Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy

by

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

Many organizations are considering the deployment of biometric technologies to meet the growing need for securely identifying and authenticating individuals in allowing access to their information systems, structural premises or business services. Biometric technologies present many benefits, such as stronger user authentication, greater user convenience and improved security and operational efficiencies. However, biometric technologies also present certain risks that organizations should carefully take into account, including risks associated with inadequate privacy protection that may cause loss of public support for the initiative. **To ensure that organizations comply with privacy laws, they should first examine whether alternative non-biometric means to authenticate users would meet the same objective(s).**

Regardless of the following claims: (i) the stored biometric information is just a meaningless number and therefore not personally identifiable information (PII); (ii) the biometric templates stored in a database cannot be linked to other databases; or (iii) a biometric image cannot be reconstructed from the stored biometric template; organizations must realize that any biometric information, be it images or templates, is considered to be PII. Therefore it is protected under privacy legislation such as the *Freedom of Information and Protection of Privacy Act, the Municipal Freedom of Information and Protection of Privacy Act*, **and the** *Personal Health Information Protection Act* **in Ontario, and the federal** *Personal Information Protection and Electronic Documents Act*.

It is important to note that privacy, and specifically *informational privacy*, subsumes a set of protections far greater than security. While security is a critical component of any identification/authentication system, it is only one of the means used to achieve informational privacy. Informational privacy refers to an individual's personal control over the collection, use and disclosure of their personal information. In addition, it also refers to an organization's responsibility for data protection and the safeguarding of PII in its custody or control. Informational privacy is at the heart of user confidence, trust and acceptance of new technologies. Consequently, safeguarding informational privacy should be a key concern for any organization that wishes to successfully deploy a biometric system.

Below is a list of sample questions that will assist organizations in conducting their due diligence **prior to implementing a biometric system, and in meeting their clients' and customers' expectations of privacy. Although the questions focus mostly on fingerprints – the most common biometric in use today – they may also be adapted to other types of biometric systems.**

System Design, Components and Parameters

- Please describe the system architecture in detail. In particular, is enrollment and authentication done locally or on a server?
- Which hardware and software products from the vendor are used? Can you provide specifications for those products, besides those publicly available on the vendor's website?
- In the case of a one-to-many identification system, how many templates is the system capable of matching (e.g., 1:3000, 1:20000)? The answer to this question is critical.
- What is the actual number for the False Acceptance Rate (FAR) that is configured for the system? Does this number refer to a one-to-many or a one-to-one system? Is it applicable to one or two-finger scanning?
- Does the system create a record of attendance and/or transactions? How are those data used?

Enrollment Process

- How many fingers are needed per user, and which ones (e.g., right index + left index) are enrolled?
- How many fingers and which ones are normally needed for authentication (i.e. one of the enrolled fingers or both)?
- Is submission of fingerprints voluntary for a user? What are the other options available to the user?
- Some users do not have fingerprints of acceptable quality, i.e. there is a failure to enroll. How are these cases handled?
- During enrollment, if an employee sees the fingerprint image on the monitor, can that employee capture the image using the *Print Screen* button?

Authentication Process

- Is authentication done under supervision or in the presence of a security guard?
- How is a false rejection handled, especially for users having difficulties with the system?
- Is there a scenario where a false acceptance would have an impact on the user? Take the following example: suppose that in a one-to-many system, an enrollee is misidentified as another enrollee. Then, in a situation where there is an account for transactions, the wrong enrollee's account would be negatively affected. With a biometric, it may be more difficult to repudiate the validity of the incorrect transaction.
- Does the user see the fingerprint image during authentication (e.g., are there monitors on site to display the image)?
- After the fingerprint authentication, does the system use any other means (e.g., a person's photo), to further confirm their identity?

Fingerprint Templates

- Are the fingerprint templates compatible, or can they be made compatible, with one of the following standards: ANSI-INCITS 378, ISO/IEC 19794-2, FIPS 201, ILO SID-0002?
- Does the template contain fingerprint minutiae x, y positions and directions?
- Does the template contain the following data: minutiae type, quality; fingerprint core and delta positions; ridge count; orientation field?
- Is the template size fixed or variable? What would be an approximate size of the template containing e.g., 30 fingerprint minutiae?

Storage and Security

- Where are the templates stored (i.e., locally or on a server)?
- Are the fingerprint images stored on a server or somewhere else in the system? Is this option (i.e., to store the images or not) configurable? Who does the configuration?
- Are the stored templates encrypted?
- How are the stored data protected (e.g., from an insider's attack or if the server is stolen)?
- Who has access to the stored templates? How is access controlled?
- Does the biometric vendor regularly access the stored templates? How are the upgrades and maintenance of the biometric system performed?
- How and where is the template storage backed up?
- Is wireless connection used anywhere in the system? If Yes, is it encrypted? (This is a must.)
- Are the biometric servers connected to the Internet or an Intranet?
- What are the safeguards, if any, against spoofing (i.e., applying a fake fingerprint)?
- If there is a request from a law enforcement agency, can the biometric template be extracted from the system? What is the procedure? Who will perform the extraction?

Data Retention Policy

- How long is the biometric information retained in the system?
- Can the user request the deletion of his/her biometric information?

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario