Facial Recognition and Biometrics
By Samantha Moodie

With citizens facing the ever-growing threat of identity theft and fraud, and with advances in camera and monitoring technology, the science fiction image of using iris and facial scans to enhance security is becoming a reality. Biometric screening technology allows users to identify and track human characteristics. Its uses are growing beyond such traditional methods as fingerprinting to include facial recognition, voice recognition, iris scans, and even DNA or other unique measurable personal characteristics.

Biometric technology can be useful in the public sphere to monitor border security, identify criminals, combat terrorism and eliminate identity fraud, among other things. In the private sector, biometrics can help verify employee information and hours worked, make advertising more effective, help social media users identify and tag other users, and enhance security by controlling access to sensitive locations. Employers cite biometric time-clocking as an almost fool-proof way to keep accurate employee time records. Biometric technology generally makes these tasks easier and more efficient and accurate.

Although biometrics have been touted as a way to improve security and limit fraud, privacy advocates have raised serious concerns about this technology. They include the “big brother” effect of constant and surreptitious surveillance of individuals by the government and private entities.

In addition, if a person’s biometric data were to be compromised, it would always be compromised. Unlike other types of theft, such as that of a credit card number, people cannot obtain new facial bone structure or DNA. Other concerns revolve around privacy issues. They include employers being able to discover protected health information; ambiguous standards about when biometric information can be shared, including with law enforcement; and multimodal big data storage, in which multiple images and various types of biometrics are stored in a database for widespread use.

Protective actions to mitigate these concerns include restricting biometric data collection to a single biometric in one database; using biometric data collection only when there is a compelling need; and, if biometrics are used, including authentication factors such as a card and/or pin in addition to biometric scans.
State Action

Actions in some states reflect the uncertainty and concern about the potential adverse effects of biometric tracking. Illinois and Texas laws prohibit commercial entities from capturing an individual’s biometric identifier without his or her consent. Both states also require businesses to protect biometrics using a reasonable standard of care that is the same as, or more protective than, that used for other confidential or sensitive information. They also prohibit selling or disclosing a biometric without consent, with certain exceptions, such as for law enforcement purposes.

In addition, at least 19 states restrict using, disclosing or sharing biometric data by either public or private entities, or require security measures, such as encrypting or properly destroying records with biometrics. At least 20 states have enacted legislation to protect the personal biometric information of students or minors.

Other states have laws authorizing the use of biometrics for criminal justice purposes, such as for criminal background checks; to monitor probation or prevent identity theft; or provide that biometric information in a criminal history file can be shared with the FBI.

States also are using facial recognition technology to identify cases of driver’s license fraud by comparing driver’s license photos with other department of motor vehicle images on file. According to a U.S. Government Accountability Office report, 41 states and the District of Columbia were using facial recognition and other biometric techniques to prevent these abuses by driver’s license applicants. Maine, Missouri and New Hampshire, however, prohibit collecting and using biometrics to produce a driver’s license or identification card.

Federal Action

The National Telecommunications and Information Administration recently convened discussions with stakeholders regarding commercial use of facial recognition, with the goal of developing a voluntary privacy-protective policy standard for companies that use facial recognition. In addition, the Department of Homeland Security has developed and is testing systems to match faces in a crowd to names on a watch list, or to spot people using travel documents that don’t belong to them.

NCSL Contacts and Resource

Pam Greenberg
NCSL—Denver
(303) 856-1413

Jon Adame
NCSL—Washington, D.C.
(202) 624-8686


Additional Resource