Information Management

UNDERSTANDING BIOMETRICS' IG OBLIGATIONS

Judy Vasek Sitton, CRM, FAI

Biometric identifiers are measurable characteristics – either physiological or behavioral – used to label and describe individuals for identification purposes. For information governance (IG) purposes, the identifiers impact access control to physical or electronic records systems and provide authentication for records throughout their life cycle. Because the identifiers are unique to individuals, they are purported to be more reliable in verifying identity than security tokens or knowledge-based methods.

The use of biometrics impacts IG professionals because of its role in authentication and access control, its inherent sensitive nature as an identifier, the mandates for its maximum retention periods, and any privacy protection obligations, such as breach notification policies and any restrictions on the use and release of biometric data.

Because biometric identifiers can be especially sensitive examples of personally identifiable data, information management professionals must be aware of their proper use and their jurisdictional requirements. This article describes many types of biometrics in use today, and it summarizes the emerging legal landscape, with an eye on proper retention, protection, and destruction of biometric information.

Biometrics for Personal Identification

The types of biometrics being used and collected for personal identification are varied and now include single and multimodal biometrics.

Single Modal Biometrics

Chemical biometrics, such as DNA profile matching, DNA fingerprinting, and olfactory or body odor recognition, is used in forensics, paternity tests, and ancestry matching. Generally speaking, these identifiers are protected under genetic protection and other laws rather than biometric laws.

Vascular biometrics recognizes the vein patterns of an individual's palm, finger, or back of the hand, as well as retina veins and finger veins. In the medical environment, some patient identification systems link the biometric palm vein pattern to the patient's medical record at registration or within electronic medical record systems. The technique is designed to forestall the creation of duplicate medical records and prevent medical identity theft and fraud. Vein recognition is also used in professional exam centers to validate identities.

Visual biometrics is used for such things as determining television viewership ratings; authenticating the identities of those who take tests, conduct banking, and play games online; detecting sleep-deprived drivers; and tracking employees' time. Examples of visual biometrics are ear pattern or shape identification, eye or iris pattern recognition, face recognition, fingerprint recognition, and lip-print wrinkles or grooves. Tools that collect these biometrics are said to operate effectively in complete darkness or brightly lit rooms.

Behavioral biometrics includes gait biometrics, which recognizes a person's walking style, which is useful for surveillance, monitoring, and unobtrusive identification at a distance. Gait biometrics can be based on body shape and body movement. Additionally, within the realm of behavioral biometrics is typing and keystroking recognition, conducted to establish identification. This technique is useful for access control at sites of high risk and is usually paired with other means of biometric identification to get stronger security.

Auditory biometrics is especially useful for interfacing with technology, ensuring call center fraud protection, and activating artificial intelligence assistance. It uses such factors as voice pitch, speaking style, tone, cadence, and frequency for purposes of identification. Speaker voice verification or authentication occurs when verifying a speaker's voice against a template or a voice print. Speaker voice identification is the term for determining an unknown speaker's identity by comparing it against multiple templates. Note that there is a difference between *speaker or voice recognition* and *speech recognition*: the former recognizes *who* is speaking, and the latter recognizes *what* is being said.

Multimodal Biometrics

Multimodal biometrics refers to a fusion of biometrics. These tend to be visual and spatial biometrics, such as finger, hand, and footprint geometry recognition.

Visual/behavioral biometrics such as signature recognition, in which what the signature *looks like* is combined with *how it was signed* (e.g, pressure, speed) is used in e-business applications and other applications in which a signature is used for personal authentication.

Biometric Protection Laws

As of March 2018, two types of laws affect the use of biometric information: laws specifically addressing the use of biometric identifiers and broad privacy laws that include biometric information in their definition of personal information.

Currently, these three U.S. laws specifically address the use of biometric identifiers:

- Illinois 740 ILCS 14 Biometric Information Privacy Act (BIPA), enacted in 2008

- Texas Business and Commerce Code – BUS & COM § 503.001, Capture or Use of Biometric Identifier, enacted in 2009
- Washington State H.B. 1493 – an act relating to biometric identifiers, and adding a chapter to Title 19 RCW, enacted in 2017

The following instances contain biometric information within their definitions of personal data:

- Maryland Personal Protection Act House Bill 947 – expanded definition of personal information to include biometric data, enacted in 2018
- Security breach notification laws within other U.S. state laws
- Biometric implications in U.S. federal data breach and data protection laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA)
- Biometric implications in the European Union's General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronics Document Act (PIPEDA), The Australian Privacy Act (amended in 2014), and Japan's Act on the Protection of Personal Information (APPI), which was amended in 2017
- Emerging data protection laws under consideration in other countries, such as Chile and Peru

Because Illinois's BIPA was the first biometric-specific law in the United States, the other state laws tend to follow its requirements, which are as follows:

- Requires informed consent prior to collection – in effect, stating why the biometric is being collected and what will be done with it
- Prohibits profiting from biometric data – meaning the biometric information can't be sold
- Allows only limited right to disclose the biometric information – usually limited to what is mentioned in the informed consent
- Mandates protection obligations and retention guidelines (more details below)
- Creates a private right of action (possible lawsuit) for individuals harmed by violators of BIPA – if the other criteria in this list aren't followed

Texas and Washington do not offer a right of action by individuals. Also, Washington-based companies are not required to have opt-in consent in all cases for the collection, use, and disclosure of biometric data. Options for obtaining consent can vary.

Managing Biometric Data

Traditionally, records retention periods are discussed as the minimum time a record has to be kept, but the biometric laws and other privacy legislation set retention at the maximum time the biometric record may be retained, depending on the purpose for which it was collected. Retention requirements can vary from law to law and even within the same law.

Read More About It

Grother, Patrick; Wayne Salamon; and Ramaswamy Chandramouli. "Biometric Data Specification for Personal Identity Verification." NIST Special Publication 800-76. National Institute of Standards and Technology, July 2013. Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf*

National Conference of State Legislatures. "2017 Security Breach Legislation." National Conference of State Legislatures, Dec. 29, 2017. Available at *http://www.ncsl.org/research/telecommunications-and-information-technology/2017-security-breach-legislation.aspx*

National Conference of State Legislatures. "Data Disposal Laws." National Conference of State Legislatures, Dec. 1, 2016. Available at *http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx*

Waldmann Agarwal, Marian A. and Adam J. Fleisher. "Biometric Information as Personal Information – A Brave New World of Compliance." Morrison Foerster, April 4, 2017. Available at *https://www.mofo.com/resources/publications/170404-biometric-information-personal.html*

For example, according to Illinois' BIPA, a business may not store biometric data for longer than the earlier of three years from the individual's last interaction with the company or when the initial purpose for collecting the data has been fulfilled. The Texas law, to cite a second example, specifies three retention times that depend on the purpose of the biometric use:

1. …"shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).
2. (c-1) If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period prescribed by Subsection (c)(3), the person who possesses the biometric identifier shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law.
3. (c-2) If a biometric identifier captured for a commercial purpose has been collected for security purposes by an employer, the purpose for

collecting the identifier under Subsection (c)(3) is presumed to expire on termination of the employment relationship."

Washington State H.B. 1493 also contains data security and retention requirements. In particular, the statute requires (1) reasonable care to guard against unauthorized access to and acquisition of biometric identifiers and (2) retention of biometric identifiers for no longer than necessary to comply with the law, protect against fraud, criminal activity, security threats or liability, or to provide the service for which the biometric identifier was enrolled.

Biometrics information is considered to be personally identifiable information (PII). As reported on March 29 on the website of the National Conference of State Legislatures, all 50 U.S. states, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have legislation requiring private or governmental entities to notify individuals of security breaches involving PII.

Records destruction requirements for biometrics are generally equal to the destruction requirements for other sensitive, confidential, or personally identifiable data.

Emerging Lawsuits

Of the U.S. biometric laws, BIPA is the oldest and has a private right of action that the other laws do not yet have. As a result, lawsuits mentioned in this article have been filed in Illinois. The roughly 35 class action lawsuits filed in reference to BIPA since September 2017 and the 60-plus claims filed since its enactment have caused some in the legal industry to refer to BIPA as a "cash cow."

Lawsuits began to emerge around 2015 alleging that social media sites had conducted improper collection of facial biometrics from photos without notice or consent. Current suits are filed on behalf of employees and customers of a wide variety of industries such as healthcare, manufacturing, retail, hospitality, entertainment, and personal services. To date, the claims have been filed as negligence claims for failure to comply with consent, disclosure, retention, or protection obligations when utilizing biometrics for security protocols, to track employee time worked, to verify purchases at self-service kiosks, to grant admission to a venue, to verify membership privileges, or for similar purposes.

Recognizing Biometrics' Impact on IM

Information management (IM) professionals must understand the emerging role of biometrics and be aware of their use under any jurisdiction. The use of biometrics in the workplace is becoming more common; in some applications, such as work-time management, the technique is used every day. Sanctions can be hefty for negligence or non-compliance, but even without that incentive, biometrics obligations are serious business. Passwords can be reset and access cards can be replaced, but it is nearly impossible to change a biometric attribute. Biometrics laws mandate how data will be collected, stored, retained, used, and destroyed for a reason: these identifiers are extremely personal and if compromised can cause irreversible damage to the owner. E

About the Author: Judy Vasek Sitton, CRM, FAI, is senior information governance analyst for Kinder Morgan, Inc. in Houston, Texas, and co-author of the 2014 ARMA-published book *Managing Active Business Records.* Having been a practitioner and consultant in records and information governance for 40 years, she is a recognized leader in the profession. She is a Certified Records Manager and Fellow of ARMA International. Sitton can be contacted at *Judy_Sitton@kindermorgan.com.*