Model Language: Surveillance Technology Regulation Act

Purpose:

For the purpose of prohibiting the use of certain surveillance technology by a government entity except under certain circumstances; establishing the Surveillance Technology Board in the Department of Public Safety and Correctional Services for certain purposes relating to the use of surveillance technology by a government entity; requiring a government entity to submit certain reports to the Board for surveillance technology used by the entity; and generally relating to the acquisition and use of surveillance technology by government entities.

Text:

Section 1. Definitions.

1. "**Board**" means the Surveillance Technology Board.
2. "**Exigent circumstances**" means the good faith belief by a government entity that there is a danger of, or an imminent threat of the destruction of evidence regarding, death of or serious threat of the destruction of evidence regarding, death of or serious bodily injury to a person.
3. "**Government entity**" means
    a. the state, a county, a municipality, a higher education institute, a local district, a special service district, a school district, an independent entity, or any other political subdivision of the state or an administrative subunit of any political subdivision, including a law-enforcement entity; or
    b. an agent of an entity described above.
4. **"Third Party"** means a party, different from the person or government, who maintains digital information about the person as part of providing that person goods or services.
5. "**Surveillance Technology**" means
    a. any software or electronic device system primarily intended to collect, retain, analyze, process, or share information in the form of audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group; or
    b. software designed to monitor social media services or forecast criminal activity or criminality.

Section 2. Use of Surveillance Technology Prohibited.

1. Except as provided in this subtitle, a government entity may not:
    a. acquire or use surveillance technology;
    b. enter into a contract or agreement with a third party to use surveillance technology;
    c. collect, analyze, or store data that would not have been obtained without the use of surveillance technology.

Section 3. Audit of Surveillance Technology.

1. All government entities that use or have used surveillance technology in the last ten years must submit a report to the state auditor by [INSERT DATE].
2. The report shall include:
    a. A description of each surveillance technology that was used by the entity;
    b. A description of how each surveillance technology was used, including the type and quantity of data gathered by each surveillance technology;
    c. How often data acquired through the use of the surveillance technology was shared with an outside entity, including:
        i. The name of the recipient entity;
        ii. The type of data disclosed; and
        iii. Justification for the disclosure;
    d. A general description of where each surveillance technology was deployed geographically within the jurisdiction of the government entity;
    e. A summary of community complaints or concerns about each surveillance technology;
    f. Any specific measures taken to protect individual civil rights and civil liberties from possible infringement by a surveillance technology;
    g. Any data breach or unauthorized access to the data collected by each surveillance technology and any action taken in response;
    h. The total annual fiscal cost of each surveillance technology, including personnel and ongoing costs; and
    i. Information and relevant crime statistics to help assess whether each surveillance technology has been effective at achieving the identified purpose.
3. Any report required under this section shall be a public record.

Section 4. Role of State Auditor.

1. The State Auditor shall:
    a. Appoint the members of the Surveillance Technology Board described in Section 5 of this code;
    b. Receive and review annual reports and impact reports from any government entity using surveillance technology;
    c. Submit a summary with a copy of each report to the Surveillance Technology Board;
    d. Publish the findings and decisions made by the State Auditor and Surveillance Technology Board.
    e. The Office of the State Auditor shall provide staff for the Board.

Section 5. The Surveillance Technology Board

1. There is created, within the Office of the State Auditor, the Surveillance Technology Board.
2. The Board consists of the following members:

a. The President of the [INSERT STATE] State's Attorneys' Association, or the President's Designee;
b. The [INSERT STATE] Public Defender, or the Public Defender's designee; and
c. The following members, appointed by the State Auditor:
    i. A representative from a privacy advocacy organization with recognized expertise in defending civil liberties;
    ii. A legal academic with recognized expertise with Fourth Amendment jurisprudence.
    iii. Two representatives from law enforcement, one of whom shall, at the time of appointment, serve in local law enforcement;
    iv. Two representatives with experience in cybersecurity;

d. A chair from among the Board's members shall be selected by the governor.

3. The term of a member is four years.
    a. At the end of a term, an appointed member continues to serve until a successor is appointed and qualifies.
    b. A member who is appointed after a term has begun serves only for the rest of the term and until a successor is appointed and qualifies.
    c. A member may be reappointed to the Board.
4. A Board member:
    a. Shall refrain from participating in a review of:
        i. An entity of which the member is an employee; or
        ii. A technology in which the member has a financial interest.
    b. May not receive compensation for serving on the Board; but
    c. Is entitled to reimbursement for expenses under the standard state travel regulations, as provided in the state budget.
5. A majority of the Board's members constitutes a quorum.
6. The Board may adopt rules for conducting business.
7. The Board shall:
    a. Authorize, restrict, or prohibit the purchase, use, or continued use of surveillance technology by government entities;
    b. Authorize, restrict, or prohibit the use of existing surveillance technology or the information that the surveillance technology provides for a purpose, in a manner, or in a location not previously authorized by the Board;
    c. Hold quarterly meetings with the heads of government entities utilizing surveillance technologies and providers of those technologies to review surveillance impact reports, required under Section 7, submitted by the government entity;
    d. Receive public input about proposed surveillance technologies;
    e. Review annual reports, required under Section 7, by government entities on the operation of surveillance technology used for the previous calendar year; and
    f. Make publicly available the annual surveillance reports and surveillance impact reports required under Section 7.

g. Determine, if a government entity is using surveillance technology that fails to meet minimum acceptable standards, whether to require the government entity to:
    i. If the government entity is a state entity, terminate the use of that technology or policy on or before [INSERT DATE] of the year following the notification.
    ii. If the government entity is a local government entity, terminate the use of that surveillance technology within 180 days after the day on which the local government entity receives notice of the determination.

Section 6. Board Authorization

1. Each government entity shall obtain authorization from the Board before:
    a. Accepting state funds, federal funds, or any other funds for surveillance technology;
    b. Acquiring new surveillance technology;
    c. Using new surveillance technology;
    d. Using existing surveillance technology or the information that the surveillance technology provides for a purpose, in a manner, or in a location not previously authorized by the Board.
2. Each authorization granted by the Board for surveillance technology shall sunset after one year, at which point the State Auditor and the Board shall perform a review to determine if anything has changed about the use of authorized surveillance technology. If so, the State Auditor and Board shall review it.
3. Any government entity found using surveillance technology without authorization of the Board must terminate within 180 days all use of unauthorized surveillance technology and permanently destroy in an unrecoverable manner any data collected by the unauthorized technology.
4. Board authorizations do not exempt law enforcement or other government entities from search warrant requirements found in [INSERT STATE CODE FOR SEARCH WARRANTS]

Section 7. Impact Report and Annual Surveillance Report.

1. Before seeking authorization from the Board, each government entity shall submit a surveillance impact report to the Board for each surveillance technology to be used by the entity.
2. A surveillance impact report shall include:
    a. A description of the surveillance technology;
    b. The proposed use for the surveillance technology;
    c. General descriptive terms of any location the surveillance technology is intended to be used within the jurisdiction of the government entity and the crime statistics for the locations;
    d. Whether the surveillance technology has been used or deployed in a manner that is discriminatory, viewpoint-biased, or algorithm-biased;

e. Any specific technical or procedural measure that will be implemented to safeguard the public from possible discriminatory surveillance;
f. A list of the types and sources of data to be collected, analyzed, or processed by the surveillance technology;
g. Information regarding any third party that the information may be shared with or accessed by;
h. The time period for which information collected from the surveillance technology will be retained by the agency;
i. The steps that will be taken to ensure that adequate security measures are used to safeguard the data from unauthorized access;
j. The fiscal cost for the proposed surveillance technology, including initial purchase and ongoing costs;
k. A summary of alternative methods considered before deciding to use the proposed surveillance technology; and
l. A summary of other known entities that use the proposed surveillance technology and any known experience with the proposed surveillance technology.

3. A government entity that is approved by the committee to use any surveillance technology must annually submit the report provided in Section 3(2).
    a. Failure to provide the annual report will result in immediate termination of Board authorization for use of any surveillance technology.
4. A government entity that ceases to use any approved surveillance technology must notify the State Auditor and Board and provide a final report.
5. Any report required under this section shall be a public record.

Section 8. Penalties.

1. A violation of this subtitle constitutes an injury, and a person may institute proceedings for injunctive relief or declaratory relief to enforce this subtitle.
2. A person who has been subjected to a surveillance technology, or who has had personal information obtained, retained, accessed, shared, or used in violation of this subtitle may institute proceedings against the government entity and shall be entitled to recover actual damages of $100 per day for each day of the violation.
3. In any action brought to enforce this subtitle, a court may award reasonable attorney's fees to a prevailing plaintiff.
4. All information obtained by a surveillance technology in violation of the chapters above shall be inadmissible in a court of law.

To learn more about this model language, please contact David Iglesias at david@libertas.org