary Checklist</b><br><i>Matters Requiring Drafting or Committee Review</i>                      | 49 |
| <b>Primary Authorities and Source Notes</b><br><i>Constitutional, Statutory, Legislative, and Case Authorities</i>               | 56 |
| <b>Comparative State Law Analysis</b>                                                                                            | 60 |
| <b>South Carolina Digital Bill of Rights — Frequently Asked Questions</b>                                                        | 73 |

# LEGISLATIVE EXECUTIVE BRIEF

## Decisions Requested of the General Assembly

### Purpose

The South Carolina Digital Bill of Rights is the constitutional framework already circulated to South Carolina legislators. This Judiciary packet develops the legislative implementation and supporting analysis necessary to translate that framework into enforceable South Carolina law.

### Five Decisions Requested of the General Assembly

- **Recognize the need for a technology-neutral statutory framework** protecting constitutional liberty as governmental surveillance, data acquisition, artificial intelligence, biometric systems, automated decision making, and other high-consequence digital technologies expand.
- **Direct Legislative Council and appropriate committees to evaluate statutory implementation** of the Digital Bill of Rights principles, including privacy, government acquisition by proxy, due process, independent human review, independent verification, auditability, procurement and supply chain accountability, records, transparency, oversight, and remedies.
- **Review existing South Carolina Code provisions** to identify laws that should be preserved, strengthened, modernized, amended, or conformed to the framework, while identifying conflicts, gaps, and provisions that no longer adequately address modern governmental technologies.
- **Address statutory gaps through affirmative, technology-neutral legislation**, including gaps involving automated license plate reader systems and other surveillance or high-consequence governmental technologies, rather than relying exclusively upon vendor-, product-, or technology-specific rules. Coordinate related legislative work where distinct issues—including private-land surveillance and image, voice, likeness, biometric, or children's digital-information protections—require separate or complementary statutory treatment.
- **Use the proposed Digital Liberty and Government Technology Accountability Act as a starting point for committee-ready legislation, Legislative Council refinement, and appropriate conforming amendments** that preserve legitimate governmental and law-enforcement functions while requiring lawful authority, constitutional process, accountable human decision-making, independently verifiable and auditable systems,

meaningful governmental oversight, procurement and supply-chain accountability, and enforceable remedies.

The objective is not to prohibit technological innovation or prescribe particular technologies.

It is to establish durable rules governing governmental power by **function and effect**, so that constitutional protections do not depend upon the technology, vendor, platform, component, or system through which governmental power is exercised.

# THE SOUTH CAROLINA BILL OF DIGITAL RIGHTS

## Preamble

We hold these principles to be self-evident: that 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.

The digital age has transformed the way people communicate, travel, conduct business, worship, learn, receive medical care, participate in government, and exercise their constitutional freedoms. While technology has expanded opportunity, it has also created unprecedented abilities to collect, store, analyze, manipulate, and monetize personal information, yet no advancement in technology may be permitted to erode the liberties that belong inherently to the people.

Article I, Section 10 of the Constitution of South Carolina expressly secures the people against unreasonable invasions of privacy and requires particularity as to the information to be obtained. South Carolina's constitutional protections therefore do not depend solely upon the minimum protections recognized under the Fourth Amendment to the Constitution of the United States.

The rights guaranteed by the Constitutions of the United States and South Carolina do not diminish because life increasingly occurs in digital spaces. Constitutional liberties must remain constant even as technology evolves.

The purpose of the South Carolina Bill of Digital Rights is to affirm that every South Carolinian retains a constitutionally protected legal interest in digital information generated by, derived from, or uniquely linked to that individual's identity, body, communications, biometric characteristics, precise location, and lawful private activities. The collection, possession, storage, transmission, processing, or analysis of such information by another does not, standing alone, extinguish that protected interest.

Nothing in this Bill of Digital Rights shall be construed to transfer ownership of records, expressive works, intellectual property, or information lawfully created by another person, nor to abridge freedoms of speech or of the press secured by the Constitution.

These principles shall guide future legislation governing digital technology, artificial intelligence, surveillance systems, biometric information, communications, and all forms of electronic data.

## Definitions

For purposes of this Bill of Digital Rights, unless the context clearly requires otherwise:

## **Government**

Government means the United States, any State, territory, tribal government, political subdivision, municipality, agency, department, instrumentality, public official, employee, contractor, or any person or entity acting on behalf of government or exercising governmental authority.

## **Government Contractor**

Government Contractor means any private person or entity that performs governmental functions, collects, processes, stores, analyzes, or maintains information on behalf of government, or provides technology, services, infrastructure, or data used in governmental operations.

## **Protected Digital Information**

Protected Digital Information means digital information generated by, derived from, concerning, reasonably associated with, or uniquely linked to an identifiable individual, including but not limited to personal information, communications, metadata, biometric information, precise location information, behavioral information, algorithmic inferences, account credentials, and other electronically stored information protected by this Bill.

## **Digital Property**

Digital Property means every legally protected interest an individual retains in Protected Digital Information as recognized by this Bill, regardless of who possesses, stores, processes, licenses, transmits, or analyzes that information.

## **Metadata**

Metadata means information describing, generated by, or associated with electronic communications, devices, accounts, transactions, locations, or activities, including information concerning time, routing, identifiers, relationships, or usage, regardless of the content of the communication itself.

## **Surveillance**

Surveillance means the observation, monitoring, collection, recording, tracking, interception, retention, disclosure, analysis, aggregation, or use of information concerning individuals, communications, property, activities, movements, or associations through technological means.

## **Aggregated Surveillance**

Aggregated Surveillance means the collection, combination, correlation, retention, or analysis of information obtained across multiple sources, technologies, databases, locations, observations, or

periods of time in a manner that reveals substantially more about an individual or group than any isolated observation would reveal independently.

## **Search**

Search means any governmental effort to obtain, access, examine, monitor, analyze, infer, reconstruct, aggregate, or otherwise acquire information concerning an individual, regardless of whether accomplished physically, digitally, directly, indirectly, manually, or through automated means.

## **Biometric Information**

Biometric Information means measurable biological, physiological, or behavioral characteristics that may be used to identify, authenticate, recognize, or track an individual, including facial characteristics, fingerprints, palm prints, iris or retinal patterns, DNA, voiceprints, gait, keystroke dynamics, device-interaction patterns, behavioral biometrics, mathematical templates, embeddings, vectors, or similar identifiers.

## **Artificial Intelligence**

Artificial Intelligence means any computational system that performs functions associated with learning, prediction, classification, recommendation, generation, pattern recognition, decision-making, or other cognitive processes through automated means.

## **Automated Decision**

Automated Decision means any determination, recommendation, prediction, classification, ranking, action, or materially influential output produced wholly or substantially through automated technological processes.

## **Technology**

Technology means present or future hardware, software, algorithms, sensors, communications systems, artificial intelligence, networks, databases, or other systems capable of collecting, processing, storing, transmitting, analyzing, or utilizing information.

## **Government by Proxy**

Government by Proxy means the use of a private person or entity to perform, facilitate, or obtain information or accomplish actions that government would be constitutionally prohibited from performing or obtaining directly, or to evade constitutional limitations through delegation, contractual arrangement, purchase of information, or other indirect means.

## **Particularized Warrant**

Particularized Warrant means a warrant issued by a neutral judicial officer upon probable cause that particularly describes the place to be searched, the person or thing to be seized, and the information to be obtained, consistent with the Constitution of the United States and Article I, Section 10 of the Constitution of the State of South Carolina.

## **Rules of Construction**

Unless expressly stated otherwise:

1. The singular includes the plural, and the plural includes the singular.
2. The words "includes" and "including" mean "includes, but is not limited to."
3. References to technology include technologies existing now and those developed in the future.
4. References to digital information include information regardless of the medium, format, method of storage, method of transmission, or method of processing.
5. The rights recognized in this Bill shall not be diminished by changes in technology, commercial practices, contractual arrangements, or the use of private intermediaries.

## **ARTICLE I — Equality of Constitutional Rights**

The rights guaranteed by the Constitution of the United States shall apply equally in physical and digital environments.

Freedom of speech, religion, peaceful assembly, association, press, petition, and political participation shall receive equal protection regardless of the technology through which they are exercised.

No individual shall lose constitutional protections because a right is exercised, recorded, stored, transmitted, or affected through digital technology.

## **ARTICLE II — Ownership of Personal Digital Property**

Every individual retains a constitutionally protected legal interest in digital information generated by, derived from or uniquely linked to that individual's identity, body, communications, precise location, or private activities.

Digital property includes, but is not limited to:

- Personal information
- Personal communications
- Metadata
- Location information and location history
- Biometric identifiers
- Digital identity and account credentials
- Financial and medical records
- Browsing and search history
- Behavioral information and algorithmic inferences
- Creative works
- Other electronically stored information reasonably associated with an individual

The collection, possession, storage, processing, transmission, licensing, monetization, or analysis of such information by another does not, standing alone, extinguish that protected interest.

### **ARTICLE III — Searches, Surveillance, and Digital Privacy**

Every person has the right to be secure against unreasonable digital searches, surveillance, monitoring, tracking, interception, collection, retention, disclosure or analysis of protected digital information.

No person's protected digital information shall be searched, seized, compelled, or acquired by government except pursuant to a particularized warrant supported by probable cause and particularly describing the place to be searched, the person or thing to be seized, and the data to be obtained.

### **ARTICLE IV — Constitutional Treatment of Aggregated Surveillance**

Government shall not evade constitutional limitations by dividing continuous, aggregated, historical, retrospective, or persistent surveillance into individual or isolated observations, queries, data points, or periods of collection.

The constitutional significance of digital surveillance shall be evaluated in light of the nature, precision, duration, aggregation, persistence, and revealing character of the information obtained.

Whether surveillance constitutes a search or otherwise implicates constitutional protections shall be determined by evaluating the surveillance program as a whole rather than by artificially separating individual observations, devices, databases, or periods of collection.

### **ARTICLE V — Transparency**

Every individual has the right to meaningful transparency concerning the collection, retention, use, storage, access, analysis, deletion, modification, disclosure, sale, licensing, or transfer of protected digital information by government and by commercial entities engaged in the systematic processing of personal data, subject only to narrowly tailored exceptions necessary to protect an identified investigation, another person's rights, or information independently protected by law.

## **ARTICLE VI — Access and Correction**

Every individual has the right to inspect information maintained about them by government agencies.

Every individual has the right to challenge inaccurate information and seek timely correction.

Government agencies shall establish reasonable procedures for correcting erroneous information that materially affects an individual's rights or interests.

## **ARTICLE VII — Due Process**

No person shall be deprived of life, liberty, property, employment, licenses, benefits, constitutional rights, or legal protections through automated systems, algorithmic determinations, artificial intelligence, surveillance technologies, or digital profiling without due process of law and meaningful human accountability, including independent human review.

Meaningful human accountability requires independent human review by an identified human decision-maker with authority to independently evaluate the relevant evidence, reject or modify the automated determination, and provide an accountable basis for the final decision. Merely confirming, adopting, transmitting, or implementing an automated output does not constitute independent human review.

## **ARTICLE VIII — Constitutional Integrity**

Government shall not purchase, license, lease, request, receive, access, query, compel, use, rely upon, benefit from or otherwise acquire from a private person or entity protected digital information that government would be constitutionally prohibited from obtaining directly without required constitutional or judicial process.

The source, custodian, method of collection, contractual arrangement, commercial availability, de-identification, aggregation, pseudonymization, third-party possession, or use of a contractor, surveillance vendor, data broker, artificial intelligence system, nonprofit organization, or other intermediary shall not, standing alone or in combination, diminish constitutional protections.

## **ARTICLE IX — Freedom of Movement and Association**

Every individual retains the freedom to travel, assemble, associate, worship, petition, and engage in lawful activities without continuous digital surveillance or the creation of persistent, aggregated, historical, or retrospective records of a person's movements, associations, or lawful activities, absent individualized suspicion, a particularized warrant, or a constitutionally recognized exception.

No governmental entity shall evade constitutional limitations by characterizing a movement history as a collection of isolated public observations. The framework expressly distinguishes an isolated observation from the creation of a movement history.

## **ARTICLE X — Biometric Rights**

Every individual retains constitutionally protected legal interest and exclusive control of his or her biometric identifiers, including but not limited to behavioral biometrics, facial geometry/characteristics, fingerprints, palm prints, iris or retinal patterns, DNA profiles, voiceprints, gait analysis, keystroke patterns, device-interaction patterns, physiological identifiers, mathematical templates, embeddings, vectors, or other data derived from biological or behavioral characteristics for identification or persistent recognition.

Such information shall receive the highest level of legal protection.

## **ARTICLE XI — Data Security**

Government agencies entrusted with personal information have a duty to protect that information from unauthorized disclosure, misuse, or unauthorized access.

Individuals shall receive timely notification when their personal information has been compromised through a government data breach.

## **ARTICLE XII — Equal Constitutional Protection**

Constitutional protections shall apply equally regardless of whether information is collected:

- physically or digitally;
- directly by government or indirectly through private entities;
- manually or through automated systems;
- by technologies existing today or developed in the future.

Technological advancement shall never diminish constitutional liberty.

## **ARTICLE XIII — Reserved Digital Rights**

The enumeration of certain digital rights within this Bill shall not be construed to deny or disparage other rights retained by the people.

The rights guaranteed by this Bill of Digital Rights shall be interpreted consistently with the Constitutions of the United States and the State of South Carolina. Liberty endures. Technology evolves. The Constitution remains.

## **ARTICLE XIV- Constitutional Administration of Government**

Whenever government exercises constitutional authority through digital systems, automated processes, artificial intelligence, or private contractors, the constitutional rights of the people shall remain fully applicable.

Government shall not diminish constitutional protections by delegating governmental functions to private entities or by relying upon digital technologies that are not reasonably capable of meaningful transparency, accountability, independent verification, and lawful review.

## **FINAL ARTICLE — Construction and Interpretation**

These principles shall be interpreted consistently with the Constitution of the United States and the Constitution of the State of South Carolina and construed to preserve and strengthen constitutional liberty.

No provision shall be interpreted to authorize surveillance, collection, acquisition, retention, analysis, disclosure, or government access that would otherwise violate the Constitution of the United States or the Constitution of the State of South Carolina.

No exception to the rights secured herein shall be implied solely from technological capability, commercial availability, private ownership of infrastructure, contractual consent, third-party possession, algorithmic determination, or administrative convenience.

Every exception created by implementing legislation shall be expressly stated, narrowly drawn, and no broader than constitutionally permissible for the purpose it serves.

**Severability.** If any provision of this Bill, or its application to any person or circumstance, is held invalid, the remaining provisions and their application shall remain in full force and effect to the fullest extent permitted by law.

# THE CASE FOR A SOUTH CAROLINA BILL OF DIGITAL RIGHTS

## A State Constitutional Framework for Liberty in the Digital Age

### Introduction

The Constitution of the United States has endured for more than two centuries because it was written to protect timeless principles rather than temporary circumstances. The Founders could not have anticipated automobiles, airplanes, telephones, computers, the Internet, artificial intelligence, or satellites. Yet the Constitution continues to govern because it protects liberty rather than technology.

The Constitution of the State of South Carolina reflects those same enduring principles. Like its federal counterpart, it secures fundamental liberties intended to remain constant even as society and technology evolve. Indeed, Article I, Section 10 of the South Carolina Constitution expressly protects the people against unreasonable searches, seizures, and invasions of privacy, providing an important constitutional foundation for liberty in the Digital Age.

Today, however, nearly every aspect of life has become digital. Our communications, finances, travel, medical records, education, employment, purchases, political participation, religious activities, and personal relationships generate digital information. Every advancement in technology creates new opportunities for prosperity and innovation—but also unprecedented opportunities for surveillance, manipulation, and control.

The question facing South Carolina is not whether technology will continue to evolve. It will.

The question is whether our application of enduring constitutional principles will evolve with it.

The South Carolina Bill of Digital Rights answers that question by reaffirming a simple principle:

**Technology changes. Rights do not.**

### Why South Carolina Needs a Bill of Digital Rights

Throughout American history, periods of technological innovation have required lawmakers and courts to apply longstanding constitutional principles to new realities.

The printing press expanded freedom of the press.

The telephone required courts to reconsider privacy.

Automobiles transformed freedom of movement.

Air travel changed commerce.

The Internet revolutionized communication.

Artificial intelligence now challenges assumptions about decision-making, identity, privacy, and personal autonomy.

The Digital Age presents another such moment.

Neither the Constitution of the United States nor the Constitution of the State of South Carolina becomes obsolete because technology advances. Rather, the enduring constitutional principles they secure must be faithfully applied to technologies the Framers and the people of South Carolina could not have imagined.

South Carolina's Constitution already provides an important foundation for that work. Article I, Section 10 expressly protects against unreasonable searches, seizures, and invasions of privacy, demonstrating that constitutional liberty remains the guiding principle even as the methods by which information is collected and used continue to evolve.

The South Carolina Bill of Digital Rights does not create new constitutional rights. It reaffirms that the liberties already secured by the Constitutions of the United States and South Carolina remain fully applicable in the Digital Age.

## **What is Digital Property?**

For purposes of this paper, "digital property" is shorthand for the legally protected interests an individual retains in Protected Digital Information. It includes digital information that identifies, describes, records, predicts, or otherwise reflects an individual's identity, activities, communications, body, location, or personal affairs.

Examples include personal communications, biometric identifiers, location information, financial and medical information, browsing and search history, digital identity and account credentials, photographs, documents, metadata, behavioral profiles, algorithmic inferences, and other electronically stored information associated with that person. The term does not mean that an individual necessarily holds title to every record, copy, expressive work, or item of intellectual property created or lawfully possessed by another. The central principle is that third-party possession, storage, processing, licensing, transmission, or analysis, does not, standing alone, extinguish the individual's constitutionally protected legal interest in qualifying digital information.

Photographs, recordings, and other expressive works may contain Protected Digital Information without transferring ownership of the photograph, recording, or expressive work to the person depicted. The protected interest concerns qualifying information about the individual including

biometric identifiers, location, associations, behavioral information, and information derived or inferred from the image or recording- rather than automatic ownership or control of every expressive work in which the individual appears.

For legislative analysis, capture, publication or distribution, biometric or algorithmic processing, and commercial exploitation should be treated as distinct acts that need not be governed by the same consent standard. Review should expressly consider livestreaming and archived recordings, republication, facial or other biometric extraction, identification, tracking, profiling, and commercial use. An image or recording may also reveal or permit inference of sensitive location, religious or associational activity, political participation, medical activity, companions, movements, or behavior. Any implementing legislation should preserve constitutionally protected speech, press, public-interest reporting, ordinary photography, public proceedings, and other lawful expressive uses while addressing materially different downstream uses.

## **Protected Interests in the Digital Age**

The core question is not who owns every copy of a digital record. It is whether constitutional protection disappears merely because information about a person is generated, stored, processed, or held by someone else. The South Carolina Bill of Digital Rights answers that question no. Throughout American history, rights in persons, papers, property, privacy, speech, association, and due process have served as safeguards of individual liberty. As more of life is recorded and mediated digitally, those constitutional protections should remain effective when the information at issue reflects a person's identity, activities, communications, movements, associations, or private affairs. The framework therefore protects a retained constitutional interest without purporting to transfer ownership of records, expressive works, intellectual property, or information lawfully created by another person.

## **The Principle of Technological Neutrality**

A constitutional right should never depend upon the technology through which it is exercised.

Freedom of speech deserves the same protection whether expressed in a town square, a newspaper, a telephone conversation, an email, or an online forum.

Likewise, the protections against unreasonable searches should not disappear simply because personal papers have become digital records, letters have become emails, or travel has become location data.

**Technology changes.**

**Rights do not.**

## **Government by Proxy**

If individuals retain constitutional rights in protected digital information, those protections cannot be circumvented simply because the information is held by someone else.

One of the oldest principles in American law is that government may not accomplish indirectly what it is prohibited from doing directly.

This principle remains equally important in the Digital Age.

Government should not evade constitutional limitations by purchasing information from private companies, relying upon data brokers, or outsourcing surveillance to third-party vendors when those same activities would require constitutional process if performed directly by government agents.

Constitutional protections should not depend upon who controls the technology.

## **Surveillance and a Free Society**

Throughout history, governments have sought information in order to govern more effectively.

Technology has transformed the scale at which information can be collected.

Modern technology enables forms of large-scale and persistent surveillance that were previously impossible, allowing governments and private entities to collect, analyze, and retain vast quantities of information about ordinary people with unprecedented speed and precision.

Modern surveillance systems can document where people travel, whom they associate with, where they worship, where they receive medical care, how they communicate, what they purchase, and what they believe.

Such capabilities require equally robust constitutional safeguards.

A free people should not live under continuous surveillance merely because technology makes such surveillance possible.

## **Aggregated Surveillance**

Historically, courts often evaluated surveillance by examining individual observations in isolation. A police officer seeing a vehicle drive down a public road, observing someone enter a building, or recording a single license plate generally raised few constitutional concerns because each observation, standing alone, revealed relatively little.

Modern technology has fundamentally changed that analysis.

Today's surveillance systems can automatically collect millions of observations over extended periods of time. When combined, those observations may reveal a person's home, workplace, medical providers, religious practices, political activities, friendships, travel habits, daily routines, and countless other details that no single observation could disclose.

The constitutional concern is therefore no longer limited to individual observations. It is the government's ability to aggregate, retain, correlate, and analyze otherwise ordinary information into a detailed pattern of an individual's life.

Recent decisions of the Supreme Court of the United States, together with the protections secured by Article I, Section 10 of the South Carolina Constitution, reflect this evolving understanding.

In *United States v. Jones* (2012), several Justices recognized that prolonged GPS monitoring can reveal an intimate picture of a person's life that differs fundamentally from isolated public observations. The concern was not merely where a person traveled on a particular day, but what months of continuous tracking revealed about that person's private life.

That principle became even clearer in *Carpenter v. United States* (2018). The Supreme Court held that obtaining historical cell-site location information generally requires a warrant because prolonged location records reveal "the privacies of life." Although each individual location point may have been generated through ordinary use of a cellular telephone, the accumulated record created a comprehensive chronicle of the person's movements that deserved constitutional protection.

South Carolina's first appellate decision addressing Flock Safety technology illustrates both the importance and the limits of existing case law. In *State v. Faile*, Unpublished Opinion No. 2026-UP-323 (S.C. Ct. App. July 1, 2026), the Court of Appeals affirmed the denial of suppression where officers used two Flock images, taken one day apart, to identify a vehicle rather than to reconstruct the defendant's movements over time. The opinion is unpublished and expressly has no precedential value except as provided by Rule 268(d)(2), SCACR. It is therefore cited here only as an illustration of how the constitutional analysis may differ between limited observations and persistent, aggregated surveillance capable of reconstructing a person's movements or associations.

Together, these decisions reflect constitutional principles grounded in both the Constitution of the United States and the Constitution of the State of South Carolina. Article I, Section 10 of the South Carolina Constitution independently protects the people against unreasonable searches, seizures, and invasions of privacy, providing an important state constitutional foundation for applying those enduring principles to modern technologies. The South Carolina Bill of Digital Rights seeks to reaffirm and faithfully apply those constitutional protections to technologies capable of collecting, retaining, aggregating, correlating, and analyzing personal information on an unprecedented scale.

The South Carolina Bill of Digital Rights recognizes that constitutional protections should be evaluated based upon the overall nature, duration, precision, persistence, and revealing character

of surveillance rather than by artificially dividing a surveillance program into individual observations, devices, databases, or periods of collection.

Technology has made comprehensive surveillance increasingly inexpensive, automated, and persistent. Constitutional liberty requires that the protections guaranteed by the Constitutions of the United States and South Carolina evolve in their application—not because those Constitutions have changed, but because technology now permits forms of surveillance that previous generations could scarcely imagine.

The General Assembly need not wait for each new surveillance technology to be addressed through years of litigation before reaffirming the constitutional principles that already govern governmental power.

## **Artificial Intelligence**

Artificial intelligence will increasingly assist both governments and private organizations in making decisions that affect individual liberty.

While AI offers tremendous promise, it must remain subject to human accountability.

Human decision-makers must remain constitutionally accountable for decisions affecting individual rights, regardless of whether artificial intelligence assisted the process.

No person should lose liberty, property, employment, benefits, licenses, or constitutional rights solely because an algorithm reached a conclusion.

Technology may assist human judgment. It must never replace constitutional due process.

## **Innovation and Liberty**

Protecting digital rights is not anti-technology.

Innovation and liberty are complementary.

Clear constitutional protections increase public trust, encourage responsible innovation, reduce legal uncertainty, and ensure that technological progress strengthens rather than weakens a free society.

The goal is not to limit innovation.

The goal is to preserve liberty while innovation continues.

## Why South Carolina Should Lead

Throughout its history, South Carolina has often stood at the forefront of constitutional debate and the defense of fundamental principles.

Regardless of one's views of every chapter of that history, there is little question that South Carolinians have long believed questions of constitutional liberty deserve serious consideration and principled leadership.

Today, the Digital Age presents another such moment.

Rapid advances in surveillance technologies, artificial intelligence, digital property, biometric identification, and government access to personal information are reshaping the relationship between citizens and government.

States need not wait for Congress or the federal courts to address every emerging challenge. South Carolina possesses both the constitutional authority and the opportunity to act.

By adopting a South Carolina Bill of Digital Rights, our State can become the **first in the South** to establish a comprehensive constitutional framework for protecting digital liberty.

In doing so, South Carolina can provide a principled model for other states while demonstrating that technological innovation and constitutional freedom are not competing values—they are strengthened when each is governed by the rule of law.

Leadership is not measured by adopting the newest technology first. It is measured by ensuring that technological progress remains accountable to enduring constitutional principles.

South Carolina has an opportunity to lead once again by affirming a timeless truth:

**Technology changes. Rights do not.**

## A Call to Leadership

The Constitution of the United States and the Constitution of the State of South Carolina have endured because they protect enduring principles rather than temporary technologies.

The South Carolina Bill of Digital Rights does not create new rights.

It reaffirms that the constitutional liberties already secured to the people remain fully applicable in a world increasingly shaped by digital technology.

Every generation inherits the responsibility to preserve liberty.

This generation's responsibility is to ensure that constitutional rights remain meaningful in a world increasingly shaped by digital technology.

Government derives its powers from the Constitution—not from technological advancement.

Innovation should expand human opportunity—not diminish human freedom.

Every generation must decide whether technology will remain the servant of liberty—or whether liberty will become the servant of technology.

The Constitution leaves no doubt.

Government exists to secure the rights of the people, and those rights endure regardless of how technology evolves.

# 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.**

# **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.

# SECTION-BY-SECTION JUDICIARY SUMMARY

## Summary of the South Carolina Digital Liberty and Government Technology Accountability Act

- **Section 1:** Names the Act.
- **Section 2:** States constitutional and legislative findings, including South Carolina's express privacy protection and the principle that technological capability does not create governmental authority.
- **Section 3 / Section [--10]:** Defines key terms governing the Act, including governmental entities, protected digital information, surveillance technology, automated decision systems, biometric information, and high-consequence governmental digital systems.
- **Section [--20] through Section [--50]:** Establishes constitutional-process, aggregation, government-by-proxy, and shared/federated-system rules.
- **Section [--60]:** Requires independent human review when automated systems materially affect substantial legal interests and provides for notice and a reasonable opportunity to challenge material factual or computational error when an automated system materially contributes to an adverse governmental determination, subject to exceptions expressly provided by law.
- **Section [--70] through Section [--90]:** Requires impact assessment, independent verifiability, audit evidence, and record integrity. Provides that certification, testing, accreditation, approval, procurement acceptance, or compliance with a technical standard does not, standing alone, constitute independent verification or create a conclusive presumption of system correctness, integrity, security, or lawful operation.
- **Section [--100] and Section [--110]:** Establishes procurement, supply-chain, contractor-accountability, and lawful oversight-access requirements\*\*, including accountability for material commercial off-the-shelf components and relevant foreign access, control, or operational dependencies.

- **Section [--120] and Section [--130]:** Requires affirmative public approval for new categories or materially new uses of political-subdivision surveillance technology and creates a public technology inventory.
- **Section [--140] and Section [--150]:** Establishes data-security, correction/preservation, and anti-circumvention duties.
- **Section [--160]:** Provides equitable enforcement, attorney's fees and litigation costs where awarded by the court, remedies for knowing or willful substantive violations as provided by law, and preservation of existing remedies.
- **Section [--170]:** Makes the Act a constitutional floor, not a safe harbor or ceiling, preserves greater local protections when otherwise authorized by law, and addresses federal preemption.
- **Sections 4-5:** Provide severability, transition, and effective-date provisions. The transition period for an existing covered system's initial inventory and impact assessment does not delay another substantive requirement of the Act unless expressly provided by law.

Matters requiring further drafting, reconciliation, or committee determination are identified separately in the Legislative Counsel & Judiciary Checklist

# EXISTING LAW AND PENDING LEGISLATION REVIEW

## Implementation and Reconciliation Memorandum

This memorandum identifies enacted South Carolina law and pending or prior legislation that should be preserved, strengthened, reviewed, amended, conformed\*\*, or reconciled\*\* as the General Assembly considers statutory implementation of the framework. It is not a declaration that existing provisions are unconstitutional or that every identified gap requires a separate statute.

| Law / Area           | Classification    | Current Role                                                                                | Implementation / Reconciliation Direction                                                                                                      |
|----------------------|-------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| S.C. Code §17-13-142 | REVIEW / AMEND    | Electronic communications; federal §2703(d) orders, warrants, and specified ICAC subpoenas. | Add an express South Carolina constitutional savings rule and review process standards under Article I, §10.                                   |
| Title 17, Chapter 30 | MODERNIZE         | Older electronic communications and interception architecture.                              | Modernize definitions and ensure tracking, location, metadata, modern devices, cloud services, and derived information are treated coherently. |
| Title 17, Chapter 29 | PRESERVE / REVIEW | Pen register and trap-and-trace procedures.                                                 | Preserve useful process protections; review modern identifiers, aggregation, and technology-neutral terminology.                               |
| Title 30, Chapter 2  | PRESERVE / EXPAND | Family Privacy Protection Act; privacy policies, legitimate public purpose, personal-       | Use as an existing statutory foundation for minimization, purpose limitation, access, correction, and modern digital-                          |

|                                             |                                         |                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             |                                         | information definitions.                                                                                                                                                                                                                              | information governance.                                                                                                                                                                                                                                                                                                                                 |
| S.C. Code §30-2-40(C)                       | REVIEW                                  | Notice/privacy-policy exception for criminal justice and judicial agencies.                                                                                                                                                                           | Ensure exceptions do not unnecessarily displace broader accountability, security, minimization, or correction rules.                                                                                                                                                                                                                                    |
| Government Data Retention and Disposition   | STATUTORY REVIEW / FRAGMENTED FRAMEWORK | Retention, preservation, disposition, and records requirements arise from multiple general and program-specific authorities rather than a single technology-neutral framework governing protected digital information.                                | Review existing retention schedules, public-record obligations, litigation holds, evidentiary requirements, investigative needs, and other preservation duties. Establish appropriate purpose-based minimization, retention, anonymization, and disposition standards without requiring deletion where another law independently requires preservation. |
| Individual Access, Accuracy, and Correction | PRESERVE / EXPAND                       | Existing privacy, records, and program-specific laws provide portions of the framework for access to and correction of governmental information, but do not establish one comprehensive technology-neutral process for protected digital information. | Establish meaningful procedures, subject to legitimate investigative, security, confidentiality, and other legal limitations, for individuals to inspect appropriate governmental information concerning themselves, challenge demonstrably inaccurate information, seek                                                                                |

|                       |                   |                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       |                   |                                                                                                                                                                                                                                                                                                                                             | timely correction, and address materially inaccurate information propagated to downstream governmental systems or recipients.                                                                                                                                                                                                                               |
| Biometric Information | PRESERVE / EXPAND | Title 30, Chapter 2 includes biometric identifiers within South Carolina's existing personal-information framework, but does not by itself establish the complete set of safeguards contemplated by the Digital Bill of Rights for governmental biometric collection, use, retention, sharing, analysis, and derived biometric information. | Preserve existing protections while evaluating enhanced, technology-neutral safeguards for facial geometry, fingerprints, palmprints, iris or retinal patterns, DNA profiles, voiceprints, gait, behavioral biometrics, templates, embeddings, vectors, and future biometric identifiers. Reconcile these protections with H.3404 and other applicable law. |
| Title 30, Chapter 4   | CONFORM           | Freedom of Information Act.                                                                                                                                                                                                                                                                                                                 | Preserve exemptions while clarifying that public-disclosure exemptions do not defeat lawful court, legislative, audit, or inspector access.                                                                                                                                                                                                                 |
| Title 11, Chapter 35  | CONFORM / EXPAND  | State procurement framework.                                                                                                                                                                                                                                                                                                                | Add covered-system contract requirements for audit access, records, cybersecurity, material changes, subcontractors, remote access, data disposition, and oversight. Address, as appropriate, material hardware, software, firmware,                                                                                                                        |

|                                          |                                            |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          |                                            |                                                                                                                                                                                                                                                                                                    | commercial off-the-shelf components, update authority, cloud dependencies, authentication dependencies, and material foreign ownership, access, control, or operational dependencies. Clarify that procurement, certification, testing, accreditation, or technical approval does not itself create substantive governmental authority or conclusively establish system correctness, integrity, security, or lawful operation. |
| Government Technology Impact Assessments | STATUTORY GAP / NO COMPREHENSIVE FRAMEWORK | Impact-assessment requirements may exist in particular programs or contexts, but no comprehensive technology-neutral statewide framework has been identified in this review requiring governmental impact assessment for designated high-consequence digital systems or surveillance technologies. | Establish appropriate assessment triggers for deployment, renewal, material change, or other designated events. Address legal authority, constitutional and privacy implications, data sources, automated functions, human review, independent verification, cybersecurity, remote access, cloud and subcontractor dependencies, material foreign dependencies, and other risks                                                |

|                                                                |                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                |                                                         |                                                                                                                                                                                                                                                                                                                                                                                        | appropriate to the system.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Statewide ALPR Framework                                       | PENDING / NO COMPREHENSIVE ENACTED FRAMEWORK IDENTIFIED | No comprehensive enacted statewide ALPR statute governing ALPRs as a class. Multiple proposals in the 126th General Assembly address ALPR use, including S.447, H.3155, and H.4013.                                                                                                                                                                                                    | Address through affirmative technology-neutral surveillance legislation rather than vendor-specific rules**, while reconciling compatible protections contained in pending ALPR legislation.**                                                                                                                                                                                                                             |
| High-consequence digital systems                               | STATUTORY GAP / NO COMPREHENSIVE FRAMEWORK              | No general statewide framework combines independent verification, auditability, human accountability, procurement controls, and anti-circumvention.                                                                                                                                                                                                                                    | Create a general statutory framework tied to function, capability, operation, and effect.                                                                                                                                                                                                                                                                                                                                  |
| Commercial Off-the-Shelf Components / Independent Verification | STATUTORY GAP / NO COMPREHENSIVE FRAMEWORK              | Governmental digital systems may incorporate hardware, software, firmware, libraries, modules, cloud services, and other commercial components supplied, updated, administered, tested, or certified by multiple entities. Existing procurement or certification processes do not necessarily provide an independent mechanism for verifying every consequential governmental outcome. | Establish appropriate traceability, material-change, remote-access, update, audit, and oversight requirements for consequential components. Preserve independent verification where required and clarify that certification, accreditation, testing, procurement acceptance, or compliance with a technical standard does not, standing alone, create a conclusive presumption of correctness, integrity, security, lawful |

|                                                       |                     |                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                       |                     |                                                                                                                                                                                                                                                                                                       | operation, or statutory compliance.                                                                                                                                                                                                                             |
| S.447 (2025-2026) — License Plate Reader System       | PENDING — RECONCILE | Proposes §23-1-235 governing automatic license plate reader systems and §57-3-786 concerning certain cameras on non-interstate highway rights-of-way. S.447 was introduced March 12, 2025, referred to Senate Judiciary, and received a favorable Senate Judiciary Committee report on April 9, 2026. | Reconcile its ALPR-specific authorization, use, access, retention, sharing, and right-of-way provisions with the broader technology-neutral framework. Preserve compatible safeguards while avoiding conflicting definitions or parallel compliance structures. |
| H. 4013 (2025-2026) - Automated License Plate Readers | PENDING - RECONCILE | Proposes §23-1-235 ALPR rules including public policy, documented law-enforcement purpose, access logs, audit schedule, visual confirmation before a stop, and 90-day retention; currently residing in the House.                                                                                     | Preserve compatible safeguards; reconcile retention, audit, authorization, sharing, and access rules with the technology-neutral framework rather than duplicate them.                                                                                          |
| H. 3155 (2025-2026) - Automatic license plate readers | PENDING - REVIEW    | Earlier ALPR proposal referred to House Judiciary; includes permitted uses, 90-day retention, sharing limits, and a criminal penalty.                                                                                                                                                                 | Compare definitions and permitted-use structure with S.447, H.4013, and the general framework; avoid conflicting definitions or parallel compliance regimes.                                                                                                    |
| H. 4675 (2025-2026) - Video Surveillance              | PENDING - RECONCILE | House Judiciary proposal addressing third-party storage, vehicle-feature recognition, 21-day retention, warrant requirements, access logging, independent audits, transparency                                                                                                                        | Reconcile overlapping surveillance, audit, retention, third-party hosting, emergency, remedy, and oversight provisions; preserve compatible protections while                                                                                                   |

|                                                               |                                                     |                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               |                                                     | reports, penalties, and civil remedies.                                                                                                                                                                                                                                                                                         | avoiding technology-specific conflict.                                                                                                                                                                                                                                                                                                                                                                                                  |
| H.3400 (2025-2026)<br>— Child Data Privacy and Protection Act | PENDING —<br>REVIEW /<br>RECONCILE                  | Proposes legislation addressing children's personal data, including data-protection impact assessments, collection, retention, processing, sale, privacy-by-default requirements, parental access in specified circumstances, privacy policies, enforcement, and related protections. The bill was referred to House Judiciary. | Reconcile H.3400 with the Digital Bill of Rights' Children's Digital Rights initiative. Distinguish regulation of private online products from governmental collection and use of children's protected digital information, while reviewing parental authority, education, child-protection responsibilities, persistent identifiers, biometrics, profiling, automated decision-making, retention, and applicable federal requirements. |
| S.C. Code §50-3-420<br>- DNR entry onto private property      | REVIEW / AMEND                                      | Provides specified Department of Natural Resources enforcement officers and Lake Wylie Marine Commission officers immunity from criminal prosecution, while acting in official capacity within territorial jurisdiction, for entering private property whether or not posted against trespassing.                               | Reconcile with proposed statutory protections for governmental investigative entry onto private real property beyond curtilage. Distinguish warrants, owner consent, emergencies, lawful easement or property-management functions, and other expressly authorized governmental entry.                                                                                                                                                  |
| Open Fields / Remote Surveillance of Private Land             | STATUTORY GAP /<br>NO<br>COMPREHENSIVE<br>FRAMEWORK | No comprehensive statewide statutory framework in this package establishes heightened rules for                                                                                                                                                                                                                                 | Develop technology-neutral companion legislation addressing physical entry, installation or                                                                                                                                                                                                                                                                                                                                             |

|                                                                                                     |                              |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                     |                              | governmental investigative entry or targeted technological surveillance of privately owned land beyond curtilage.                                                                                                                                                                               | placement of surveillance equipment, unmanned aircraft and remote sensing, owner consent, warrants, emergencies, remedies, and interaction with §50-3-420 and existing constitutional doctrine.                                                                                                                           |
| H. 3596 (124th General Assembly, 2021-2022) - Surveillance (prior-session legislation; not enacted) | PRIOR LEGISLATIVE HISTORY    | Prior proposal would have prohibited state or local law enforcement from installing surveillance equipment on farmland, timberland, fields, or other land beyond curtilage without a warrant or property-owner permission and would have excluded unlawfully obtained recordings from evidence. | Use as prior South Carolina legislative history when drafting broader, technology-neutral Open Fields and private-land surveillance reform; review scope, exceptions, remedies, and treatment of physical entry as distinct from installed surveillance equipment.                                                        |
| H. 3404 (2025-2026) - Ensuring Likeness, Voice, and Image Security Act                              | PENDING - REVIEW / RECONCILE | Proposes a property right in the use of an individual's name, photograph, voice, or likeness and civil liability for specified unauthorized uses, including certain technologies used to produce a person's photograph, voice, or likeness.                                                     | Reconcile with the Digital Bill of Rights distinction between expressive-work ownership and protected information contained in or derived from an image or recording. Review commercial exploitation, synthetic or biometric use, minors, consent, news and public-interest uses, expressive activity, and constitutional |

|  |  |  |                               |
|--|--|--|-------------------------------|
|  |  |  | speech and press protections. |
|--|--|--|-------------------------------|

## Reconciliation Principle

The objective of this review is not to replace existing South Carolina protections that remain useful or to create unnecessary parallel regulatory regimes. Implementing legislation should preserve compatible protections, modernize outdated provisions, reconcile overlapping requirements, close identified gaps, and establish technology-neutral standards where existing law is fragmented, incomplete, or technology-specific.

# LEGISLATIVE COUNSEL AND JUDICIARY CHECKLIST

## Matters Requiring Drafting or Committee Review

This checklist identifies drafting, reconciliation, implementation, and policy questions requiring Legislative Council or committee review as the South Carolina Digital Bill of Rights framework moves toward statutory implementation. Inclusion of an issue does not presume a particular legislative outcome; it identifies matters requiring deliberate resolution in final legislation.

### Code Placement and Structure

- Determine final placement of the general digital-rights implementation chapter and necessary conforming amendments.
- Avoid duplicative definitions where existing Code definitions can be incorporated without weakening the framework.

### Definitions

- Refine protected digital information, automated decision system, adverse governmental determination, high-consequence system, surveillance technology, material change, governmental entity, contractor, and third party.
- Keep high-consequence coverage tied to function, capability, operation, and effect rather than vendor labels.

### Constitutional Floor

- State expressly that statutory compliance is not a safe harbor for unconstitutional conduct.
- Preserve independent protections of S.C. Const. art. I, §10.

### Government by Proxy

- Use functional-equivalence language that prevents commercial availability, third-party possession, contracting, or shared-system access from independently creating governmental authority.

### Law Enforcement and Emergencies

- Preserve constitutionally recognized warrant exceptions and carefully defined emergencies.

- Review §17-13-142 and Titles 17 Chapters 29 and 30 for state-constitutional savings clauses and modern definitions.

## **Data Minimization, Retention, and Disposition**

- Determine appropriate purpose-limitation, minimization, retention, anonymization, and disposition requirements for protected digital information.
- Reconcile those requirements with public-record obligations, records-retention schedules, litigation holds, evidentiary duties, criminal investigations, court orders, program-specific requirements, and other independent legal preservation obligations.
- Avoid indefinite retention based solely on technological capability or storage convenience while preserving information that lawfully must be retained.

## **Individual Access, Accuracy, and Correction**

- Determine when individuals should be permitted to inspect governmental information concerning themselves, challenge demonstrably inaccurate information, and obtain timely correction.
- Define appropriate exceptions for active investigations, security, confidentiality, protected third-party information, judicial records, and other circumstances in which access or correction would conflict with law or legitimate governmental functions.
- Address downstream correction when materially inaccurate information has been transmitted to or relied upon by another governmental system or recipient.

## **Biometric Information**

- Determine whether enhanced safeguards for governmental collection, generation, use, retention, analysis, sharing, and disclosure of biometric information should be incorporated into the principal Act, companion legislation, or existing privacy law.
- Reconcile biometric protections with Title 30, Chapter 2, H.3404, law-enforcement authorities, identification functions, security needs, and other applicable law.
- Ensure definitions remain technology-neutral enough to address templates, embeddings, vectors, behavioral biometrics, and future biometric identification or persistent-recognition methods.

## **Automated Decisions**

- Define when independent human review, notice, explanation, correction, and challenge are required.
- Protect legitimate investigative and security needs without allowing blanket automation exceptions.
- Specify the minimum characteristics of meaningful independent human review, including an identified human decision-maker with sufficient information and actual authority to

evaluate, reject, correct, or modify a material automated determination rather than merely ratify the system's output.

## **High-Consequence Systems**

- Define independent verification and reconstructability by outcome/risk rather than mandating one technology.
- Determine appropriate exceptions where independent evidence is technologically impossible or disproportionate, with written findings and compensating safeguards.

## **Impact Assessments**

- Determine which high-consequence governmental digital systems, surveillance technologies, automated decision systems, and material changes require an impact assessment before deployment, renewal, or continued use.
- Define minimum assessment content, including legal authority, constitutional and privacy implications, data sources, automated functions, human review, independent verification, cybersecurity, remote access, material foreign dependencies, cloud services, subcontractors, records, and anticipated effects on substantial legal interests.
- Determine appropriate treatment of confidential, security-sensitive, trade-secret, and law-enforcement information while preserving meaningful legislative, judicial, audit, inspector, and public accountability.

## **Procurement and Contractors**

- Require audit/oversight access, records, material-change notice, cybersecurity duties, subcontractor transparency, remote-access disclosure, data disposition, and flow-down clauses.
- Clarify that procurement authority, contractual access, possession of technology, or technical capability does not independently create substantive governmental authority to use every capability of an acquired system.

## **Commercial Off-the-Shelf Components / Certification**

- Determine appropriate disclosure, traceability, testing, update, remote-access, and material-change requirements for commercial off-the-shelf hardware, software, firmware, modules, libraries, and other components incorporated into high-consequence governmental systems.
- Ensure certification, accreditation, testing, procurement approval, or compliance with a technical standard does not, standing alone, create a conclusive presumption of correctness, integrity, security, lawful operation, or statutory compliance.

- Determine when independent verification must be capable of detecting a material error or compromise notwithstanding prior vendor, laboratory, governmental, or third-party certification or testing.

## **Foreign Dependencies**

- Distinguish foreign manufacture from material foreign control or operational dependency.
- Define reportable remote administration, data access, update authority, authentication, cloud, and subcontractor dependencies.
- Determine appropriate risk-assessment, disclosure, mitigation, and oversight requirements where material foreign control, access, administration, update authority, authentication dependency, or other operational dependency could affect a high-consequence governmental function.

## **Public Records and Trade Secrets**

- Preserve existing FOIA exemptions.
- Clarify that a public-disclosure exemption does not eliminate lawful court, legislative, audit, or inspector access.

## **Remedies and Immunities**

- Resolve standing, injunctive/declaratory relief, preservation, attorney fees, civil remedies, suppression where appropriate, and interaction with governmental immunities.

## **Objective Standards**

- Replace subjective operative terms with objective tests where practical, particularly for human review, emergency authority, material changes, auditability, and compliance triggers.

## **Audit Evidence**

- Specify which covered systems must create audit evidence, required fields, retention periods, integrity controls, and vendor production obligations.

## **Independent Audits**

- Determine whether designated categories of high-consequence governmental digital systems or surveillance technologies should be subject to periodic or event-triggered independent audits in addition to impact-assessment, independent-verification, and audit-evidence requirements.
- Define appropriate audit triggers, independence requirements, scope, access, records, frequency, reporting, remediation, and treatment of confidential or security-sensitive information.

## **Public Technology Inventory**

- Determine whether public technology inventories should remain maintained by individual governmental entities as provided in the proposed Act or whether the State should additionally provide a centralized public reporting or searchable mechanism.
- Determine minimum inventory fields, update frequency, treatment of materially changed systems, and narrow exclusions necessary to protect legitimate investigative or security interests without defeating meaningful transparency.

## **State-Agency Surveillance Authorization**

- Determine whether an affirmative-authorization mechanism analogous to the political-subdivision process should apply when a State agency proposes to deploy a new category of surveillance technology or a materially new use of existing surveillance technology and, if so, what authorization, notice, review, and accountability process is appropriate to State-agency governance.

## **Statewide Oversight**

- Determine whether existing oversight authorities are sufficient to administer and oversee statewide compliance or whether additional jurisdiction, designation of a lead oversight entity, or another coordination mechanism is warranted.
- Consider the appropriate roles, if any, of existing inspectors, auditors, procurement authorities, legislative oversight bodies, courts, or another designated entity without unnecessarily duplicating existing jurisdiction.

## **Renewals / Material Changes / Legacy Systems**

- Define transition periods and event triggers so legacy status does not become indefinite grandfathering; distinguish routine maintenance from material capability changes.

## **Anti-Circumvention**

- Confirm that paid and unpaid access, third-party queries, shared/federated systems, derived information, and divided governmental functions cannot be used to evade otherwise applicable duties.

## **Local Government / Home Rule**

- Determine which duties apply statewide to political subdivisions and how local authorization requirements interact with home-rule authority.

## **Children's Digital Rights**

- Reconcile the Digital Bill of Rights framework with H.3400 and other applicable state and federal protections governing children's data, education records, parental authority, child protection, and online services.
- Determine which protections should apply specifically to governmental collection, generation, use, retention, sharing, profiling, biometric processing, persistent identification, or automated decision-making involving minors.
- Preserve legitimate educational, health, safety, child-protection, and other lawful governmental functions while establishing appropriate safeguards for children's protected digital information.

## **Image, Voice, Likeness, and Photo Consent**

- Reconcile H. 3404 with the Digital Bill of Rights without converting the presence of a person in a photograph or recording into ownership of the expressive work.
- Define the relationship among consent, commercial exploitation, synthetic or biometric use, minors, news and public-interest uses, ordinary photography and recording, and constitutional speech and press protections.
- Clarify that protected digital information may be contained in or derived from an expressive work without transferring ownership of the work.

## **Open Fields / Private-Land Surveillance**

- Review S.C. Code §50-3-420 and the scope of governmental investigative entry onto posted and unposted private property beyond curtilage.
- Determine the statutory rule for physical entry, installed or placed surveillance equipment, unmanned aircraft, remote sensing, owner consent, warrants, emergencies, and other lawful authority.
- Coordinate remedies with Section [--160] of the proposed Digital Liberty and Government Technology Accountability Act while distinguishing suppression or exclusion issues from civil and equitable remedies.

## **Transition and Fiscal Impact**

- Establish prospective application, treatment of renewals/material changes, legacy-system transition periods, and reasonable implementation deadlines.
- Identify fiscal effects of inventories, audit logs, procurement clauses, incident response, and oversight.
- Consider phased or proportionate compliance mechanisms for smaller political subdivisions where appropriate without creating permanent exemptions from core constitutional or accountability requirements.

## **Federal Law**

- Identify areas governed by federal communications, disability-access, criminal-procedure, grant, or procurement requirements and include savings clauses accordingly.
- Review applicable federal electronic-communications, stored-communications, interception, pen-register/trap-and-trace, motor-vehicle-record, education, children's privacy, and other federal requirements implicated by final implementation language.
- Identify preemption, federal-funding, interoperability, or other federal-law constraints without treating federal minimum requirements as a ceiling on protections South Carolina may lawfully provide.

# PRIMARY AUTHORITIES AND SOURCE NOTES

## Constitutional, Statutory, Legislative, and Case Authorities

### South Carolina Constitution

- S.C. Const. art. I, §2 - speech, religion, assembly, and petition.
- S.C. Const. art. I, §3 - due process and equal protection.
- S.C. Const. art. I, §10 - unreasonable searches and seizures, unreasonable invasions of privacy, probable cause, and particularity as to information to be obtained.
- S.C. Const. art. I, §22 - administrative due process and judicial review.
- S.C. Const. art. I, §23 - mandatory and prohibitory character of constitutional provisions.

### South Carolina Code

- S.C. Code Title 30, Chapter 2 - Family Privacy Protection Act.
- S.C. Code §30-2-20 — requires state entities to develop privacy policies and procedures and limits collection of personal information to information required and necessary to accomplish a legitimate public purpose.
- S.C. Code §30-2-30 — defines personal information for purposes of the Family Privacy Protection Act, including specified identifying, financial, medical, photographic, and biometric information.
- S.C. Code Title 30, Chapter 4 - Freedom of Information Act.
- S.C. Code Title 11, Chapter 35 - South Carolina Consolidated Procurement Code.
- S.C. Code §17-13-142 - electronic communications; warrants, orders, and subpoenas.
- S.C. Code Title 17, Chapter 29 - pen registers and trap-and-trace devices.
- S.C. Code Title 17, Chapter 30 - interception of wire, electronic, and oral communications.
- S.C. Code §50-3-420 - specified enforcement-officer immunity from criminal prosecution for entering private property, whether or not posted, while acting within official authority.

### South Carolina Appellate Authorities

- State v. Forrester, 343 S.C. 637, 541 S.E.2d 837 (2001) — addresses South Carolina's express constitutional privacy protection in the search-and-seizure context and recognizes that the South Carolina Constitution may afford protections beyond the federal

constitutional minimum, while declining to require police to advise an individual of the right to refuse consent before a consensual search.

- *State v. Weaver*, 374 S.C. 313, 649 S.E.2d 479 (2007) — applies Article I, §10's privacy protection in the warrantless vehicle-search context and examines the reasonableness of the governmental intrusion under South Carolina law.
- *State v. Counts*, 413 S.C. 153, 776 S.E.2d 59 (2015) — discusses South Carolina's express constitutional privacy protection in the investigative “knock and talk” context and South Carolina's authority to provide protections beyond the federal constitutional baseline.
- *Planned Parenthood South Atlantic v. State*, 438 S.C. 188, 882 S.E.2d 770 (2023) — contains extensive and differing judicial analyses concerning the history and scope of Article I, §10's “unreasonable invasions of privacy” language. Use with care for propositions extending beyond the decision's specific holding.
- *State v. Michael Lindsay Faile*, Unpublished Opinion No. 2026-UP-323 (S.C. Ct. App. July 1, 2026) — unpublished, nonprecedential opinion addressing limited warrantless use of two Flock Safety images; see Rule 268(d)(2), SCACR.

## **Current / Pending South Carolina Legislation**

### **Automated License Plate Readers**

- S. 447 (126th General Assembly) — License Plate Reader System; current-session ALPR legislation that received a favorable Senate Judiciary Committee report in 2026.
- H. 4013 (126th General Assembly) - Automated License Plate Readers.
- H. 3155 (126th General Assembly) - Automatic license plate readers.

### **Surveillance**

- H. 4675 (126th General Assembly) - Video Surveillance / South Carolina Community Data Protection and Responsible Surveillance Act

### **Image, Voice, and Likeness**

- H. 3404 (126th General Assembly) - Ensuring Likeness, Voice, and Image Security Act.

### **Children's Digital Privacy**

- H. 3400 (126th General Assembly) — Child Data Privacy and Protection Act; addresses collection, retention, processing, sale, privacy protections, parental rights, data-protection impact assessments, and related protections concerning children's personal data.

## **Prior South Carolina Legislative History**

- H. 3596 (124th General Assembly, 2021-2022) - Surveillance; proposed warrant or owner-permission requirements for state or local law-enforcement installation of surveillance equipment on farmland, timberland, fields, or other land beyond curtilage, with an evidentiary exclusion remedy. This prior-session bill is distinct from H. 3596 of the 126th General Assembly (2025-2026), the unrelated Kingston Act concerning children's access to firearms.

## **Federal Constitutional Authorities**

- U.S. Const. amends. I, IV, V, IX, and XIV.
- *Kyllo v. United States*, 533 U.S. 27 (2001) — use of sense-enhancing technology to obtain information regarding the interior of a home that could not otherwise have been obtained without physical intrusion.
- *United States v. Jones*, 565 U.S. 400 (2012) — GPS tracking involving physical installation of a tracking device; concurring opinions provide important analysis concerning prolonged technological monitoring and aggregation.
- *Riley v. California*, 573 U.S. 373 (2014) — recognizes the extraordinary quantity and qualitative character of personal information stored on modern digital devices in requiring a warrant before searching a cell phone seized incident to arrest.
- *Carpenter v. United States*, 585 U.S. 296 (2018) — addresses governmental acquisition of historical cell-site location information and declines to mechanically extend traditional third-party doctrine to the detailed location history at issue.

## **Federal Statutory Authorities**

- 18 U.S.C. §§2510 et seq. — Wiretap Act / Title III; federal definitions and requirements governing interception of wire, oral, and electronic communications.
- 18 U.S.C. §§2701-2713 — Stored Communications Act; governs access to stored electronic communications and certain provider records, including governmental process for compelled disclosure under §2703.
- 18 U.S.C. §§3121-3127 — Pen Register and Trap and Trace Device Statute; establishes federal requirements governing installation and use of pen registers and trap-and-trace devices.
- 18 U.S.C. §§2721-2725 — Driver's Privacy Protection Act; governs disclosure and permissible uses of personal information obtained from state motor-vehicle records.

## **Research and Citation Caution**

The authorities identified in this section establish important constitutional, statutory, and doctrinal principles but do not resolve every modern surveillance, digital-data, automated-decision, biometric, artificial-intelligence, or governmental-technology question addressed by the proposed framework. Holdings should be cited only for propositions they actually decide, and unpublished opinions should be identified according to their precedential status. Committee materials should distinguish existing constitutional requirements from statutory protections the General Assembly may choose to enact above the constitutional floor and should account for applicable federal preemption or other federal-law limitations.

# 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.

# Frequently Asked Questions

## Understanding the South Carolina Bill of Digital Rights

### Introduction

#### Why was the South Carolina Bill of Digital Rights created?

The South Carolina Bill of Digital Rights was created to reaffirm that the constitutional liberties secured by the United States Constitution and the South Carolina Constitution remain fully applicable in the Digital Age.

It does not seek to create new rights. Rather, it recognizes that technological advancement should not diminish freedoms that South Carolinians already possess.

Just as previous generations applied constitutional principles to telephones, automobiles, radio, television, and the Internet, this framework seeks to apply those same enduring principles to artificial intelligence, digital communications, biometric identification, surveillance technologies, connected devices, commercial data markets, and technologies yet to be invented.

Its central premise is simple:

**Technology changes. Rights do not.**

### Foundational Questions

#### What is the South Carolina Bill of Digital Rights?

A technology- neutral constitutional and legislative framework designed to preserve privacy, due process, liberty, transparency, and governmental accountability as public agencies use increasingly powerful digital technologies.

#### Why do we need a South Carolina Bill of Digital Rights?

Because nearly every aspect of modern life has become digital.

- Communication
- Banking
- Healthcare

- Travel
- Education
- Employment
- Commerce
- Government
- Personal relationships
- Political participation
- Religious practice

The Constitution protects liberty—not technology. The South Carolina Bill of Digital Rights explains how those constitutional protections apply in today's world and provides a technology-neutral framework for applying the protections of the United States Constitution and the South Carolina Constitution to the realities of modern digital life—and to technologies that have yet to be invented.

### **Doesn't the Constitution already protect these rights?**

Yes.

The United States Constitution and the South Carolina Constitution already protect the fundamental liberties at the heart of the South Carolina Bill of Digital Rights.

The purpose of the South Carolina Bill of Digital Rights is not to create new rights or replace the Constitution. It is to reaffirm and clarify how existing constitutional protections apply as technology evolves.

Constitutional rights do not become weaker simply because technology creates new ways to collect, analyze, store, or use information about people.

### **Are these new rights?**

No.

The framework begins with existing constitutional protections, including South Carolina's express protection against unreasonable invasions of privacy, and identifies statutory rules needed to make those protections meaningful in modern technological settings.

### **What legal rights do individuals retain in their digital information?**

The South Carolina Bill of Digital Rights recognizes that individuals retain constitutionally protected interests in digital information generated by, derived from, or uniquely linked to them.

This includes information concerning a person's identity, communications, precise location, biometric characteristics, activities, and other personal information.

The collection, storage, processing, transmission, analysis, licensing, or possession of that information by another person or entity does not, by itself, extinguish those constitutional protections.

This principle does not mean every piece of digital information is owned in the same way as physical property. Rather, it recognizes that constitutional rights should continue to protect individuals even when information is stored by third parties, processed by modern technologies, or transmitted through digital systems.

The central question is not simply who possesses the information.

The question is whether constitutional liberties continue to protect the individual to whom the information relates.

The South Carolina Bill of Digital Rights answers that question **yes**.

## **What is protected digital information?**

For purposes of this initiative, "protected digital information" refers to electronically stored information generated by, derived from, or uniquely linked to a person's identity, body, communications, precise location, biometrics, private activities, and other highly revealing personal information, subject to definitions and lawful exceptions in implementing legislation, including but not limited to:

- personal information
- communications
- location history
- metadata
- financial information
- health information
- biometric identifiers
- digital identity
- behavioral information
- creative works
- other personally identifiable information

## **Why do legal rights in digital information matter?**

Constitutional rights become difficult to protect if individuals lose their legal interests in personal information simply because that information is stored, transmitted, processed, or analyzed by others.

Clear legal protections help determine:

- when information may be collected;
- how it may be used;
- whether it may be disclosed or shared;
- whether it may be sold or monetized;
- who may access it;
- how long it may be retained;
- how individuals may inspect or correct it; and
- what constitutional safeguards apply when government seeks to obtain it.

The South Carolina Bill of Digital Rights recognizes that constitutional protections should follow the individual—not merely the location where information happens to be stored.

### **Does the Digital Bill of Rights mean a person owns every photograph or recording in which that person appears?**

No. A photograph, video, audio recording, or other expressive work may contain Protected Digital Information without transferring ownership of the work to the person depicted or recorded.

The protected interest concerns qualifying information about the individual - such as biometric identifiers, location, associations, behavioral information, or information derived or inferred from the image or recording - while ownership, publication, consent, and expressive rights remain governed by otherwise applicable law.

### **What is the central principle of the South Carolina Bill of Digital Rights?**

Technology changes.

Rights do not.

## **Constitutional Questions**

### **How does this relate to the Bill of Rights?**

It applies existing constitutional principles to modern technologies rather than creating new constitutional rights.

## **Isn't the Fourth Amendment already enough?**

The Fourth Amendment remains a cornerstone of American liberty.

However, new technologies raise questions that did not exist when many laws were written.

Cloud computing.

Artificial intelligence.

Commercial data brokers.

Biometric databases.

Persistent surveillance.

Connected vehicles.

The South Carolina Bill of Digital Rights provides a framework for applying longstanding constitutional protections to these modern realities.

## **Does the framework abolish the Open Fields Doctrine?**

Not by itself.

The South Carolina Bill of Digital Rights primarily governs digital information, governmental technology, surveillance, and government acquisition by proxy.

Separate implementing legislation should address governmental investigative entry onto privately owned land beyond curtilage and targeted technological surveillance of that land, while preserving warrants, valid consent by a person with lawful authority, emergencies, and other lawful authority expressly recognized by law.

## **How does this relate to the First Amendment?**

Digital platforms have become today's public square for many Americans.

Freedom of speech, religion, association, petition, and peaceful assembly deserve equal protection whether exercised in person or through digital technologies.

## **How does this relate to due process?**

No one should lose liberty, property, employment, benefits, licenses, or constitutional rights solely because an algorithm, artificial intelligence system, or automated process reached a conclusion.

Meaningful human accountability remains essential.

## **Why discuss property rights at all?**

Property rights have long been one of the principal safeguards of individual liberty under American law.

As more of life becomes digital, questions naturally arise regarding the legal interests individuals retain in information generated by, derived from, or uniquely linked to them.

The South Carolina Bill of Digital Rights does not depend upon resolving every question of technical ownership under property law. Instead, it recognizes that constitutional protections should not disappear simply because information is stored by a third party, processed by modern technologies, or transmitted through digital systems.

Whether analyzed through the principles of property, privacy, liberty, or due process, technological advancement should never diminish the constitutional rights retained by the people.

## **Does this require changing the Constitution?**

Not necessarily.

Many of these principles can be implemented through legislation while remaining fully consistent with existing constitutional protections.

## **Does this apply to private companies as well as government?**

The Constitution primarily limits government action.

However, governments increasingly partner with private companies to provide services, manage data, develop artificial intelligence, operate surveillance technologies, and store public information.

The South Carolina Bill of Digital Rights recognizes that constitutional protections should not be circumvented simply because government relies upon contractors, vendors, nonprofit organizations, or other third parties.

It also encourages legislatures to establish appropriate standards governing how private entities collect, use, retain, share, and monetize personal information while respecting individual rights.

### **Why doesn't this simply call for more privacy?**

Privacy is only one constitutional principle.

The South Carolina Bill of Digital Rights also protects:

- liberty
- property
- due process
- transparency
- accountability
- freedom of speech
- freedom of religion
- freedom of association
- freedom of movement
- human dignity

Privacy exists to protect liberty—not replace it. The purpose of this bill is to preserve the broader constitutional framework that allows free people to flourish.

## **Government Questions**

### **Is this anti-government?**

No.

Government has legitimate responsibilities.

This framework supports constitutional government.

It simply recognizes that government power should remain subject to constitutional limitations.

### **Is this anti-law enforcement?**

No.

Law enforcement plays an essential role in protecting public safety.

Nothing in this framework prevents lawful investigations conducted with appropriate legal authority.

### **Does this prevent police from solving crimes?**

No.

The framework recognizes warrants, judicial oversight, due process, and existing constitutional exceptions such as emergencies.

It addresses how government obtains and uses information—not whether crimes should be investigated.

### **Does this interfere with lawful law enforcement?**

No.

Implementing legislation should preserve constitutional warrant exceptions, emergencies, and legitimate investigative authorities through express and narrow provisions.

### **What about emergencies?**

Existing constitutional principles recognize emergency exceptions.

Nothing in this framework is intended to interfere with emergency response or imminent threats to life.

## **What about terrorism or child exploitation?**

These are serious crimes.

The South Carolina Bill of Digital Rights does not eliminate lawful investigative authorities.

It emphasizes that extraordinary investigations should still operate within constitutional and statutory safeguards.

## **Should government ever use AI?**

Yes.

Artificial intelligence can improve efficiency and assist decision-making.

However, government should remain accountable for decisions affecting constitutional rights.

AI should assist people—not replace due process.

## **What is a high-consequence governmental digital system?**

A functional category for digital, automated, algorithmic, electronic, or computational systems that materially make, record, calculate, authenticate, recommend, transmit, certify, or influence official governmental actions affecting significant legal interests.

## **Should government use surveillance technology?**

Sometimes, yes.

The question is not whether surveillance technologies exist.

The question is what constitutional safeguards govern their use.

## **What does “procurement is not authorization” mean?**

The authority to buy or license a product is not automatically substantive authority to use every capability the product offers. Governmental power must come from the Constitution and law.

## **Does vendor secrecy block oversight?**

It should not. Legitimate trade secrets can be protected from unnecessary public disclosure while still being available to courts, auditors, inspectors, legislators, and other lawful oversight bodies when necessary.

## **What about public records and sensitive information?**

The framework does not erase existing FOIA exemptions. It distinguishes public disclosure from lawful oversight access and requires segregation and disclosure of nonexempt material where current law requires it.

## **What is Aggregated Surveillance?**

Aggregated surveillance occurs when many individual observations are combined over time to create a detailed picture of a person's life.

A single observation may reveal very little. Thousands or millions of observations collected over days, months, or years can reveal where a person lives, works, worships, receives medical care, whom they associate with, where they travel, and many other aspects of daily life.

The constitutional concern arises not from any single observation, but from the government's ability to aggregate, retain, correlate, and analyze large amounts of information into a comprehensive record of an individual's activities.

Duration, precision, continuity, retrospective capability, aggregation, and pattern-of-life reconstruction can matter even when an isolated observation reveals little.

## **Why isn't one camera the issue?**

One camera observing one location has existed for decades.

The constitutional question is not whether individual cameras exist.

The question is whether modern technologies allow government or private entities acting on behalf of government to combine information from thousands of cameras, databases, sensors, automated license plate readers, mobile devices, commercial data brokers, and other technologies into persistent records that reveal a person's movements, associations, and private life.

The South Carolina Bill of Digital Rights does not oppose individual technologies simply because they exist. It recognizes that constitutional protections must account for the capabilities created when many technologies operate together.

Technology changes.

Rights do not.

### **What is government acquisition by proxy?**

The principle that government should not evade constitutional process by purchasing, licensing, querying, requesting, or receiving substantially equivalent protected information through a broker, vendor, contractor, shared system, or other intermediary.

### **Why shouldn't government accomplish indirectly what it cannot do directly?**

Constitutional limitations exist to protect liberty.

Those protections should not disappear simply because information is obtained through contractors, data brokers, vendors, nonprofit organizations, or other third parties.

Government should not be able to avoid constitutional safeguards by outsourcing activities that would otherwise require judicial authorization.

### **Does this prevent existing investigations?**

No.

Nothing in the South Carolina Bill of Digital Rights is intended to invalidate lawful investigations or existing judicial authorities.

Its purpose is to ensure that future investigations continue to operate within constitutional safeguards while protecting the rights of innocent citizens.

### **Would this affect existing surveillance systems?**

Not necessarily.

The South Carolina Bill of Digital Rights does not require eliminating every existing surveillance technology.

Instead, it encourages legislatures to evaluate whether existing systems operate with sufficient constitutional safeguards, transparency, accountability, judicial oversight, and public oversight.

Some systems may require little or no change, while others may warrant additional safeguards depending on how they are used.

## **Technology Questions**

### **Is this only about Flock cameras?**

No.

Flock is one example among many.

This document applies broadly to current and future technologies.

### **Does this apply to...**

- Artificial Intelligence?

Yes.

- Automated License Plate Readers?

Yes.

- Drones?

Yes.

- Facial Recognition?

Yes.

- Connected Vehicles?

Yes.

- Smartphones?

Yes.

- Smart Homes?

Yes.

- Social Media?

Yes.

- Government Databases?

Yes.

- Data Brokers?

Yes.

- Future Technologies?

Yes.

The principles remain the same regardless of technology.

### **Why avoid naming specific technologies?**

Technology changes rapidly.

Constitutional principles endure.

The document is intended to remain relevant decades into the future.

### **What is meant by "technology-neutral"?**

Technology-neutral means constitutional rights should never depend upon the technology involved.

Whether information is collected through:

- paper records
- telephones
- computers

- smartphones
- drones
- satellites
- automated license plate readers
- connected vehicles
- wearable devices
- artificial intelligence
- or technologies yet to be invented—

the constitutional principles remain the same.

Technology changes.

Rights do not.

### **Is this anti-technology?**

No. Government may use technology. The proposal says technology does not itself create governmental authority or eliminate constitutional accountability.

### **What does independent human review mean?**

An identified human decision-maker must have authority and sufficient information to independently evaluate, reject, correct, or modify a material automated determination. Merely rubber-stamping an automated output is not meaningful review.

### **What does independent verification mean?**

For designated consequential outcomes, government should be capable - where reasonably practicable and required by law - of verifying a material result without relying exclusively on the same system being examined.

## **Does that mean computers cannot be used?**

No. It is an integrity principle, not a technology ban. Different systems may satisfy independent verification through different evidence or review mechanisms appropriate to their function.

## **Why require audit logs?**

Because meaningful oversight requires the ability to reconstruct material system activity, including administrative access, configuration changes, versions, updates, data transfers, remote access, automated actions, errors, and security events.

## **Why does the document avoid naming specific companies?**

Companies change.

Technology changes.

Constitutional principles endure.

The South Carolina Bill of Digital Rights is intended to remain relevant regardless of which companies develop or market future technologies.

Its purpose is to establish enduring constitutional principles rather than regulate individual businesses or products.

## **Does foreign manufacture make a system unsafe?**

No. Foreign manufacture alone does not establish compromise. The relevant concerns are material foreign control, data access, remote administration, software/update authority, authentication, cloud dependencies, and other operational dependencies.

## **What about commercial off-the-shelf components?**

The use of commercial off-the-shelf components does not, by itself, establish that a governmental system is secure or insecure.

The relevant questions include the component's function, access to protected information, software and firmware dependencies, update authority, remote administration capabilities,

authentication, network connectivity, supply-chain dependencies, auditability, and whether the component can materially affect or influence a consequential governmental outcome.

Security and accountability should be evaluated based on the function and capabilities of the component within the system, not merely where the component was manufactured or whether it is commercially available.

## **What if a certified system or component is compromised?**

Certification, testing, procurement approval, or compliance with a technical standard should not be treated as conclusive proof that a consequential governmental system is secure, accurate, or constitutionally compliant.

For designated high-consequence governmental systems, meaningful accountability may require independent verification, auditability, supply-chain transparency, integrity controls, and evidence sufficient to evaluate material outcomes without relying exclusively upon the same system, component, vendor, manufacturer, testing process, or certifying authority being examined.

The purpose is not to presume that a particular manufacturer, country, component, or certifying body is untrustworthy. It is to ensure that public accountability does not depend exclusively upon institutional or technological trust.

## **Privacy Questions**

### **If I have nothing to hide, why should I care?**

Privacy is not about hiding wrongdoing.

Privacy protects autonomy.

It protects freedom of thought.

Freedom of association.

Religious liberty.

Medical confidentiality.

Attorney-client relationships.

Journalism.

Political participation.

Constitutional rights protect everyone—not only those accused of crimes.

### **Isn't there no expectation of privacy in public?**

Public observation has long existed.

Modern technology, however, can aggregate millions of observations into detailed histories revealing patterns of life, associations, routines, and personal activities.

The South Carolina Bill of Digital Rights argues that technological advances should not erode constitutional protections simply because surveillance has become more comprehensive.

### **Does third-party possession automatically erase privacy protection?**

The framework says no. Third-party collection or possession, standing alone, should not automatically extinguish the constitutional inquiry.

### **What is a "pattern of life"?**

A pattern of life is a detailed picture of an individual's routine built from accumulated data over time.

It may reveal:

- where someone lives
- works
- worships
- shops
- receives medical care
- who they associate with
- their daily habits
- their political activities
- their travel

Modern technologies can generate these profiles without any single observation being especially revealing.

## **What is metadata?**

Metadata is information about information.

Examples include:

- time
- date
- location
- recipient
- device
- duration

Even without message content, metadata can reveal extensive information about an individual's life.

## **Why are biometrics different?**

Unlike passwords, biometric characteristics cannot easily be changed.

Once compromised, facial characteristics, fingerprints, iris scans, DNA, and voiceprints remain compromised indefinitely.

## **Should people be able to see government information about themselves?**

Whenever consistent with legitimate law enforcement needs and existing legal protections, individuals should have meaningful opportunities to know what information government maintains about them and to correct demonstrably inaccurate information.

## **Should people have the right to delete government information about themselves?**

Government has legitimate reasons to retain certain records.

However, where information no longer serves a lawful governmental purpose and retention is not otherwise required by law, legislatures should consider establishing reasonable procedures governing deletion, anonymization, or limited retention of personal information.

Such procedures should balance individual liberty with legitimate governmental needs.

## **What happens when government databases contain incorrect information?**

Government decisions increasingly rely upon digital information.

Inaccurate records can affect employment, licensing, benefits, investigations, reputation, and constitutional rights.

Individuals should have meaningful opportunities to inspect government records concerning themselves, challenge demonstrably inaccurate information, and seek timely correction through fair administrative procedures.

## **Business Questions**

### **Is this anti-business?**

No.

Clear rules create trust.

Trust encourages innovation.

Responsible businesses benefit from predictable legal standards.

### **Can companies sell my information?**

Current law varies by jurisdiction and by the type of information involved.

The South Carolina Bill of Digital Rights argues that individuals should have meaningful rights regarding how their personal information is collected, used, and shared.

### **Will this hurt innovation?**

Innovation and liberty are complementary.

Strong constitutional protections encourage responsible innovation and public confidence.

## **What is informed consent?**

Meaningful consent requires more than simply clicking "I Agree."

Individuals should understand:

- what information is collected;
- why it is collected;
- how it will be used;
- how long it will be retained;
- who will receive it;
- whether it will be sold or shared; and
- how consent may be withdrawn when appropriate.

Consent should be informed, voluntary, and understandable.

## **Will this increase costs?**

Possibly.

Protecting constitutional rights sometimes requires investments in cybersecurity, auditing, transparency, oversight, and responsible data management.

Throughout American history, preserving liberty has required resources.

The South Carolina Bill of Digital Rights recognizes that protecting constitutional freedoms is a necessary investment in a free society and that clear standards may also reduce long-term costs associated with litigation, uncertainty, and loss of public trust.

## **Practical Questions**

### **How would the South Carolina Bill of Digital Rights be implemented?**

The South Carolina Bill of Digital Rights establishes principles for protecting constitutional liberty as technology evolves.

Those principles may be implemented through legislation governing governmental technology, digital information, surveillance, automated systems, procurement, auditability, transparency, due process, and related areas.

Implementation should remain consistent with the Constitutions of South Carolina and the United States and with applicable federal law.

### **How would violations be enforced?**

Enforcement would depend upon the implementing legislation and the right or requirement involved.

Potential enforcement mechanisms may include judicial review, injunctive or declaratory relief, administrative or legislative oversight, preservation and correction requirements, civil remedies, attorney fees and costs where authorized, and other remedies provided by law.

### **Would this create more lawsuits?**

It could result in litigation where the meaning or application of a new law is disputed.

However, one purpose of implementing legislation is to establish clearer standards governing governmental authority, individual rights, technological systems, and accountability.

The goal is not to encourage litigation. The goal is to establish clear, enforceable rules so that government, individuals, vendors, oversight bodies, and courts understand the rights and responsibilities that apply.

### **Could the South Carolina Bill of Digital Rights become part of the South Carolina Constitution?**

The South Carolina Bill of Digital Rights is written as a statement of constitutional principles grounded in protections already recognized by the South Carolina and United States Constitutions.

Many of its principles can be implemented through legislation. Particular protections could also be proposed as amendments to the South Carolina Constitution through the constitutional amendment process.

Whether any provision should ultimately be placed in the South Carolina Constitution would be a separate decision made through that process.

## **Philosophical Questions**

### **Can liberty survive if every movement is permanently recorded?**

This is one of the defining questions of the Digital Age.

The South Carolina Bill of Digital Rights recognizes that freedom depends not only upon what government may lawfully do, but also upon limits on governmental power.

Persistent, aggregated, historical, or retrospective surveillance can reveal far more about a person's life than any single observation. Constitutional protections should therefore remain meaningful even as technology makes increasingly comprehensive surveillance possible.

### **Why should constitutional rights be technology-neutral?**

Because liberty should not expand or diminish merely because technology evolves.

The Constitution governs government.

Technology does not redefine constitutional limits.

A constitutional protection should not depend upon whether government uses a camera, database, algorithm, artificial intelligence system, biometric system, commercial data source, or a technology that has not yet been invented.

### **How do we balance liberty and security?**

Liberty and security are not opposing goals.

A free society requires both.

Our constitutional system permits government to protect public safety while limiting governmental power through due process, judicial oversight, particularized legal process, transparency, accountability, and the rule of law.

The South Carolina Bill of Digital Rights follows that principle by recognizing that legitimate governmental authority and constitutional liberty can coexist. Public safety does not require abandoning constitutional protections simply because new technology makes broader surveillance, collection, or analysis possible.

### **Is this a technology problem or a constitutional problem?**

Technology and artificial intelligence are not inherently threats to liberty.

The central question is whether constitutional principles continue to govern how government uses them.

The South Carolina Bill of Digital Rights is not based upon the premise that technology is inherently good or bad. It recognizes that technological capability does not itself create governmental authority.

Every generation has a responsibility to ensure that enduring principles of liberty, privacy, due process, property rights, transparency, accountability, and limited government remain meaningful as technology changes.

Technology will continue to evolve. Constitutional protections must endure.

# **The Future**

## **Why now?**

Artificial intelligence, biometrics, automated decision-making, connected infrastructure, digital identity systems, commercial data markets, and increasingly powerful surveillance and analytical technologies are developing rapidly.

Government's technological capabilities are changing faster than many laws were written to anticipate.

The South Carolina Bill of Digital Rights is intended to establish durable, technology-neutral principles before particular technologies or practices become so embedded in governmental systems that constitutional questions are addressed only after problems occur.

The goal is not to predict every technology that will exist in the future.

It is to establish principles capable of governing technologies that do not yet exist.

## **What happens if we do nothing?**

Technology will continue to evolve whether the law addresses these questions or not.

Government will gain new capabilities to collect, aggregate, analyze, share, and act upon digital information. Automated systems will increasingly be capable of influencing governmental decisions and consequential outcomes.

The question is whether constitutional protections remain meaningful as those capabilities change.

The South Carolina Bill of Digital Rights is intended to ensure that technological capability does not, by itself, redefine the limits of governmental authority.

## **What can citizens do?**

Read the South Carolina Bill of Digital Rights and the proposed implementing legislation.

Consider how its principles would apply to government technologies and practices in your own community and across South Carolina.

Ask questions. Provide constructive feedback. Participate in public meetings and legislative processes. Discuss these issues with civic organizations, elected officials, policymakers, legal scholars, technology professionals, law enforcement, and other members of the community.

Most importantly, remain engaged in the continuing discussion about how constitutional rights should be protected as governmental technology evolves.

## **Why begin this effort in South Carolina?**

South Carolinians have long taken pride in being First in the South—not simply as a matter of chronology, but as a reflection of the state's willingness to engage consequential questions about government, liberty, and the relationship between citizens and the state.

Throughout American history, South Carolina has often played an outsized role in shaping debates about constitutional government, federalism, individual liberty, and the proper limits of governmental power.

Today, the Digital Age presents a new constitutional challenge. As technology rapidly transforms how Americans communicate, travel, work, worship, conduct business, and interact with government, states have an opportunity to help define how timeless constitutional principles should be applied to modern realities.

South Carolina also has a unique historical connection to this discussion. The modern Open Fields Doctrine traces its origins to *Hester v. United States* (1924), a case arising from South Carolina. More recently, South Carolina has become part of the national conversation regarding automated license plate reader systems, digital surveillance, and government transparency.

If constitutional liberty is to remain meaningful in the Digital Age, someone must be willing to lead that conversation.

Just as South Carolina has often been First in the South in shaping important national debates, this initiative seeks to encourage South Carolina to once again lead—not by being first for its own sake, but by helping ensure that the enduring principles of liberty continue to guide America in a rapidly changing technological world.

## **What is the General Assembly being asked to do now?**

Move the principles of the South Carolina Bill of Digital Rights toward enforceable law.

That means defining covered information, technologies, and governmental systems; establishing clear standards, processes, and oversight; modernizing conflicting or outdated provisions of South Carolina law; closing statutory gaps; and providing meaningful mechanisms for accountability and enforcement.

The goal is not to regulate technology by brand, vendor, or product name.

It is to regulate governmental power by function and effect—so that constitutional protections remain meaningful regardless of the technology government uses.

## **Final Thought**

The South Carolina Bill of Digital Rights rests on one enduring principle:

**Liberty is timeless. Technology is temporary.**

The Constitutions of South Carolina and the United States were written to secure the rights of the people—not to preserve the technologies of a particular era.

Technology will continue to evolve. The tools available to government will change. New capabilities will emerge that previous generations could not have imagined.

But technological capability does not redefine constitutional limits, and constitutional protections should not diminish simply because the means of collecting information, exercising governmental power, or making consequential decisions have changed.

**Technology changes. Rights do not.**