The Privacy Protection Act

Purpose:

This proposal establishes criteria for the government's adoption of new and emerging surveillance technologies while ensuring privacy protections for individuals.

Text:

Section 1. Definitions

1. "Commission" means the Personal Privacy Oversight Committee created in Section 4.
2. (a)"Government entity" means the state, 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.
   (b) "Government entity" includes an agent of an entity described in Subsection (2)(a).
3. "Independent entity" means the same as that term is defined in (INSERT RELEVANT STATE CODE).
4. (a) "Personal data" means any information relating to an identified or identifiable individual.
   (b) "Personal data" includes personally identifying information.
5. (a) "Privacy practice" means the acquisition, use, storage, or disposal of personal data.
   (b) "Privacy practice" includes:
      i. a technology use related to personal data; and
      ii. policies related to the protection, storage, sharing, and retention of personal data.

Section 2. Auditor's Role

Note: State code will need to be amended to allow for the state auditor's office to oversee the privacy officer and the committee established in this proposal while establishing an avenue for the state auditor to publish their findings, as well as recommendations.

1. The state auditor shall:

a. with the advice and consent of the Senate, appoint the state privacy officer described in Section 3;
b. appoint the members of the Personal Privacy Oversight Committee described in Section 4;
c. publish the reviews and recommendations made by the state privacy officer and the Personal Privacy Oversight Committee; and
d. determine, upon notification from the Personal Privacy Oversight Committee that a government entity is using a technology or privacy policy that fails to meet minimum acceptable standards, whether to require the government entity using the technology or policy to:
    i. if the government entity is a state entity, terminate the use of that technology policy on or before June 1 of the year following the notification unless the Legislature authorizes the continued use of that technology or policy in statute; or
    ii. if the government entity is a local government entity, terminate the use of that technology or policy within 180 days after the day on which the local government entity receives notice of the determination unless the local government authorizes the continued use of that technology or policy.

Section 3. Creation of State Privacy Officer

The state privacy officer shall:

1) based on recommendations from the Personal Privacy Oversight Committee, develop guiding standards for best practices with respect to government privacy policy, technology uses related to personal privacy, and data security;
2) based on recommendations from the Personal Privacy Oversight Committee, develop minimum acceptable standards for government privacy policies and technology uses related to personal privacy;
3) compile information about government privacy policy, technology uses related to personal privacy, and data security;
4) make public and maintain information about government privacy policy, technology uses related to personal privacy, and data security on the state auditor's website;
5) provide government entities with educational and training materials developed with the input of the Personal Privacy Oversight Committee that include the following information:
    a) the privacy implications and civil liberties concerns of the government use of certain technologies;

b) best practices for government collection and retention policies regarding personally identifiable information;
c) best practices for government data security standards; and
d) the purpose and the process of the state privacy officer and the Personal Privacy Oversight Committee

6) implement a process to analyze and respond to requests from individuals for the state privacy officer to review a government entity's use of technology that implicates the privacy of individuals' data;
7) identify annually which government entity's technology use of technology that implicates the privacy of individuals' data;
8) review each year, in as timely a manner as possible and with the assistance of the Personal Privacy Oversight Committee, the technology uses and privacy policies that the privacy officer identifies under Subsection (6) or (7) as posing the greatest risk to individuals' privacy;
9) when reviewing a government entity's use of technology or privacy policy under Subsection (8), include in the review:
    a) details about the technology or the policy and the technology's or the policy's application;
    b) information about the type of data being used;
    c) information about how the data is obtained, stored, kept secure, and disposed;
    d) information about with whom the government entity shares the information;
    e) information about whether an individual can or should be able to opt out of the retention and sharing of the individual's data;
    f) information about how the government entity de-identifies or anonymizes data;
    g) a determination about the existence of alternative technology or improved practices to protect privacy; and
    h) a finding of whether the current government entity's use of technology or policy adequately protects individual privacy;
10) after completing a review described in Subsection (9), determine:
    a) each entity's use of personally identifying information, including the entity's practices regarding data:
        i) retention;
        ii) storage;
        iii) protection; and
        iv) sharing;
    b) the adequacy of the entity's practices in each of the areas described in Subsection (10)(a); and

c) for each of the areas described in Subsection (10)(a) that require reform, provide recommendations to the government entity for reform; and

11) annually report, on or before October 1, to the Judiciary Interim Committee:
    a) the results of the reviews described in Subsection (8), if any reviews have been completed;
    b) the information described in Subsection (10); and
    c) recommendations for legislation based on the guiding standards and minimum standards described in Subsections (1) and (2).

Section 4. Personal Privacy Oversight Committee

1) There is created within the Office of the State Auditor the Personal Privacy Oversight Committee.
2) (a) The committee shall be composed of the following members appointed by the state auditor:
    i) two members with experience in internet technology services, one of whom shall, at the time of appointment, provide internet technology services for a county or municipality;
    ii) two members with experience in cybersecurity;
    iii) two members representing private industry in technology;
    iv) two members representing law enforcement, one of whom shall, at the time of appointment, serve in local law enforcement;
    v) two members with experience in data privacy law;
    vi) one member with experience in data privacy policy; and
    vii) one member with experience in civil liberties law or policy and with specific experience in identifying whether the use of a technology or policy may result in disparate impacts on different populations.
    b) the committee shall be composed of one member with experience in civil liberties law who is appointed by the attorney general and, at the time of appointment, is an assistant attorney general.
3) (a) Except as provided in Subsection (3)(b), the auditor shall appoint a member for a term of four years.

    b) The state auditor shall, at the time of appointment or reappointment, adjust the lengths of the terms to ensure that the terms of committee members are staggered so that approximately half of the committee is appointed every two years.

    c) When the term of a committee member expires, the state auditor shall reappoint the member or appoint a new member in accordance with this Subsection (3).

4) (a) When a vacancy occurs in the membership for any reason, the state auditor shall appoint a replacement in accordance with Subsection (3) for the unexpired term.

b) A member whose term has expired may continue to serve until a replacement is appointed.

5) (a) The state privacy officer shall serve as chair of the committee.

b) The committee shall select officers from the committee's members as the committee finds necessary.

6) A majority of the members of the committee is a quorum.

7) A member may not receive compensation or benefits for the member's service but may receive per diem and travel expenses incurred as a member of the committee.

8) A member shall refrain from participating in a review of:
   a) an entity of which the member is an employee; or
   b) a technology in which the member has a financial interest.

9) The committee shall meet as required by the state privacy officer to accomplish the duties described in Subsection (10).

10) (a) At the request of the state privacy officer, the committee shall review the proposed and current uses of technology described in Section (3) Subsection (8).

b) The committee shall notify the state auditor if the committee finds that a government entity's use of technology or privacy policy does not comply with the minimum acceptable standards of privacy protection described in Section (3) Subsection(2).

c) If the committee finds that a use of technology or a policy reviewed under Subsection (10)(a) does meet the minimum acceptable standards of privacy protection, the committee shall review the technology use or policy again two years following the date of the initial review to determine if the use still meets acceptable privacy standards.

To learn more about this model language, please contact Rees Empey at rees@libertas.org