

# 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.