An insight into biometrics good practices

2021 ICAO TRIP VIRTUAL SYMPOSIUM

25 May 2021

Isabelle Moeller

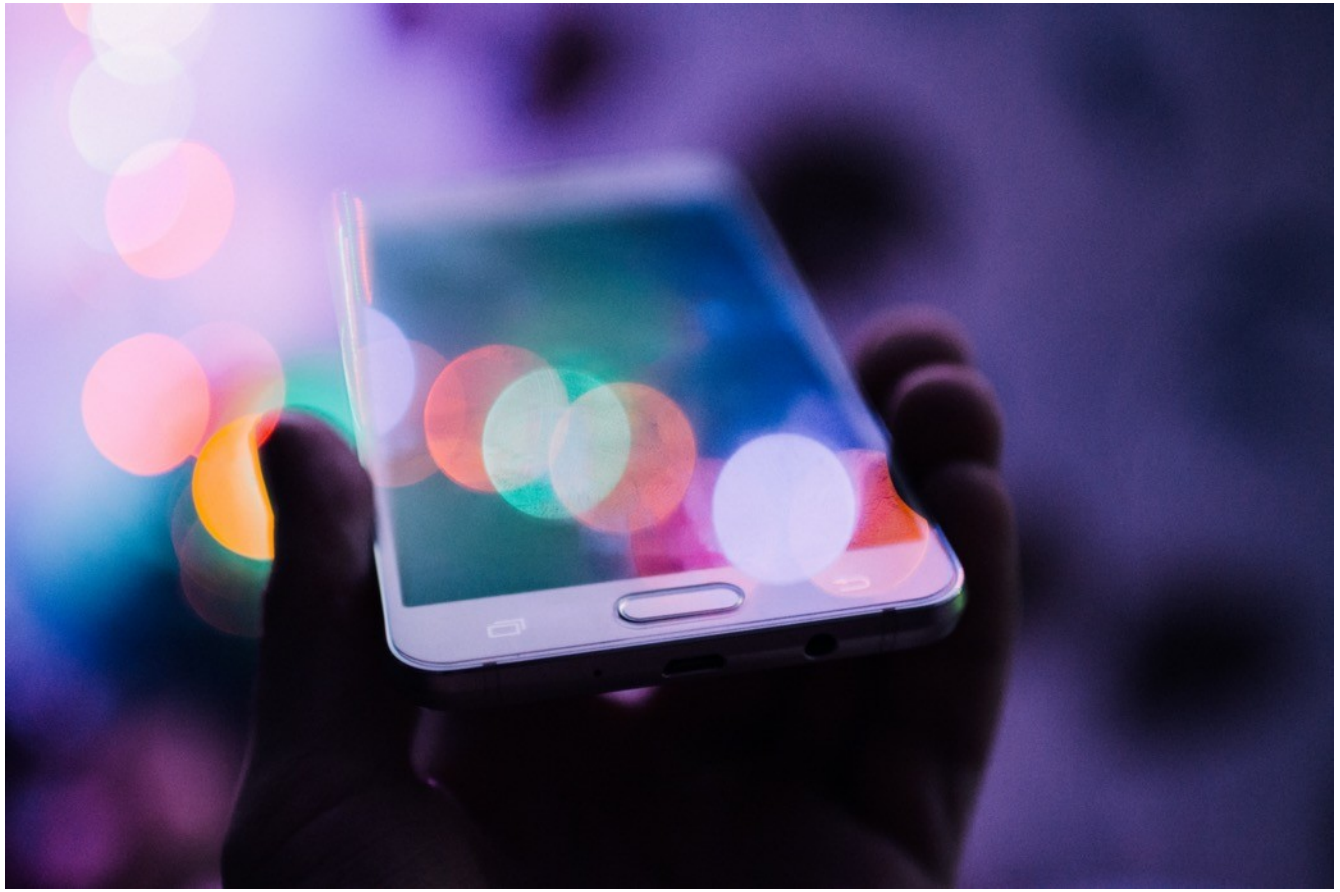
Chief Executive,

Biometrics Institute

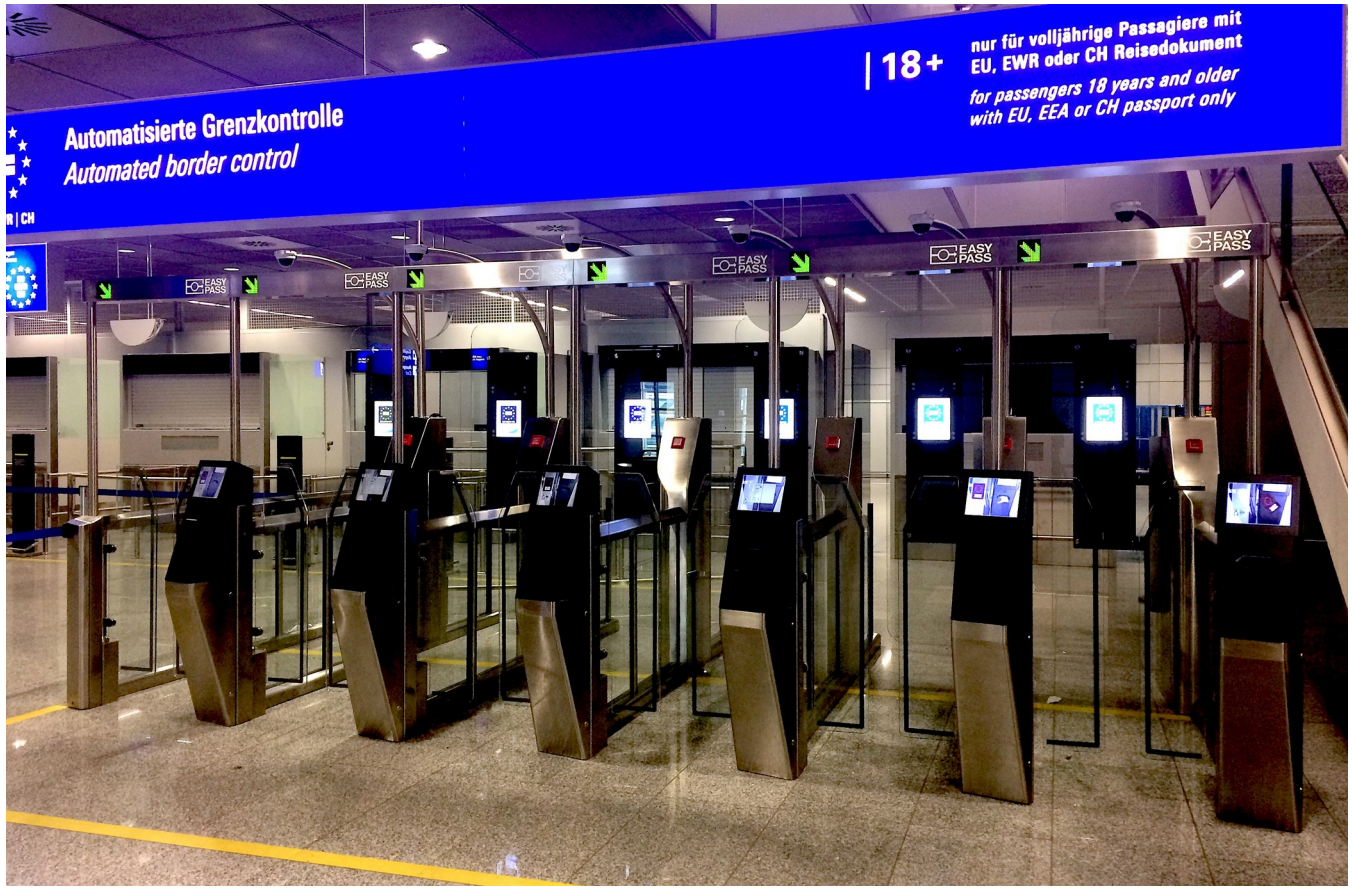
Policy and standards development takes time

Contactless is imperative

Surge in remote onboarding



Biometric gates provide efficiency and security



Identity and health credentials

Know your implementation - recent releases

Should we ban facial recognition viewpoint paper

Digital onboarding and biometrics guiding paper

State of Biometrics Report podcast

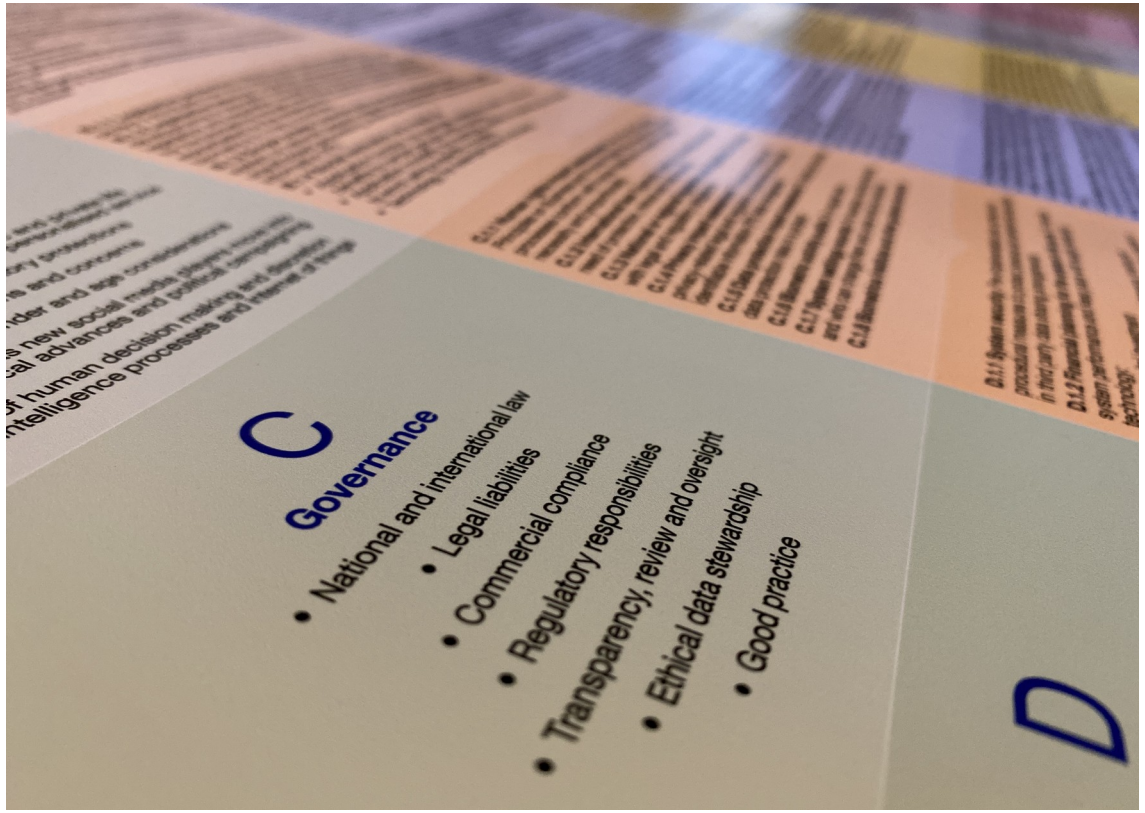
The Three Laws of Biometrics

1. **POLICY** – comes first: Any use of biometrics is proportionate, with basic human rights, ethics and privacy at its heart.

2. **PROCESS** – follows policy: Safeguards are in place to ensure decisions are rigorously reviewed, operations are fair and operators are accountable.

3. **TECHNOLOGY** – guided by policy and process: Know your algorithm, biometric system, data quality and operating environment and mitigate vulnerabilities, limitations and risks.

Biometrics Institute Good Practice Framework

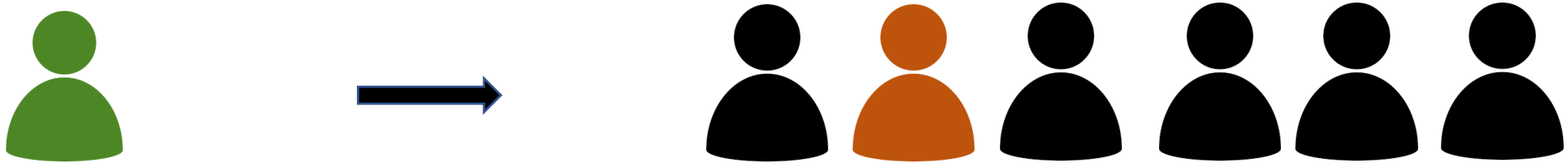


A first-of-its-kind tool which provides a structured pathway through the factors that may influence or constrain a biometric application

Privacy Guidelines update

- The revised *Privacy Guidelines* released at the beginning of May
- Two new principles have been added

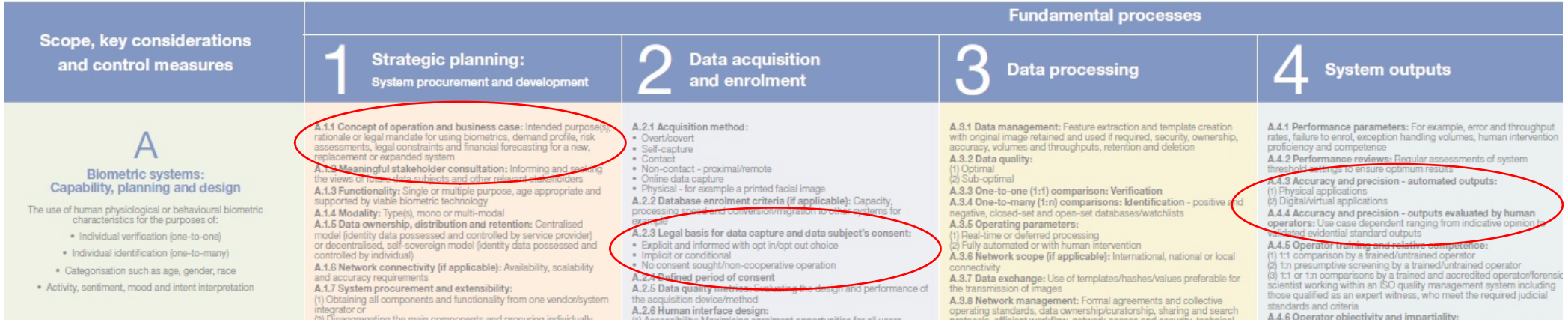
What does this mean in practice?



Scenario:

1 : 1 automated face verification e-gates -> adding watch list capability to search the faces 1:n

What does this mean in practice?



Scope, key considerations and control measures	Fundamental processes			
	1 Strategic planning: System procurement and development	2 Data acquisition and enrolment	3 Data processing	4 System outputs
A **Biometric systems: Capability, planning and design** The use of human physiological or behavioural biometric characteristics for the purposes of: • Individual verification (one-to-one) • Individual identification (one-to-many) • Categorisation such as age, gender, race • Activity, sentiment, mood and intent interpretation	**A.1.1 Concept of operation and business case:** Intended purpose(s), rationale or legal mandate for using biometrics, demand profile, risk assessments, legal constraints and financial forecasting for a new, replacement or expanded system **A.1.2 Meaningful stakeholder consultation:** Informing and seeking the views of future data subjects and other relevant stakeholders **A.1.3 Functionality:** Single or multiple purpose, age appropriate and supported by viable biometric technology **A.1.4 Modality:** Type(s), mono or multi-modal **A.1.5 Data ownership, distribution and retention:** Centralised model (identity data possessed and controlled by service provider) or decentralised, self-sovereign model (identity data possessed and controlled by individual) **A.1.6 Network connectivity (if applicable):** Availability, scalability and accuracy requirements **A.1.7 System procurement and extensibility:** (1) Obtaining all components and functionality from one vendor/system integrator or	**A.2.1 Acquisition method:** • Overt/covert • Self-capture • Contact • Non-contact - proximal/remote • Online data capture • Physical - for example a printed facial image **A.2.2 Database enrolment criteria (if applicable):** Capacity, processing speed and conversion/migration to other systems for example **A.2.3 Legal basis for data capture and data subject's consent:** • Explicit and informed with opt in/opt out choice • Implicit or conditional • No consent sought/non-cooperative operation **A.2.4 Defined period of consent** **A.2.5 Data quality metrics:** Evaluating the design and performance of the acquisition device/method **A.2.6 Human interface design:**	**A.3.1 Data management:** Feature extraction and template creation with original image retained and used if required, security, ownership, accuracy, volumes and throughputs, retention and deletion **A.3.2 Data quality:** (1) Optimal (2) Sub-optimal **A.3.3 One-to-one (1:1) comparison: Verification** **A.3.4 One-to-many (1:n) comparisons: Identification** - positive and negative, closed-set and open-set databases/watchlists **A.3.5 Operating parameters:** (1) Real-time or deferred processing (2) Fully automated or with human intervention **A.3.6 Network scope (if applicable):** International, national or local connectivity **A.3.7 Data exchange:** Use of templates/hashes/values preferable for the transmission of images **A.3.8 Network management:** Formal agreements and collective operating standards, data ownership/curatorship, sharing and search	**A.4.1 Performance parameters:** For example, error and throughput rates, failure to enrol, exception handling volumes, human intervention proficiency and competence **A.4.2 Performance reviews:** Regular assessments of system threshold settings to ensure optimum results **A.4.3 Accuracy and precision - automated outputs:** (1) Physical applications (2) Digital/virtual applications **A.4.4 Accuracy and precision - outputs evaluated by human operators:** Use case dependent ranging from indicative opinion to validated evidential standard outputs **A.4.5 Operator training and relative competence:** (1) 1:1 comparison by a trained/untrained operator (2) 1:n presumptive screening by a trained/untrained operator (3) 1:1 or 1:n comparisons by a trained and accredited operator/forensic scientist working within an ISO quality management system including those qualified as an expert witness, who meet the required judicial standards and criteria **A.4.6 Operator objectivity and impartiality:**

Good Practice Framework

A.1.1 Concept of operations and business case & **A.2.3** legal basis for data capture & **A.1.2.** Meaningful stakeholder consultation

A.1.4 Modality & **A.4.3** accuracy **& B.4.2** system bias

What does this mean in practice?

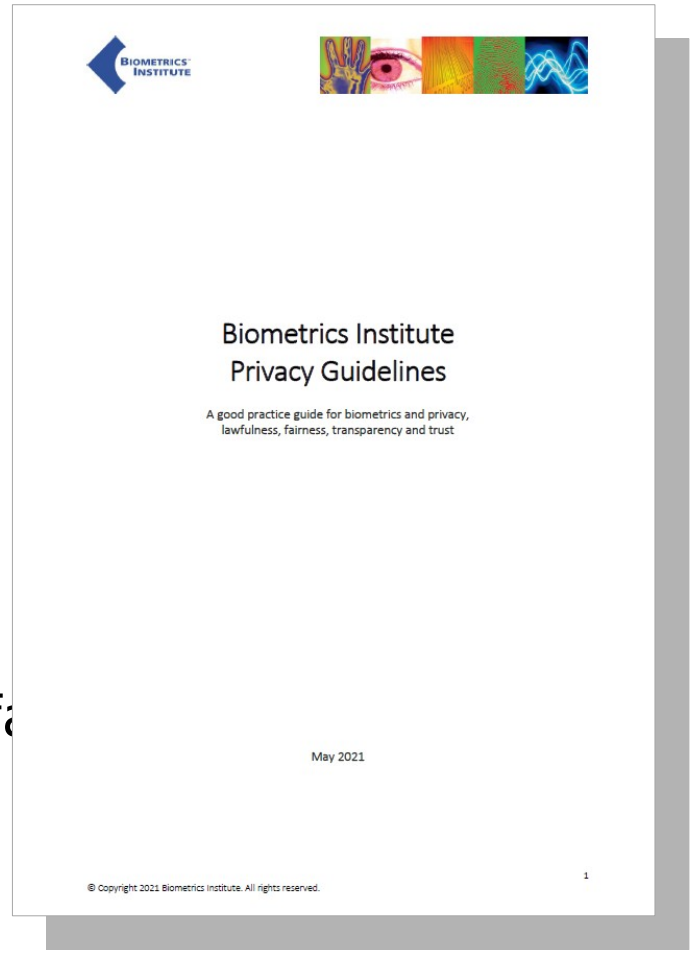
Privacy Guidelines

Mistakes occur - expert human intervention needed

Principle 8: Non-discrimination

Principle 6: Fair handling of complaints and enquiries

Principle 6: Truth and accuracy in business and legal affa



Engage with us

isabelle@biometricsinstitute.org |

www.biometricsinstitute.org

Connect with us on social media:

#IDBorders
#BIDebates

Upcoming events

- **2 June 2021:** Member Meeting – Updates from Australia and New Zealand, online
- **29 June 2021:** Member Meeting – Updates from the US, online
- **6, 13, 20 & 26 October 2021**: Biometrics Institute Congress, London, online
- **17 November 2021:** Showcase Australia, Canberra
- **On demand:** Biometrics Vulnerabilities Workshop - How robust is your system?
- **On demand:** Global Good Practice Series: Biometrics and surveillance