DIACC CCIAN

Guidance on the Acceptable Use of Biometrics

DIACC Special Interest Group Insights

Contents of this paper have been submitted by the DIACC Biometrics Special Interest Group. For further information about the topics discussed in this paper, or to join the DIACC community, visit www.diacc.ca or contact info@diacc.ca.

Table of Contents

About the DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the Digital ID & Authentication Council of Canada **(**DIACC**)** is a non-profit coalition of public and private sector leaders who are committed to developing a Canadian digital identification and authentication framework that will secure Canada's full and secure participation in the global digital economy.

About the DIACC Special Interest Groups

A DIACC Special Interest Group (SIG) provides a mechanism in which to engage our community in discussion around a specific interest. They enable more opportunities to connect subject matter experts from around the world and to broaden the conversations outside of our DIACC membership.

A DIACC SIG does not create intellectual property but rather contemplates a specified question to make a recommendation to DIACC regarding the next steps that should be considered for incorporation into the DIACC strategy and roadmap.

Background

In the fall of 2020, A DIACC Special Interest Group (SIG) was created to address the following question, "Do we need a made-for-Canada biometrics standard or Pan-Canadian Trust Framework (PCTF) component or does an existing national, international, or industry standard meet our needs?".

With input from public and private sector DIACC members and liaisons, the following guidance was created as a recommendation that the DIACC's Trust Framework Expert Committee (TFEC) agreed to consider. Specified business, legal, and technical process requirements will be identified and considered by the TFEC for inclusion in future versions of the PCTF.

Biometrics technologies are tools that can be used for person verification, authentication, identification, and location. The tools are used by government, industry, and consumers for a variety of purposes. However, their use is not without controversy such as its use for surveying and control of citizens to its unauthorized collection and use for profit. Furthermore, biometrics can be, and in many cases is, invisible to the average person.

Identity is fundamental to how people conduct their affairs both physically and increasingly digitally. Biometrics is advantageous for identity verification and authentication. However, its use is not regulated and there is a lack of guidance on how, when, and who can use biometrics, for what purpose and how to protect the privacy and security of biometric information.

Biometric Terminology

- **Foundational Evidence of Identity:** Evidence of Identity that establishes the existence, uniqueness, and Digital Representation of real, legally recognized Identities, based on fact-based foundational events (e.g., birth, immigration, incorporation). The establishment and maintenance of foundational identity evidence is the exclusive domain of the public sector.
- **Contextual or Functional Identity:** Evidence of Identity that establishes the existence and Digital Representations of Entities within a specific context and for a specific purpose once Foundational Evidence of Identity is proven and accepted.
- **Identity Proofing:** A process of establishing with a level of confidence in the Foundational or Functional (Conceptual) Identity of an applicant by validation and verification during enrollment into an Identity Management System (IdMS).
    - **Validation:** A process to authenticate and legitimize Personal Identifiers and Identity Attributes, like identity-related documents and biometric identifiers, presented by the applicant during enrollment into an Identity Management System.
    - **Verification:** A process to establish a provable high confidence in a claimed connection between an applicant and validated Personal Identifiers and Identity Attributes.
- **Authentication:** An access control process of using a biometric to confirm the legitimate connection between a proven and entitled privilege holder Identity and an individual claimant attempting to access the privilege.
- **Identification:** A process of identifying a provable connection between unknown and unverified biometric data and known and verified biometric data to establish the identity of an unknown individual.
- **Detection/Deduplication:** A biometric Identification process to establish and maintain Identity Profile database integrity by identifying potential connections between enrolment applicants and previously verified and enrolled Profiles within the database.

Use of Biometrics

- Biometrics **SHOULD** only be used where its use is demonstrably necessary and is the best mechanism to meet a specific need and the use of biometrics and the loss of privacy is proportionate to basic human rights, privacy laws, and justifiable to the benefits gained.
- The biometric technology **MUST** require suitable accuracy, minimize data collection, limit the collection of personal information, and limit the retention of biometric information to a period only necessary to fulfill the stated purpose.
- The evaluation of proportionality **SHOULD** include evaluating the scope of the proposed biometric program using criteria such as sensitivity, necessity, proportionality, effectiveness, and minimal intrusiveness.

Disclosure of Biometric Collection of Use

- Any collection, management, or use of biometric data **MUST** specify the purpose for its use and what is achieved in using biometric information, what biometric information is being collected, what the biometric information is being compared to (what database(s) if any), what will happen to their biometric information, and where their biometrics information is stored so it's easily understood by an average person within a Statement of Biometric Collection and Use.
- Such statement **SHOULD** include recognition of legal obligations for its collection, use, and disclosure in accordance with Canada's federal or provincial privacy laws and in some cases cite laws outside of Canada's jurisdiction.
- Such Statements **MUST** be disclosed both uniquely and within any broader Notice of Privacy Policy.
- All relevant individuals **SHOULD** be specifically directed to such Disclosures.

Biometric Privacy and Security Risk Disclosure

- Organizations that use biometrics are responsible for protecting the biometric and personal information they process and collect and **MUST** implement security safeguards appropriate to the sensitivity of the information and degree to which it may be at risk.
- If biometrics are used or collected the data **MUST** be given strong protections because of the risk of harm that can result from a breach of an individual's private information and biometrics.
- Organizations and institutions using biometrics to protect personal information **MUST** use effective protection against spoofing and falsification; attack methods and conduct testing and vulnerability assessments.
- The risk and responsibility relating to the collection, management, or use of biometric data **SHOULD** be specifically described and easily understood by an ordinary consumer, within a Biometric Privacy Risk Disclosure.
- Such Statements **SHOULD** be disclosed both uniquely and within any broader Notice of Privacy Policy.
- All relevant individuals **SHOULD** be specifically directed to such Disclosures.

Voluntary Consent to Biometric Data Collection and Use

- All individuals **SHOULD** be required to acknowledge a full understanding of the Statement of Biometric Collection and Use, as well as the Biometric Privacy Risk Disclosure.
- All individuals **SHOULD** be required to either accept or decline consent to its use, therein, before any biometric data collection occurs.

- Any extension of the use of biometrics **MUST** not be attempted without first obtaining the individual's consent for the new use unless a valid legal exception to consent applies. Individuals have the right to withdraw the consent they previously provided, subject to legal or contractual restrictions.
- Individuals **SHOULD** be provided with an easy and accessible method to withdraw consent then delete all the biometric information collected about them, including any personal information created using analysis, unless otherwise required by law.

Compliance and Audit Use

- All management and use of any biometric data **SHOULD** ensure there is clear legal authority for the collection and use of biometrics and comply exactly, and only with, the Statement of Biometric Collection and Use.
- Such data **SHOULD NOT** be managed or used in any way not specifically described and consented to.
- All such use **SHOULD** be recorded and audited, periodically, and made quickly and easily available for review upon request.
- Any violation of such compliance **SHOULD** be immediately reported to the affected individual and other stakeholders, including related government, regulatory bodies, and law enforcement.