Model Language: Government's Use of Facial Recognition Technology

Purpose:

This proposal implements guardrails on the government's use of facial recognition technology.

Text:

Section 1. Definitions.

1. "Authorized database" means a database maintained by the department that contains only:
   a. images of an individual taken when the individual applies for a license certificate or identification card; or
   b. images of an individual taken when the individual is taken into custody by a law enforcement agency or the Department of Corrections.
2. "Department" means the Department of Public Safety.
3. "Facial biometric data" means data derived from a measurement, pattern, contour, or other characteristic of an individual's face, either directly or from an image.
4. "Facial recognition comparison" means the process of comparing an image or facial biometric data to an authorized database.
5. a) "Facial recognition system" means a computer system that, for the purpose of attempting to determine the identity of an unknown individual, uses an algorithm to compare biometric data of the face of the unknown individual to biometric data in a database of facial images, or a database of biometric data taken from facial images, of known individuals.
   b) "Facial recognition system" does not include a system described in Subsection (5)(a) that is available for use, free of charge, by the general public.
6. "Government entity" means:
   i. an executive department of the state;
   ii. the office of the governor, lieutenant governor, state auditor, attorney general, or state treasurer;
   iii. the Board of Pardons and Parole,
   iv. the Board of Examiners;
   v. the National Guard;
   vi. the Career Service Review Officer;
   vii. the State Board of Education;
   viii. the State Board of Regents;

       ix.   the State Archives;

       x.   the Office of the Legislative Auditor General;

       xi.   the Office of the Legislative Fiscal Analyst;

       xii.   the Office of Legislative Research and General Counsel;

       xiii.   the Legislature;

       xiv.   a legislative committee of the Legislature;

       xv.   a court, the Judicial Council, the Administrative Office of the Courts, and similar administrative units in the judicial branch;

       xvi.   a state-funded institution of higher education or public education; or

       xvii.   a political subdivision of the state.

    b. "Government entity" includes:

       i.   every office, agency, board, bureau, committee, department, advisory board, or commission of an entity described in Subsection (6)(a) that is funded or established by the government to carry out the public's business; or

       ii.   a person acting as an agent of an entity described in Subsection (6)(a) or (6)(b)(i) or acting on behalf of the entity.

7. "Law enforcement agency" means a public entity that exists to primarily prevent, detect, or prosecute crime or enforce criminal statutes or ordinances.

Section 2. Restrictions on Government's Use of Facial Recognition Systems.

1. Except as provided in this section, a government entity may not use a facial recognition system.

2. a) The department is the only government entity in the state authorized to use a facial recognition system.

b) The department may not use a facial recognition system for any purpose other than a purpose authorized in this section.

c) All requests for a facial recognition comparison shall be made to, and completed by, individuals employed by the department who:

    i) are trained to make a facial recognition comparison and identification; and

    ii) have completed implicit bias training.

d) Except as provided in Subsection (3), the department may not comply with a request for a facial recognition comparison unless:

    i) the request is made by a law enforcement agency;

    ii) the request is:

       A) submitted electronically through an encrypted state system;

       B) accompanied by a case identification number; and

Model language provided by Libertas Institute.

C) supported by a statement of the specific crime and factual narrative to support that there is a fair probability that the individual who is the subject of the request is connected to the crime;

    iii) the request is made for the purpose of:

        A) investigating a felony, violent crime, or threat to life; or

        B) identifying a deceased or incapacitated individual or an individual otherwise unable to identify the individual; and

    iv) the law enforcement agency agrees to use the comparison:

        A) in accordance with the requirements of law; and

        B) only in relation to a purpose described in Subsection (2)(d)(ii).

3. The department may compare an image taken of an applicant for a license certificate or an identification card, to determine whether the applicant has submitted a fraudulent or inaccurate application

4. The department may not use a facial recognition system for a civil immigration violation.

5. To make a facial recognition comparison, an employee described in Subsection (2)(c) shall:

    a. run the comparison using a facial recognition system that, in accordance with industry standards:

        i. makes the comparison using an algorithm that compares only facial biometric data;

        ii. is secure; and

        iii. is produced by a company that is currently in business;

    b. if the facial recognition system indicates a possible match, make an independent visual comparison to determine whether there is a likely match;

    c. if the employee determines that there is a likely match, seek a second opinion from another trained employee or the employee's supervisor; and

    d. if the other trained employee or the employee's supervisor agrees that there is a likely match:

        i. report the results to the requesting law enforcement agency via an encrypted method; and

        ii. return to the requesting law enforcement agency only a single result that is the likely match.

6. A law enforcement agency of the state or of a political subdivision shall, when submitting a case to a prosecutor, disclose to the prosecutor, in writing:

    a. whether a facial recognition comparison was made in investigating the case; and

      b.   a description of how the facial recognition comparison was used in the investigation.

Section 3. Data Protection and Disclosure.

1) Notwithstanding (INSERT STATE CODE TO OPEN RECORDS LAWS), data relating to a facial recognition comparison may not be used or shared for any purpose other than a purpose described in Section 2.
2) (a) The department shall, upon request, release statistical information regarding facial recognition comparisons, including:
    - i) the number of each crime type for which a request is received; and
    - ii) the number of likely matches provided in response to requests received for each crime type.
    - b) A release of statistical information under Subsection (2)(a) may not disclose details regarding a pending investigation.
3) On or after August 1 but before November 15 of each year, the department shall provide to the (INSERT RELEVANT LEGISLATIVE COMMITTEE) a report that:
    - a) discloses;
        - i) the number of each crime type for which a request is received; and
        - ii) the number of likely matches provided in response to requests received for each crime type; and
    - b) may not contain any identifying information relating to requests described in Subsection (3)(a).

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

Model language provided by Libertas Institute.