Real-time Identification System using Mobile Hand-held Devices: Mobile Biometrics Evaluation Framework

Prepared by:
Raj Nanavati
International Biometric Group, 361 Queen Street S., Kitchener, ON

Scientific authority:
Pierre Meunier, 613-944-4367
DRDC Centre for Security Science

DRDC-RDDC-2014-C134
April 2014

IMPORTANT INFORMATIVE STATEMENTS

This project, *PSTP-03-427BIOM Real-time Identification Systems Using Mobile Hand-held Devices,* was supported by the Canadian Safety and Security Program (CSSP) which is led by Defence Research and Development Canada's Centre for Security Science, in partnership with Public Safety Canada. Partners in the project include International Biometric Group-Canada, 3M Cogent, DFAIT, OPC, IPC Ontario, DRDC-Toronto, DRDC-Ottawa, Transport Canada, Reboot Communications The CSSP is a federally-funded program to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence

Template in use: template-july2013-eng_V.03.01.dot

Note to readers: The publications cited in footnotes require a subscription to BIO1 https://bio1.com/

PSTP-03-0427BIOM

Real-time Identification System using Mobile Hand-held Devices: Mobile Biometrics Evaluation Framework

International·Biometric·Group
Research Consulting Integration

Table of contents

Figures

Tables

1 Introduction

To support an enduring mobile identification capability in Canada, the Study Team for PSTP-03-427BIOM evaluated the mobile biometric technology baseline, integrated a representative mobile device for operationally relevant field-testing, and developed a structured framework for analyzing national security applications of real-time, mobile biometric identification systems, encompassing technological, legal, ethical, privacy, and cultural issues.

The Study employed IBG's evaluation methodologies, based on its standards-compliant Comparative Biometric Testing and DHS accredited QPL processes. It also leveraged international standards and methodologies, including ISO/IEC 15408, FIPS 140-2, ISO/IEC 19795, and ISO/IEC 19792. OPC's existing frameworks for biometrics and national security and IBG's BioPrivacy Framework supported roadmap and framework development.

Field tests demonstrated the ability of the selected mobile device to establish connectivity with the RCMP NPS-NIST test server, transmit five test cases over both WIFI and 3G, and receive accurate results. The second Study output, the Mobile Biometrics Evaluation Framework, articulated a methodology for assessing usability and appropriateness across a variety of mobile identification and verification applications, providing specific guidance in the areas of architecture, interoperability, data format, privacy policy, solutions affordability, and legal, ethical, and cultural issues.

The Study will facilitate deployment of mobile biometric technologies and provide enduring mobile biometrics evaluation direction.

Three reports are published on this study:

REAL-TIME IDENTIFICATION SYSTEM USING MOBILE HAND-HELD DEVICES: FINAL REPORT

REAL-TIME IDENTIFICATION SYSTEM USING MOBILE HAND-HELD DEVICES: MOBILE BIOMETRICS EVALUATION FRAMEWORK

REAL-TIME IDENTIFICATION USING MOBILE HAND-HELD DEVICE: PROOF OF CONCEPT SYSTEM TEST REPORT

2 Framework for Evaluating and Deploying Mobile Biometrics

The following framework can be used to assess the use of biometrics across various mobile biometric applications (e.g., identity confirmation, watch list search) from evaluation to pilot to deployment.

2.1 Biometric Use Cases

The objectives of a mobile biometric deployment may include:

2.1.1 Watch Listing

Ensure that an individual is not present on a watch list comprised of national security threats.

In this scenario, the subject is not expected to be an enrolled member of the watch list. The user requires identity information for awareness about specific threats, while any subjects who are enrolled will wish to evade detection.

2.1.2 Identification (1:N)

Uniquely identify a subject of interest, providing situational awareness to the operator.

In this scenario, the subject may or may not be expected to be an enrolled member of a larger database. The user is seeking unique identification for general situational awareness. Information retrieved may or may not be derogatory in nature, and the subject may or may not seek to evade detection.

2.1.3 Eligibility and Access Verification

Verify a subject's Eligibility for provision of services or benefits.

In this scenario, the subject is an enrolled member of a program, and claims Eligibility for services or benefits. Genuine subjects seek to be correctly identified, while fraudulent subjects may seek fraudulent inclusion. System users require identity information only to the extent of authenticating membership or enrollment.

2.1.4 Identification Verification (1:1)

Verify a unique identity claim by a subject, for provision of personalized services or benefits.

In this scenario, the subject is an enrolled member of a program, and claims Eligibility for their specific services or benefits. Genuine subjects seek to be correctly identified, while fraudulent subjects may seek fraudulent inclusion. System users require verification that the subject has been correctly associated with an enrollment account, but may or may not require information as to the specific identity.

2.2 Biometric-Specific Usage Factors

2.2.1 Reference Data Collection and Storage

Due to sensor quality, operating environment, and data entry capabilities, mobile biometric devices are generally inappropriate for controlled enrollment operations. Reference data is generally obtained from enrollments collected under other programs, or from a distinct enrollment workflow within the same program.

An enrolled sample may be stored on an identity credential, such as a smartcard, provided by the subject. Biometric samples or templates stored on a credential or token typically require a PIN or other authentication mechanism for release.

A watch list or access list may be stored on the collection device or a coupled computer system. Mobile biometric data at rest increases the risk associated with compromised devices.

Enrolled samples may also be stored within a central repository, such as an AFIS matching system. Dissemination of watch lists for on-device storage generally necessitates an authoritative data source, and processes to track list modifications and access revocations.

2.2.2 Matching

Biometric data collected by a mobile device is matched against reference data to determine match or non-match. The location of the matching is a function of the location of the reference data.

In a match-on-card system, the probe sample is submitted from the device to the card. A low-power matching algorithm on the credential performs verification against the reference sample, returning a decision to the device.

Most local matching is performed on-device, using a list of reference samples or a single reference sample transmitted from an identity card to the device.

More accurate matching against larger databases can be performed by transmitting query images against back-end matching systems. The larger database and the more accurate algorithm increase the probability of matching against a previous enrollment, as well as the probability that the match is correct. However, remote matching introduces significant delays which may be unacceptable for some mobile identification scenarios. In some cases, match results may be submitted to a third-party adjudicator or other operator for further action.

2.2.3 Usage Locations, Environment, and Communications

Handheld biometric devices are constrained by their communications capabilities, and the physical environments they can operate in. Device requirements depend on the expected range of operations.

Fixed-Location Operations: Access Control and Border Control

While permanent biometric operations at a fixed location are generally supported by non-mobile devices, specific scenarios may call for stationary handhelds. Where real-time communication is necessary, communications can be achieved through USB or Bluetooth, or other wired and short-range wireless technologies. Wired connections may be used across all ranges of operations to download biometric and logging information when units are returned to their base.

Handheld devices may be used to augment existing biometric access points, to increase throughput during expected periods of large access volumes. They may also be deployed temporarily at existing access points that are not biometrically enabled, for example to increase the security perimeter at a public event.

Handheld devices also provide flexibility in day-to-day access control operations if not all persons are subjects to biometric or non-biometric screening. When throughput is constrained by available physical

space and biometrics are used as a secondary screening option, a handheld form-factor may be more appropriate.

Fixed-Area Operations: Authentication, Attribution and Biometric Signature

Biometrics may be used for location-constrained identity operations that do not require strict access control. Fixed-Area Operations are generally performed in indoor environments. Where real-time communication is necessary, these operations can be supported by 802.11 WiFi, and similar local wireless networks.

Biometric authentication can secure general access to mobile devices needed for day-to-day government operations. Biometric authentication can also confirm that employee and citizens are authorized for specific benefits, information, or actions.

Biometric signatures provide strong attribution for package tracking, auditing, and chain of custody, with minimal impact on existing processes. Biometric verification can also be used in a criminal justice environment to confirm prisoner identity in less-secure locations, such as courthouses.

Mobile Operations: Identification and Situational Awareness

Hand-held devices can provide real-time identification and watch list/warrant detection capabilities throughout a wide area of operations. Mobile Operations may be performed in outdoor environments, requiring improved connectivity and device ruggedness.

Improved situational awareness improves officer safety, reduces missed opportunities, and increases efficiency of law enforcement and security activities. On-the-spot identification may reduce unnecessary detainments, benefiting both civilians and police. However, mandatory identification requirements – especially when not fixed to physical location - can endanger privacy and civil liberties, and conflict with cultural norms.

2.3 Targets of Evaluation

Hand-held biometric deployments consist of several components, which must be individually and collectively evaluated against technical, business, cultural, and legal requirements and constraints. Based on system requirements, evaluations may support initial analysis of technology alternatives, identify applicability of existing devices or systems, assess the relevance of pilot system outcomes, or validate a final deployment against formal requirements. Targets of evaluation in a mobile biometric deployment include:

- Biometric Handheld Device
- Biometric Matching and Storage Systems
- Communications Network
- Operating Environment
- Locally Stored Enrollment Data
- Centrally Stored Enrollment Data
- Associated Reference Data
- Subject and Target Populations
- System Operators
- Collection Workflow, Human-Machine, and Operator-Subject Interaction
- Business Processes

A comprehensive mobile biometric deployment methodology begins with appropriate technical requirements derived from business needs and constraints, and defining a set of available technical solutions. Procedural design based on these requirements incorporates human and environmental factors into identification processes, further defining data, technology, and communications impacting system design and architecture. A holistic evaluation of system impact considers the systems expected technical capabilities and performance, as well as its impact on direct and indirect stakeholders.

2.3.1 Requirements Gathering

Defining application scale and parameters is an essential first step in determining how biometrics can be deployed successfully.

Performance Requirements. Acceptable limits for the percentage of users unable to enroll, false match and false non-match rates (for 1:1 systems), and false positive and false negative identification rates (for 1:N systems) drive technology and hardware / software selection. In mobile biometric systems, enrollments are often performed through a separate workflow, system, or agency. Users unable to enroll in a particular biometric system must be authenticated by some other means, either through another biometric or a non-biometric authentication process, necessitating parallel technologies and policies with a small form factor. Some users may be able to enroll on standard equipment, but consistently unable to provide usable data on mobile devices. Establishing system settings and policies to reduce FTE and Failure to Acquire (FTA) rates can impact other system performance rates. For example, to reduce FTE, lower quality data may need to be accepted for enrollment. In some systems, this can lead to more false matches; in others, it leads to false non-matches.

Further, the deployer may need to build in allowances for longer enrollment transaction times. In other performance tradeoffs, higher-security deployments usually minimize false match rate (or false positive ID rates) at the expense of increasing false non-match rate (or false negative ID rates).

Size of subject, enrollment, and target populations. Mobile devices are often used in an "open set" system, where not all potential subjects are enrolled, or of interest. In this configuration, identification accuracy is driven by the number of subjects who may be encountered, rather than the size of the enrollment database. A smaller database decreases the number of "imposter" comparisons performed, but proportionally decreases the probability that the encountered subject is enrolled for a "genuine" comparison.

Size of access, derogatory, or watch-list databases. Watch list database size and composition is a major determinant of mobile identification system design and calibration. Mobile devices vary in the number of biometric reference files that can be stored and matched on the device. Larger watch lists require more storage, as well as processing power to return timely results.

When referring to existing test data from "closed set" evaluations, it is generally more appropriate to consider the total number of subjects encountered, rather than the total number of database enrollments. Increased database size increases the total number of matches that must be considered by the system user, trading off between workload and detection rates. Changes in database size should not be considered to change the probability that any given match is correct, and mobile devices should generally be calibrated such that the user does not need to adjudicate multiple candidates.

Accuracy can be improved by loading subjects who are more likely than average to be encountered – effectively increasing the number of "genuine" comparisons that are performed compared to the number of "imposter" comparisons. Watch lists are often tiered, allowing for the most critical persons of interest to be included on most devices, in addition to locally relevant persons.

Dedicated enrollment process. The criteria for determining where enrollment in a biometric system might take place include availability of personnel to conduct enrollment, authority over enrollment process, ability to perform authentication, infrastructure, synergy with existing applications, and universal availability. Depending on the application, enrollment may occur at a variety of locations, including airports, financial institutions, and visa issuance centers. A mixture of locations may also be the best solution.

Existing infrastructure. Before any large-scale deployment, much investigation must be done to determine current infrastructure and capabilities so that necessary updates and changes can be addressed up front. Mobile biometric devices generally do not provide sufficient data quality for enrollment

operations, requiring either distinct biometric enrollment centers and workflows, or a distinct biometric program that incorporates enrollment.

Location and Environment. Mobile identification systems may be used across a range of unconstrained environments, and introduce a range of subject, sensor, and presentation factors that degrade the quality of collected biometric samples. More extreme environments may drive requirements for ruggedized or maritime devices that can operate reliably without component failure. Areas of operations and available networks define requirements for device connectivity.

2.3.2 Procedural Design

The processes through which users interact with biometric systems, through which enrollment agents acquire biometric data, and through which administrators manage the biometric systems are essential determinants of biometric technology selection and system design. For example, the deployment of certain biometric technologies mandates query response times which may be longer than encounters can reasonably last; similarly, collection processes may need to be streamlined to align with flexible operations outside of a fixed facility. The following factors must be addressed:

User Interaction. The degree of cooperation anticipated in a given application can have a direct impact on performance. Biometric applications are optimized to verify and identify cooperative individuals, those who willingly and knowingly provide data to biometric systems. Non-cooperative individuals are those who do not alter their behavior in the presence of a biometric system: they neither attempt to evade the biometric system nor do they deliberately engage the system. Users unaware that a biometric system is operating are by definition non-cooperative. Uncooperative users deliberately attempt to evade biometric systems by altering appearance or interacting with an acquisition device in a manner that reduces the likelihood of being identified. The large majority of individuals on watch lists will most likely be uncooperative, altering their behavior or appearance to evade detection systems.

Enrollment Agent Interaction. System operator supervision is required during enrollment to ensure high-quality enrollment and to ensure that identity-related information is validated. Because enrollment events can seem intuitive, such as placing a finger on a finger-scan device or an eye in front of an iris-scan device, enrollees may not understand that a detailed procedure needs to be followed for optimal image capture. Biometric systems have sophisticated image quality assessment modules that are capable of determining whether an image was correctly submitted to the system. Regardless, even these sophisticated environments require the presence of a supervisor to ensure that each user enrolls successfully.

Enrollment must also occur through a process which deters and detects fraudulent enrollment attempts. Procedurally, the implication is that an enrollment agent will interface with an individual and will be associated with the transaction in case collaborator fraud is suspected. Reasonably close supervision ensures that the correct biometric data is submitted, and that the quality of this enrollment data is sufficiently high. High-quality enrollment is critical to maximizing biometric matching accuracy.

High-level design of enrollment methods and process flows. Enrollment is likely to be a several minute process, depending on the depth of background information provided and the type of biometric required. Circumstances which can elongate enrollment include submission of low-quality biometric data, difficulty providing proper biographical data, or uncertainty regarding validity of identification documents.

Fraud-related risks will be reduced if individuals are enrolled in all applicable biometric systems -- both background check and transactional verification -- at one time. Providing biometric background check data, for example, then enrolling in a transactional system at a later date or in a different location increases the risk that an imposter can subvert the system. By acquiring background check data and transactional biometric data under the supervision of system operators, one can be certain that each biometric data element is from the same individual, should more than one biometric be utilized.

Depending on the technology deployed, enrollment may take place on a vendor-specific device or on a standardized, universally compatible acquisition device. For example, enrollment in fingerprint systems may be on a specific vendor's unit or may occur through RCMP-compliant hardware with 500 dpi and 8 bit grayscale capabilities. In addition, depending on project scale, deployment may be centralized or distributed; distributed enrollment would require some type of central connectivity as well. Enrollment is not only impacted by the biometrics and devices deployed, but by the amount of biometric data collected for a given technology. Acquiring multiple fingerprints, for example, either requires an attentive operator and an elongated enrollment process or requires an expensive device capable of acquiring more than one fingerprint at a time. In the case of watch list search applications, the requirement for 1:N matching may drive the number of samples enrolled.

At the time of enrollment, the biometric acquisition system must be capable of immediately assessing the image quality and soliciting a re-submission if necessary. Vendor-specific templates are generated for each biometric device to be used in 1:1 verification. These templates are used to verify travelers at security screenings, boarding gates, vehicle checkpoints, and other suitable locations at ports of entry.

Fallback enrollment processes. Where explicit enrollments occur, some percentage of individuals will be unable to enroll in the primary biometric technology, such that they will be unable to be screened as part of the identification or verification program. Providing for alternate means of biometric verification may be extremely difficult. Not only would parallel enrollment processes need to be established, with the accompanying increase in hardware, software, and training costs, but the technology would need to be present in a scenario where physical encumbrance is already at a premium. Multi-modal devices are general heavier, more expensive, and physically larger than single-modal devices, requiring more complicated and lengthy subject interactions. Providing for robust non-biometric verification methods for individuals unable to enroll may be the most viable option.

High-level design of identification and verification methods and process flows, including number of permitted attempts, fallback authentication. In a typical identity verification transaction, an individual provides biometric data to compare against the template stored on an electronic identity credential or document. Alternatively, the credential may provide an optical or electronic reference code to retrieve an enrolled sample for comparison. The 1:1 match generally takes place on the mobile device, but may be transmitted with a reference code for off-device matching.

In a typical watch list search, reference biometric data for multiple persons are stored on the mobile device. In a typical identification search, reference biometric data for large numbers of persons are stored in a remote location for matching. Identity matching against mobile devices may be inappropriate for throughput-sensitive operations.

Biometric and non-biometric data required in enrollment and registration processes. Documents such as passports, birth certificates, and drivers licenses must be checked to confirm as best possible the claimed identity. A hybrid model which combines online provision of background data with in-person data collection may be possible, though this opens up new fraud opportunities: a method of in-person validation of the individual who provided the online data would be necessary.

Process for flagging and intercepting individuals present on watch lists. Systems can be configured to alert operators when an individual is flagged as a potential match, and can retrieve watch list information (such as a face image or other personal information) to compare against the live subject or live image. System operators must determine whether the flagged individual and the watch list individual are the same person. The system's threshold for matching, which translates into the number of individuals flagged, has a direct impact on this process. If the system is configured to be highly sensitive to potential matches (i.e. configured with a low match threshold), then a substantial number of matches may occur on a daily basis.

For national and international watch lists, the likelihood of actually encountering individuals on watch lists is quite low. Over time, if no legitimate matches are located despite the substantial number of matches returned by the system, it is possible that system operators will come to anticipate that any returned matches will be false. Security thresholds can be increased to reduce the number of false matches, requiring higher match scores to alert device users. In this case, the likelihood of an individual evading detection increases.

For local watch lists or warrant lists, likelihood of encounter will be significantly higher. At the point of operator notification, the processes are non-biometric: the system has fulfilled its objective by flagging a suspect for human intervention. The decision of the biometric system is a trigger to subsequent investigation, not a final statement as to the legitimacy of the match. Even at this stage in the intervention process, the flagged and manually verified individual may well not be the individual present on the watch list.

If a mixed list of local warrants and unlikely "high value targets" is deployed, operators used to seeing match results for local subjects may misinterpret a rare HVT match as being equally likely. Authorities will need to follow a path of moderation: though some type of intervention is necessary, overly accusatory intervention will be viewed as problematic. Training should specifically address the point that identical match scores do not mean identical match likelihood, and HVT enrollments should prompt specific instructions to the operator. Procedures for exceptional cases must be sensitive to both the potential danger posed if the match is correct, and the increased probability of misidentification.

Enrollment-level biometric data quality assessment. In order to reduce software deployment costs, template generation may not need to take place at distributed enrollment points. Image acquisition may be sufficient, with centralized matching and template generation taking place. However, automated quality checks will need to be established to ensure that data is usable for template generation.

Feasibility of opt-in versus mandatory biometric usage. Unless used by a small set of employees at a fixed location, mandatory and comprehensive enrollments are generally not possible for handheld biometrics. Less-mobile biometric systems are often more appropriate for Enrolling travelers from a variety of countries with a variety of travel documents presents significant challenges, not the least of which the large number of enrollments which must occur within a dedicated span of time in order for full-scale deployment to come online.

Failure to enroll, false match / false positive ID, and false non-match / false negative ID rates. Error rates for biometric modalities are highly application-dependent and are a function of system design and calibration. Technologies have matured to the point where enrollment rates and false match / false positive ID rates are manageable in almost all application domains. For handheld real-time identification system's the primary performance related challenge for face, fingerprint, and iris recognition systems is reduction of false non-match and negative identification rates associated with lower sample quality and reduced number of biometric instances captured.

Systems in which enrollment and recognition take place through different device types are more prone to false negative errors than those that use the same device for enrollment and recognition. This is particularly a challenge for face recognition systems. While cross-device implementations may be unavoidable, system designers will often implement separate thresholds for intra-device and cross-device matching. On-device algorithms and biometric templates will generally be less accurate, due to concessions for physical size and reduced processing times. Mobile identification devices are more likely to incorporate silicon sensors, while comparing against enrollments acquired through optical fingerprint or livescan devices.

Time lapse between enrollment and recognition transactions is also a strong contributor to false non-match rates. Again, this phenomenon is likely to impact face recognition more so than fingerprint or iris recognition due to temporal impacts on face appearance.

2.3.3 System Design and Architecture

With the core technology or technologies capable of addressing application requirements defined, the Large-Scale methodology identifies the basic biometric system infrastructure best-suited to successful implementation. While developing a detailed, full-scale system design and architecture may be beyond the scope of initial project requirements, providing a basic assessment of system design and architectural elements is a critical step in determining how well biometrics will address the core requirements. Areas to address include:

Schematics for biometric data storage, matching, and transmission. Mobile Biometric systems are comprised of several biometric subsystems whose storage, matching, and transmission architectures vary. Further, a single capture device may be an input to multiple subsystems whose architectures vary. Mobile devices are typically used to execute 1:1 matches based on data previously acquired from the same subject. This 1:1 matching often takes place on a central host that stores fingerprint data in a retrievable and matchable template format. At the same time, these same fingerprint images will function as probes in 1:N watch list searches that occur on the device, and are executed in real time to determine if the individual is on any stop list. Fingerprint data will not be transmitted as uncompressed images. Instead, fingerprints will typically be WSQ-compressed at a ratio of approximately 15:1, reducing transmission overhead. The trend for fingerprint, iris, and face remains toward (1) retention of images through the capture and matching lifecycle and (2) maximum compression of image while retaining sufficient information so as to support identification performance.

Storage and usage of identifiable and template biometric data. For interoperability with ANSI-NIST-ITL based transmission standards, such as the RCMP NIST interface, mobile biometric systems generally transmit identifiable data in the form of face and fingerprint images. This data is generally retained for expert examination on "yellow resolve" matches, and for future interoperability. Initial large-scale border implementation of iris recognition was based on retention of templates as opposed to images. While retention of identifiable image biometric data is seen as presenting greater privacy risks than retention of templates, this risk is typically seen as manageable. Because this data is only used in exceptional search workflows, system design can isolate image data after template extraction with strongly encrypted storage. A reduced-resolution thumbnail image may be retained for return with any matched subjects. This thumbnail image is generally not of high enough quality for automated biometric matching, reducing the privacy impact associated with its retrieval and transmission under normal operations. Large-scale matching systems maintain indexed template data in RAM arrays or clusters. Hand-held devices often maintain watch list data consisting of templates, thumbnail photos, and textual information describing the person of interest and instructions if encountered.

Legacy data processing requirements. Mobile biometric devices often leverage a separate enrollment workflow, which may be pre-existing. These biometric records do not generally need conversion for mobile accessibility, with the exception of entries on a watch list or access list. Active management of a biometrically enabled watch list must include generation and dissemination of reference templates for any included subjects.

2.4 System Impact

2.4.1 Privacy Requirements and Impact: Biometric System Impact on Information and Personal Privacy.

With basic system design and architecture elements reviewed, and core technologies to meet project requirements identified, the methodology calls for assessment of the potential privacy impact of each of the applications. The privacy assessment addresses both informational privacy, related to the collection, storage, and usage of biometric data, and personal privacy, related to the impact biometric systems may have on individuals' personal or religious beliefs. Areas to address include:

- Privacy challenges encountered in each of the applications, evaluated through a formalized privacy framework
- Limitations on collection, use, and retention of data
- Likelihood of, and protections against, privacy-invasive biometric usage
- Association of biometric with unique identifiers
- Controls in place to limit system scope and capabilities
- Individual consent to biometric enrollment and authentication
- Disclosure of system purposes
- Incorporation of privacy-related best practices
- Requirements for privacy-sympathetic data storage and processing
- Impact of privacy requirements on system design
- Public acceptance of biometric technology
- Use of anonymous and pseudonymous identifiers
- User perceptions of relative privacy of biometric technologies: personal and informational
- Ownership of biometric data
- Positioning biometrics as a privacy-enhancing or privacy-sympathetic technology
- Impact of privacy legislation and best practices, requirement for new or altered privacy-related legislation
- Criteria for successful deployment

An assessment framework for biometric technologies and mobile biometric applications is presented in greater detail in the section entitled "BioPrivacy Assessment: Mobile Biometric Applications."

2.4.2 Legislative Requirements and Impact: Policy, Regulatory, and Legal Issues

The state of existing legislative, regulatory, and policy requirements will likely have a decisive impact on mobile biometric initiatives in one or more of the applications. Legislation and policy may need to be developed in order to support or frame the use of mobile biometrics; access to appropriate channels may be a precondition of successful piloting and deployment. Areas to address include:

Policy issues relevant to the use of biometrics in mobile biometrics. Most legislation developed which frames the use of mobile biometrics in the public sphere will likely have as a central focus the potential privacy impact of the biometric system. The types of privacy-invasive usage envisioned include expansion of biometric activities outside of originally intended purposes, voluntary nation of biometric collections, and security of biometric data distribution. Policy framing the use of biometrics can assume one of two privacy-protective approaches. In one approach, policy is designed to ensure that systems *are not* used in a privacy-invasive fashion, with controls in place such as limitations on collection, usage, and disclosure. The other approach is to ensure that the biometric system *cannot* be used in a privacy-invasive fashion, such that the system cannot be abused even in the absence of controls.

Provincial and federal legislative developments framing the deployment of mobile biometrics. Currently, there is no specific Canadian legislation governing the use of mobile biometrics. However, the Office of the Privacy Commissioner (OPC) releases comments and recommendations to agencies with planned biometric programs in place. These comments are contained primarily within the Annual Report to Parliament, and are used to inform future legislation. OPC also provides a biometric-specific framework for privacy evaluations, and has provided commentary on the notional use cases described later in this report.

Applicable biometric legislative and policy developments outside of mobile biometrics. Though neither The Privacy Act nor the Personal Information Protection and Electronic Documents Act (PIPEDA) have specific language to address the use of biometric technologies in government programs, they establish basic privacy guidelines and principles which must be adhered to by organizations that collect, use and/or disclose personal information in the course of commercial activities.

2.4.3 Stakeholder Impact: Defining External Determinants of Project Success.

Large-scale biometric projects impact, and may require cooperation from, a range of external government agencies as well as corporations, industry consortia, and public advocacy groups. It is a critical task to identify and assess the impact of biometric deployments on these and other project stakeholders. Areas to address include:

Defining key stakeholders – governmental and non-governmental. There are a number of stakeholders in mobile biometric systems, some of which have stake in the system's success, others of which would prefer to see the systems capabilities limited. Entities with an interest in mobile biometric operations include the following:

- Law enforcement agencies, both local and federal, who may be the primary users of a real-time identification capability.
- Public interest groups, who have a stake in understanding how identifiable data is used, how mobile collection operations encroach on the public sphere, and how sufficient oversight can be incorporated.
- Other security-related federal and provincial agencies, who may benefit from augmentation of current biometric capabilities, or development of new biometric initiatives.

The impact of any system under consideration on each of these stakeholder groups must be estimated and accounted for before deployment.

Synergies with government agencies and programs. As the central holder of biometric data, RCMP will be primarily responsible for a comprehensive real-time identification program. If used for identity verification, data from existing credentialing programs must be accessed and integrated. For example, in a border security solution Canada Border Services Agency is directly responsible for securing Canada's borders, Passport Canada is responsible for issuance of Canadian passports, and Citizenship and Immigration Canada oversees all visa processing for foreign nationals wishing to visit, work in, or move to Canada.

Managing public expectations and perceptions through education and outbound messages. Public acceptance of biometrics is often linked with knowledge of and familiarity with the technology. Clearly defining benefits for the end user – whether a system enhances convenience or security – often increases positive attitudes toward biometrics.

Addressing public advocacy groups. With any mobile biometric deployed that may impact the daily lives of citizens, numerous advocacy groups will have concerns and interests that need to be addressed. Transparency can significantly assist in maintaining positive relations with privacy groups and any organizations that may exhibit fears associated with widespread use of biometrics. Information and processes should be disclosed wherever possible, when this does not negatively impact program integrity or impinge on national security.

Piloting as educational tool for stakeholder perception. Before any large-scale deployment, pilot programs are conducted to gain valuable operational performance metrics and feedback from users and stakeholders. Pilot programs afford the opportunity to test a system in a supervised environment in which parameters may be changed and settings refined based on interim results. Pilots provide deployers with actionable insights into program improvements and changes necessary for full-scale implementation.

2.5 Business Case

2.5.1 Cost Assessment and Funding Alternatives: Analysis and Breakdown of Estimated Costs and Cost Avoidance for Biometric System.

A critical factor in providing a framework for assessing biometric projects is the cost of deployment and maintenance as well as the potential cost avoidance attributable to the project. In addition, locating

alternate funding opportunities can significantly reduce the financial risks involved in large-scale deployment. Areas to address include:

Hardware. While "all-in-one" mobile biometric devices are significantly more expensive than single-sensor models with near-field communications, cheaper models must generally be coupled with other computing devices capable of longer range communications. The dynamic nature of mobile biometrics allows for a more graduated "ramp-up" period, but hardware must be in place initially for backend matching or transmission to a 3rd party matching service (such as RCMP RTID).

Software. Mobile identification systems will include moderate costs for central matching components. The associated costs are contingent on the anticipated number of comparisons, the size of the user population, and the accuracy and response time required. Central matching components are an initial cost, required before the system is fully operational. If utilizing an existing 3rd party system such as RCMP RTID, mobile devices will increase the total transaction workload. Additional information technology and licensing costs will apply, and cost sharing among federal, provincial, and local users must be determined.

Integration of biometric and non-biometric systems. All new devices need to be integrated within existing facilities. Costs included will be associated with the integration of mobile biometric devices with existing store-and-forward systems, or with new matching systems. The installation of communications and power networks will also contribute to the system costs. Integration is an initial cost, required before the system is fully operational.

Requirements for dedicated professional services personnel. Costs for annual services, support and maintenance are normally set at 10-15% of the total hardware and software bid. Although the amount of professional services necessary once the system is running is uncertain, and will be based on whatever modifications to the system become necessary, it is reasonable to assume a similar cost level in this project. This is an ongoing cost, which will be encountered over the course of the project.

Long-term system auditing and maintenance. Moderate costs will be involved in the central software for mobile biometrics related to monitoring and auditing capabilities. This central software is an initial cost, required before the system is fully operational. In addition to central software for a matching repository, each federal, local or provincial user will require auditing and maintenance applicable to their local domain.

Initial and ongoing training requirements. A mobile biometric system will require training on proper collection techniques, particularly important due to its use in unconstrained environments. This is an ongoing cost, which will be encountered over the course of the project.

2.5.2 Risk Factors and Recommendations

For mobile biometric applications, the following general risk factors and recommendations have been identified:

Risk Factors

- Integration with existing systems may be the most difficult system design component. In a law enforcement setting, integration with existing livescan connectivity may simplify plans and reduce costs. However, any wireless or cellular deployment will introduce significant security impact to domains designed for wired-only security. In addition to technical difficulty, governance processes for information security will complicate deployments of wireless, free ranging devices that store biometric data at rest.
- Careful biometric placement or interaction is required to verify successfully on most devices, such that users will need to learn to interact with devices for maximum accuracy and performance. Because mobile devices are often used in situations where subjects will not become regular users of the system, collection will most likely be slower and more difficult to use than existing systems. This can have a potential impact on process flows.

- There is increasing awareness that biometric systems do not provide 100% accuracy; while errors may be rare, they do occur in all biometric systems and technologies, especially with smaller and cheaper sensors. While mobile devices can follow voluntary Subject Acquisition Profiles defined by the FBI/NIST Mobile Device Best Practices guide, these standards define sensor requirements rather than accuracy requirements. Deployers may not have access to data on performance and accuracy prior to system installation. Data supplied by manufacturers is often reflective of ideal, as opposed to real-world, performance.
- Processes must be established to accommodate individuals who cannot use a particular technology of who are falsely "not matched" by the system. While a necessity of any biometric deployment, fallback processes can result in increased system costs and can reduce system security.
- Mobile systems are generally dependent on enrollments from distinct large-scale biometric systems. Enrollment can present major logistical challenges, and reduced oversight into this process increases risk for the mobile system. Alternatively, an existing and stable source of enrollments may greatly reduce deployment risk associated with enrollments, to a question of biometric data interoperability.
- Biometric technologies are often not interoperable. Enrollment on one fingerprint device, for example, cannot be verified through another vendor's fingerprint algorithm. The interoperability problem can be a major impediment to large-scale deployment.

Recommendations

- Despite the privacy risks, identifiable biometric data – such as fingerprints and facial images – must be stored in a central biometric system. This enables criminal background searches to be resolved with minimal impact on travelers, and may allow for automated enrollment in new technologies as they emerge, reducing device obsolescence.
- Common providers for mobile-ready devices, communications networks, and store-and-forward systems reduce integration risk for potential provincial and local users. Likewise, clear guidance on security protocols for hand-held devices with wireless connectivity increases probability of adoption.

3 Hand-Held Mobile Biometrics Technologies

3.1 Modalities

3.1.1 Fingerprint

Fingerprint technology utilizes the distinctive features to identify or verify the identity of individuals. Fingerprint recognition is the most commonly deployed biometric technology, used in a broad range of physical and logical access applications. Fingerprint recognition refers to use in either 1:1 verification or small-scale identification against hundreds or thousands of enrolled records. Large-scale systems that match millions of fingerprints are referred to as AFIS (automated fingerprint identification systems). AFIS implementations are much more complex than 1:1 fingerprint implementations, though mobile biometric systems often include both 1:1 and 1:N fingerprint recognition, and reach back to 1:N AFIS.

Fingerprint systems are comprised of image acquisition hardware, image processing components, template generation and matching components, and storage components. Acquisition components are incorporated into mobile devices, with processing, template generation, storage, and matching components varying according to product and deployment.

Fingerprint: Strengths	Fingerprint: Weaknesses
• Proven technology capable of high accuracy • Performance (accuracy, throughput) of leading technologies is well-documented and understood • Ability to enroll multiple fingers; exceptionally high accuracy for tenprint collections • Ergonomic, easy-to-use devices • Fingerprint data is almost universally interoperable, facilitating searches against watch lists	• Performance can deteriorate over time • Association with forensic applications • Users can intentionally damage fingerprints, reducing performance • Implementation of large-scale systems requires highly specialized expertise for performance tuning and optimization

Table 1: Fingerprint Strengths and Weaknesses

The five stages involved in fingerprint verification and identification are image acquisition, image processing, location and encoding of distinctive characteristics, template creation, and template matching.

Fingerprint systems acquire one or more fingerprint images and convert images to digital format. Image processing subroutines eliminate gray areas from the image by converting the fingerprint image's gray pixels to white and normalizing ridge width and flow. Fingerprint recognition systems utilize proprietary algorithms to map the absolute and relative position of minutiae, the distinctive points found in fingerprint ridges. Large-scale systems also use ridge flow information. Algorithms compare template data from one or more fingerprints, working through permutations of minutiae offsets to identify and score similarities. The resulting acceptance or rejection of the user's access is based on reaching an acceptable level of correlation between the two templates. A correlation threshold is necessary because subtle changes in fingerprint placement and minutiae recognition mean that no two fingerprint templates will be exactly alike.

Positive and negative error rates, as well as enrollment failure rates, are low for most fingerprint devices and systems, assuming that multiple fingerprints are acquired on enrollment. A small percentage of users, varying by the specific technology and user population, are unable to enroll in some fingerprint systems. Furthermore, certain demographic groups – such as elderly populations and manual laborers – often have lower quality fingerprints and are more difficult to enroll. Although the fingerprint is a stable physiological characteristic, a variety of factors can cause the performance of some fingerprint recognition technologies to worsen drastically over time, particularly when a limited number of fingerprints are used for matching. Although high-quality enrollment improves long-term performance, users who work with their hands are likely to see increased error rates over time.

Fingerprint recognition technology includes peripheral devices, imbedded devices, wall mounted devices, and large units designed for heavy-duty operation. For mobile biometric deployments, which as of now only include single and dual fingerprint capture, the primary question in terms of device selection is whether a full AFIS-quality tenprint submission must be collected.

Single-finger readers are suited for deployments in which no more than two positions (e.g. left and right index) are acquired. Full tenprint collections can be achieved with dual-finger readers, but are associated with significant increases in collection times, and increased occurrence of "sequencing errors," where finger position is misidentified. Whereas fingerprint systems that leverage all ten prints are capable of robust identification against databases with several tens of millions of enrollees 2-finger systems typically will not scale to more than several million enrollees.

For 1:1 on-device matching, one or two fingerprints from a "PIV compliant" sensor will generally be sufficient (e.g. when fingerprint data is stored on a smart card). In these 1:1 applications, silicon fingerprint sensors are often deployed. Silicon sensors are smaller and less expensive than optical sensors, are less resistant to certain types of wear and tear, and can support a wider range of incorporate liveness detection capabilities than most optical devices. Leading mobile devices generally offer an option of silicon or optical components.

3.1.2 Face Recognition

Face recognition technology utilizes distinctive facial features to verify or identify individuals. Face recognition is primarily deployed in 1:N applications, though improvements in system and workflow design (as well as digital imaging) have increased the performance of face recognition in 1:1 applications. Used in conjunction with ID card systems, booking stations, and for various types of surveillance operations, face recognition's most successful implementations take place in environments where cameras and imaging systems are already present.

Face recognition systems can range from software-only solutions that process images acquired through existing cameras (e.g. still or CCTV) to full-fledged acquisition and processing systems with dedicated cameras and illuminators. In some face systems, the core technology is optimized to work with specific cameras and acquisition devices. More often, the core technology is designed to enroll, verify, and identify face images acquired through various methods such as static photographs, web cameras and surveillance cameras. Face recognition systems are not often integrated into 1:1 physical access applications and are more likely to be used in large-scale identification or surveillance.

Face Recognition: Strengths	Face Recognition: Weaknesses
• Does not require user training or effort • Can often leverage existing image databases and existing photograph processes • Capable of identification at a distance • Capable of rapid 1:N identification with relatively little processing power • Performance improves hand-in-hand with camera quality and image resolution	• Susceptible to high false non-match rates in 1:1 and 1:N applications • Changes in acquisition environment reduce matching accuracy • Changes in physiological characteristics reduce matching accuracy • Lighting, and camera angle greatly reduce matching accuracy

Table 2: Face Recognition Strengths and Weaknesses

Face recognition technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching. Face recognition technology can acquire faces from almost any static camera or video system that generates images of sufficient quality and resolution. Ideally, images acquired for face recognition will be acquired through high-resolution cameras, with users directly facing the camera, and with moderate lighting of the face.

Face images are normalized to overcome variations in orientation and distance. In order to do this, basic characteristics such as the middle of the eyes are located and used as a frame of reference. Once the eyes are located, the face image can be rotated clockwise or counter-clockwise to straighten the image along a horizontal axis. The face can then be magnified, if necessary, so that the face image occupies a minimum pixel space. Once an image is standardized according to the vendor's requirements, the core processes of distinctive characteristic location can occur. Features most often utilized in face recognition systems are those least likely to change significantly over time: upper ridges of the eye sockets, areas around the cheekbones, sides of the mouth, nose shape, and the position of major features relative to each other. Face recognition is not as effective as fingerprint or iris recognition in identifying a single individual from a large database. A number of potential matches are generally returned after large-scale face recognition identification searches. For example, a system may be configured to return the 10 or 100 most likely matches on a search of a 1m-person database. A human operator would then determine whether any candidates are legitimate matches.

Relative to fingerprint and iris recognition, face recognition systems encounter higher false non-match rates over time, as the effects of aging seem to impact face recognition performance to a greater degree than fingerprint or iris recognition. The performance gap narrows if very high-resolution face images are used for enrollment and matching. Assuming that face images are acquired from a fixed distance under consistent lighting and background conditions, the technology is substantially more accurate than is perceived.

Simple changes in user appearance can to have an impact on systems' ability to reliably identify enrolled users. Changes in hairstyle, makeup, or facial hair, or addition or removal of eyeglasses, can cause users to be falsely rejected. Emerging techniques, such as 3D reconstruction and modeling, have led to the development of more robust algorithms which may be less susceptible to such changes.

In an effort to reduce environmental impact on accuracy, deployers and practitioners have become much more cognizant of the role of image quality in face recognition accuracy. When face recognition systems perform poorly (e.g. encounter high false non-match rates), the culprit is often the imaging process as opposed to the matching algorithm. Deployers now, whenever possible, integrate real-time face image quality validation at the point of capture. By enforcing the quality of input images, the overall accuracy and scalability of face recognition systems improves substantially. This approach also brings face

recognition system design closer to that of fingerprint and iris systems, both of which implement rigorous control on input image quality.

Face recognition captured by a handheld device in an unconstrained environment will often not be of sufficient use to act as a primary matching modality. Face matching results can augment primary fingerprint or iris matches, and thumbnails for search candidates are an important component of match reporting and usability.

3.1.3 Iris Recognition

Iris recognition technology encodes and matches iris patterns to identify enrolled users. Iris recognition systems are comprised of collection devices and encoding / matching engines. Collection devices include advanced imaging and optics components along with one or more infrared illuminators. Images may be encoded and matched on the device, on a host PC, or on a central server. Iris recognition technology requires the acquisition of a high-resolution, infrared-illuminated image to effectively locate and encode iris data. Achieving correct focal length and shielding from ambient IR illumination is a difficult challenge for mobile devices. Iris collection devices developed for military use will often incorporate a physical guide to quickly place the device at the correct distance. This feature generally requires physical contact with the subject's face around the eyes, and may be unacceptable in a civil deployment.

Once the iris is located and segmented, a grayscale image is used for feature extraction. Characteristics derived from the iris include the orientation and spatial frequency of furrows and striations. Iris recognition is recognized for (1) resistance to false matching regardless of database size and (2) rapid searches of large databases. Assuming that thresholds are properly implemented, false positive matches should be exceptionally rare. In fact, some iris systems are implemented such that all matches are assumed to be positive. The tradeoff is that iris systems may be more prone to false negatives (in which an enrolled subject is falsely not identified) than, for example, fingerprint systems.

Iris Recognition: Strengths	Iris Recognition: Weaknesses
• Exceptionally resistant to false matching • Default operation is identification mode • High stability of characteristic over lifetime • Hands-free operation • Real-time searches against large databases (e.g. 10m irises) are possible with modest CPU loads	• Acquisition of iris image requires more training and attentiveness than most biometrics • User discomfort with eye-based technology • Glasses can impact performance • Propensity for false non-matching or failure to capture

Table 3: Iris Recognition Strengths and Weaknesses

The acquisition process, and the effort required on the part of the user, differs from device type to device type. More so than in many biometric systems, users must be cognizant of the manner in which they interact with the system: iris acquisition requires fairly precise positioning of the head and eyes.

The iris recognition market has undergone a radical transformation since the late 2000's. Up to that point, a single vendor dominated the market for matching technology, and capture devices had to deliver images that conformed to this vendor's requirements. Since then, numerous iris recognition algorithms have become commercially available; independent testing has demonstrated that many newer algorithms are roughly on par with more established algorithms in terms of speed and accuracy. Further, numerous capture devices have come to market – ranging from low-end peripherals to high-end stand-off devices – greatly expanding the range of applications for iris recognition technology. Perhaps most importantly, current-generation iris systems collect and store iris images as opposed to proprietary templates.

Therefore one of the largest impediments to iris recognition adoption in mobile applications – that of reliance on proprietary data formats – is a non-issue in most modern iris recognition systems.

3.1.4 Multiple biometrics

Multiple biometric solutions involve the submission of more than one biometric characteristic for verification or identification. These submissions can be simultaneous or serial; a second biometric sample may be required if a primary biometric is rejected, or may be required for each verification or identification.
Multiple biometric solutions can be designed to decrease FTE rates, as users unable to enroll in one biometric technology will generally be able to enroll in a second technology. This reduces the need for non-biometric fallback processing. Multiple biometrics can be used to increase security by requiring that an imposter defeat two biometrics to be verified; they can also increase convenience by allowing an individual to verify on a secondary biometric if the first biometric fails.

Using multiple biometrics also allows for the introduction of sophisticated decision logic when verifying or identifying individuals. Beyond a simple yes/no decision in which an individual must match in two systems in order to be verified, "fusion systems" can be implemented in which a near-match in one system allows a lower score in a second system to constitute a match. Similarly, a very low score in one biometric system may require a very high score in a second system in order for an individual to be declared a "match". By combining raw scores from vendor technologies, and adjusting thresholds based on application-specific requirements, deployers can implement more flexible systems.

In addition, using multiple biometrics during enrollment may allow for more rapid and more accurate searches. If one technology is used as a gross classifier, such that a technology eliminates 60% of individuals in a database in a rapid 1:N search, then a more robust 1:N technology can be used to search the remaining 40% of individuals for duplicates.

Many large-scale civil and criminal identification systems in the US incorporate multiple biometric elements during enrollment. This results in creation of biometric profiles for large numbers of individuals that enable future functionality through different technology combinations. Multi-modal hand-held devices originally developed for military use have often been redesigned for law-enforcement and civil use, allowing for use in face, finger, and iris deployments.

Although a handful of vendors are capable of implementing multiple biometric solutions, the percentage of real-world biometric implementations that leverage multiple biometrics is small. Further research into the viability of multiple biometric solutions, in particular "fusion systems" based on intelligent scoring and aligned with external, risk-based scoring systems, is necessary.

Multimodal biometric systems can mitigate certain performance and robustness limitations associated with single-modality systems. A multimodal biometric system based on non-correlated traits is expected to improve matching accuracy and to increase protection against spoof attacks.

A substantial body of knowledge describes various approaches that can provide more robust matching accuracy than single-modality approaches. The fundamental differentiator in multimodal system design is the level at which information from different biometric modalities is combined.

Information can be derived at the feature, decision, or score level:

Feature-level multimodal models utilize feature vectors from different biometric modalities to create a new feature vector, which is then utilized as the basis of future matching. This new feature vector may be more accurate than the two source modalities. For example, algorithms that process fingerprints create feature vectors that generate scores when compared with enrolled feature vectors. If fingerprint feature vectors were combined with face image feature vectors to create a new kind of template, the end result may be a system more accurate than either modality by itself. This represents the most hypothetical multimodal fusion approach.

Decision-level multimodal models utilize match decisions from more than one system to render a global decision. Typical decision-level multimodal system logic includes the following:

If system A = match and system B = match, then system (A+B) = match.
If system A = match or system B = match, then system (A+B) = match.
If system A = no match or system B = no match, then system (A+B) = no match.

An advantage of decision-level multimodality is that insight into specific system operations is unnecessary, and the logic used is very straightforward. A challenge associated with this approach is that performance may be limited by the weaker or weakest of the systems incorporated, such that the system could reduce false non-match rates but encounter proportionally higher false match rates. Assuming that each system's match threshold is managed independently, there is diminished opportunity to intelligently combine system outputs.

Score-level multimodal models utilize system-specific scores resulting from comparisons from multiple biometric systems to generate a single "fused" score used to differentiate impostor and genuine transactions. The primary advantage of this is that a system designer can specify optimal operating points for multiple systems, assign relative weights, and develop statistical models by which scores from divergent systems can be utilized to differentiate genuine and impostor score distributions. Most biometric systems provide access to score data, such that best-of-breed commercial algorithms can be leveraged. Similarity score level fusion relies on the scores generated by each matcher(s) associated with the modalities involved. Scores are processed through a combination of normalization and fusion techniques addressed below.

Of the three approaches, score-level fusion provides the strongest balance of performance and commercial viability. The primary challenge associated with score-level multimodal models is to maximize the benefits of score normalization and fusion based on different algorithms, modalities, and populations.

3.2 Communications

Mobile devices generally incorporate standard OEM components for communications. These are detailed in Section 4, and may generally include wired (USB), near field (Bluetooth), wireless (802.11) and cellular (2G/3G) connectivity. Satellite (BGAN) devices have been deployed, in conjunction with existing satellite communications infrastructure.

4 State of Mobile Biometric Device Market

4.1 Fingerprint Verification

4.1.1 DAP CE3240BW

The CE3240BW developed by DAP Technologies integrates its rugged mobile computing device with an attachable fingerprint reader, 1D/2D barcode reader, smartcard reader, and magnetic stripe reader. Its silicon fingerprint reader captures images at 508 dpi, and provides the operator a means to biometrically authenticate user identity. In regards to its card reading capabilities, the device's readers are compatible with smart cards that meet ISO 7816 and ISO 14443 standards for contact and contactless cards. The battery life of the unit has been recorded to last two to four working days. Communications for the device is limited to 802.11 WiFi, Bluetooth, and Ethernet connectivity.

Technical Specifications:

- Capture Modalities: Flat Fingerprint
- Match Modalities: Flat Fingerprint
- Card Interface: Smart Card, MicroSD
- Wired Connectivity: USB 1.1, LAN
- Wireless Connectivity: 802.11b, 802.11g, Bluetooth
- Cellular Connectivity: GSM [2G], UMTS [3G]
- Internal RAM (GB): 128
- Internal Storage (GB): 128
- Expandable Storage (GB): 2
- Operating System: Windows
- CPU Speed (GHz): 520
- Output Image Length (Pixels): 240
- Output Image Width (Pixels): 320
- Output Image Color: Yes
- Output Image Resolution (DPI): 500
- Length (inches): 7.70
- Width (inches): 3.10 Depth (inches): 2.10
- Weight (lbs): 1.00
- Min Temp. (Degrees C): -20
- Max Temp. (Degrees C): 50
- Ingress Protection (IP): 65
- Other Conformance/Compliance: MIL-STD-810F, CE, RoHS, FIPS 201
- Display Technology: LED
- Color: Yes

Diagonal Length (inches): 3.50

- Technology: Optical
- Finger Types: Flat
- Resolution (DPI): 500
- Battery Life (hrs): 6.00

4.1.2 Datastrip DSV2+TURBO

The DSV2+TURBO is Datastrip's rugged, compact handheld mobile biometric terminal. The unit is used in identity verification and biometric data collection applications including border control. The

DSV2+TURBOis a FIPS 201 certified single-fingerprint capture device, and also reads contact/contactless smartcards. It can be configured to operate for up to 16 on a single battery charge using an upgraded battery option. The unit offers several expansion capabilities including the ability to read magnetic stripes or 2D barcodes, as well as connectivity through USB, CF, serial, Wi-Fi, Bluetooth or cellular technologies.

Technical Specifications:

- Dimensions: 7.3" x 7.3" x 2"
- Weight: ~2.1 lbs.
- Operating System: Microsoft Windows CE.NET Version 5.0
- Processor: Renesas SH47760 True Floating Point Processor
- Display: 3.5" color-reflective TFT LCD indoor/outdoor viewable - 240 x 320 QVGA
- Memory: 64 MB RAM, 256 MB CF storage, expandable to over 4GB
- Fingerprint Sensor: FIPS 201/NIST SP 800-76-compliant UPEK TCS1 fingerprint sensor - 508-dpi capacitive solid-state - 12.8 mm x 18.0 mm sensor area
- Iris Camera: 1.3 Megapixel sensor, 640 x 480 VGA with IR illuminators and full SDK support
- Digital Camera: 3.2 Megapixel sensor, 2048 x 1635 to 160 x 120 with flash and full SDK support - Dept of Field: 0.6 m to 5.1 m
- Keypad: 5-button backlit rubber keypad
- Smartcard Interface: Supports ISO-7816 contact and ISO-14443 A/B contactless smartcards, ISO-15693 optional
- Interface: RS232 serial via docking station, mini USB client (1), USB host (1), CF slots (1 external, 1 internal), RJ45 Ethernet
- Battery: High-capacity rechargeable and user-replaceable Lithium-polymer battery. Upgraded battery operates over 16 hours
- Environmental: IP54, MIL-STD 810F

4.1.3 Datastrip DSVII-PA

"The Datastrip DSVII – PA is customized for remote identification and authentication of traveler's e-Passport and other travel documents. It is approximately 2.7lbs, operates on Microsoft Windows CE, and has a 3.5" color touchscreen monitor with stylus. The device houses a FIPS 201 compliant silicon sensor that captures fingerprints at 508 dpi.

4.1.4 Datastrip EasyRead

The Datastrip EasyRead is a handheld unit designed to validate ICAO-compliant travel documents including passports, visas and identification card. It reads the machine-readable zone (MRZ) on passports, and employs a silicon-based fingerprint sensor to capture user fingerprint images at 508 dpi resolution. Additionally, the EasyRead can connect with remote databases via Bluetooth, WiFi and cellular networks. Technical specifications of the Datastrip EasyRead are as follows:

Technical Specifications:

- Size: 6.7" x 9.0" x 3.0"
- Weight: 3.1lbs
- OS: Windows CE.NET V5.0
- Fingerprint Sensor: FIPS 201 / NIST SP 800-76 compliant; UPEK TCS1
- Scanner: Optical Camera, 4.88" x 1.65" Read Area
- Smartcard Compliancy: ISO 14443A/B; ISO 7816 (optional)
- Battery Life: Up to 12 hours at normal use

4.1.5 Datastrip DSVII-SC

This handheld device weighs about two pounds and combines a contact and contactless smart card reader, a 500 dpi fingerprint sensor for identity verification, and a color display screen. DSVII-SC supports internal wireless communication for data and fingerprint transmission for identification and verification applications involving a database.

4.1.6 Pivaris plusID 60, 75, 90

Privaris' plusID product line includes the plusID 60, plusID 75, and plusID 90. Each device incorporates a built-in, silicon fingerprint swipe reader that is used for access control applications. The device serves to store an individual's fingerprint data, and perform 1:1 matching before granting access to restricted areas. In addition to its fingerprint recognition capabilities, the plusID device serves as a contactless smart card to communicate wirelessly with other ISO 14443 compatible contactless card readers. In this fashion, the plusID functions as both an identity card document and fingerprint recognition reader. Communication with the device is limited to 13.56 MHz, Bluetooth technology, USB 2.0, and IEEE 802.15.4 communication standards.

4.1.7 CEM S3020f (Finger card)

The S3020f reader is a handheld fingerprint and card reader that can be deployed for remote identity authentication and fingerprint verification purposes. Utilizing a Suprema silicon-based fingerprint module, the unit can read and encode fingerprint data as a numerical representation. It can be coupled with a compact flash card to store approximately 100,000 card and biometric records within its local database, and can store approximately 8,000 offline card swipe transactions. Supported card technologies for the S3020f include the HID iClass, 13.56MHz MiFare and Picopass.

Technical Specifications:

- Size: 225 x 100 x 45mm
- Weight: 650 grams
- Operation Lifespan: up to 16 hours (after full charge)
- Communication Interface: TCP/IP using 802.11g WiFi

4.1.8 TransCore TWIC HandHeld Reader (Finger Card)

TransCore developed the TWIC Handheld Reader in conjunction with DAP Technologies and CoreStreet, which can be facilitate remote authentication and validation for the TWIC Program. The handheld unit is DAP Technologies' CE3240B-NA device, and has an attachable 3240-FFC fingerprint reader and contact and contactless smart card readers. The fingerprint reader is compliant to FIPS-201 standards and captures images at 508dpi. The contact and contactless smart card readers are compliant ISO 14443 A/B and ISO 15693 standards.

4.2 Fingerprint Collection

4.2.1 MaxVision 6PAC

The Maxvison 6PAC is a fast finger 10-Print capture systems. The 6PAC uses six independent FIPS 201.1 certified optical fingerprint sensors arranged in a unique patent pending softball sized hand grip which simultaneously captures all fingerprints from either the right or left hand in as little as two seconds per hand. The 6PAC's unique design and capture process eliminates the need for finger segmentation and individual thumb capture traditionally used on a "Four Slap" device. Furthermore each finger is independently processed for FIPS compliance before given a green light on each finger. The device can be acquired with a complete enrollment application.

Technical Specifications:

- Capture Modalities: Flat Fingerprint
- Match Modalities: Flat Fingerprint
- Wired Connectivity: USB 2.0
- Operating System: Windows
- Output Image Length (Pixels): 280
- Output Image Width (Pixels): 352
- Output Image Color: No
- Output Image Resolution (DPI): 500
- Length (inches): 3.80
- Width (inches): 6.00
- Depth (inches): 5.50
- Weight (lbs):1.50
- Min Temp. (Degrees C): -32
- Max Temp. (Degrees C): 50
- Ingress Protection (IP): 65
- Other Conformance/Compliance: FIPS 201
- Technology: Optical
- Finger Types: 4-Finger Slap
- Resolution (DPI): 500
- Conformance/Compliance: PIV
- Device Input: USB 2.0

4.2.2 3M Cogent BlueCheck

One of the latest portable fingerprint scanners that Cogent Systems has developed, the BlueCheck is a mobile biometric device tailored toward local law enforcement use. The BlueCheck is equipped with a small, durable LCD display for real-time feedback, a 500 dpi fingerprint scanner and utilizes Cogent's SecurASIC technology for encryption and image compression. The BlueCheck enables users to perform on-the-spot fingerprint acquisition and matching against the fingerprint templates stored on the device. Additionally, using Bluetooth communication, the BlueCheck is capable of remotely transferring captured fingerprint data to a host, such as a PDA, laptop or cellular device to allow for identification and verification of identity against a centralized database of prints. In order for this to occur, the BlueCheck connects to Cogent's BlueCheck host application, the host device can then submit ANSI-NIST format files via SMTP or FTP to a remote server or AFIS, and then the search can be conducted. Once the search is complete, the BlueCheck receives the search results from the host and displays the results on its LCD display, providing nearly real-time identification for law enforcement personnel.

Technical Specifications:

- Dimensions (H" x W" x D"): 4.5 x 1.7 x.9
- Weight: .2 lbs.

- Battery: Lithium-Ion 3.7V 900mAH
- Fingerprint: 500 dpi, 1 finger, optical or silicon sensor, 0.75'x0.5"
- On-board Storage and Matching: 1200 fingerprint templates, up to 6000 with optional flash drive, can search 500 on device templates in 1.5 seconds
- Communications; Bluetooth (up to 30 feet) USB connectivity capable
- Interface: host PDA must be Bluetooth enabled with Windows 2005 or Pocket PC 2003, LCD size: 0.85"x1.28"; single-handed operation

4.2.3 3M Cogent BlueCheck II

The 3M Cogent BlueCheck® II weighs less than 5 ounces and is available in two models, the BlueCheck II with an FBI-certified 500 ppi optical sensor and the BlueCheck II U with a PIV-certified 500 ppi silicon sensor. With the exception of the type of scanner the features and specifications are virtually identical. Features include a durable color LCD display, Bluetooth communication, and 3M Cogent's proven technology for encryption and image compression. BlueCheck II is FBI Mobile ID SAP (Subject Acquisition Profile) Level 10 compliant according to NIST Mobile ID Best Practices Guidelines, and meets Ingress Protection (IP) Level 54. Designed for single-handed operation, BlueCheck II enables users to perform two types of searches: they can capture and search against fingerprint templates stored on the device, or they can securely transfer captured fingerprints to a host, such as a PDA, laptop, or smart phone, via Bluetooth or USB connection. With Cogent's MobileID application, the host device can submit ANSI-NIST format files via SMTP or FTP to a remote server or to an Automated Fingerprint Identification System (AFIS) for fingerprint identification.

Technical Specifications:

- Capture Modalities: Flat Fingerprint
- Match Modalities: Flat Fingerprint
- Card Interface: MicroSD
- Wired Connectivity: USB 2.0
- Wireless Connectivity: Bluetooth

4.2.4 Intellicheck Mobilisa IM 2700

The IM2700 is a ruggedized mobile device that is designed to read Transportation Worker Identification Credentials (TWIC) cards. It can access data stored on the contact smartcard using 1D or 2D barcodes, magnetic stripe data, or smart chip. Additionally, the reader comes with a silicon-based single fingerprint reader to capture user fingerprint data.

4.2.5 CrossMatch MV5

The Cross Match MV 5 is an all-digital hand-held flat fingerprint capture device. The optical sensor captures a single flat fingerprint at 500 ppi. Fingerprint images are stored locally within the MV 5's on-board memory and can be transferred to a laptop, PC or MDT (Mobile Data Terminal) via a universal serial bus (USB) cable, which also serves as the unit's power source. The MV 5 is intended for state and local law enforcement applications including state, county and highway patrol, border and immigration control, and crime scene and evidence collection applications.

Technical Specifications:

- Fingerprint Sensor: Optical-based Fingerprint Sensor
- Platen Area: 1.00" x 0.96"
- Image Resolution: 500 dpi +/- 5 pixels in X and Y Axis
- Digital Output: Universal Serial Bus (USB)
- Power: 4 x 1.2 VDC NiCad AA Batteries
- Temperature Range: 32oF to 130oF
- Dimensions (H x L x W): 1.94" x 8.00" x 1.88"

- Weight: 1.4lbs

4.2.6 Cross Match Verifier Mw (Finger Capture)

Cross Match's Verifier Mw is a mobile fingerprint device tailored towards military and law enforcement applications. The handheld device captures fingerprint data at 500 dpi resolution, which can be transferred and recorded to independent AFIS systems. Communication with the device is completed through USB connectivity and wireless 802.11 WiFi option. It weighs approximately 1.4 lbs, and the housing is designed to be rugged and withstand harsh environments. The Verifier Mw was recertified in November 2009 by the FBI as tested and in compliance with the FBI's Next Generation Identification (NGI) and Integrated Automated Fingerprint Identification System (IAFIS) image quality specifications. Certification with the FBI's biometric initiatives is an important quality for the product's marketability to both state and local law enforcement agencies. The ability to access, search, and match the extensive database of criminal fingerprints is important to conducting on-site and remote fingerprint identification. Additionally, the certification can help ensure interoperability with future related advanced technology initiatives.

Technical Specifications:

- Capture Modalities: Flat Fingerprint
- Match Modalities: Flat Fingerprint
- Wired Connectivity: USB 2.0
- Wireless Connectivity: 802.11b, 802.11g, 802.11n, Bluetooth
- Max Watch List Size: 10
- Output Image Length (Pixels): 176
- Output Image Width (Pixels): 220
- Output Image Color: Yes
- Output Image Resolution (DPI): 500
- Length (inches): 8.00
- Width (inches): 1.94
- Depth (inches): 1.88
- Weight (lbs): 1.40 Min Temp. (Degrees C):0
- Max Temp. (Degrees C): 40
- FBI/NIST Mobile ID SAP: 30
- Other Conformance/Compliance: FIPS 201
- Display Technology: LCD
- Color: Yes
- Diagonal Length (inches): 2.00
- Technology: Optical
- Finger Types: Flat
- Resolution (DPI): 500
- Conformance/Compliance: PIV
- Battery Life (hrs): 10.00
- Device Input: USB

4.2.7 Integrated Biometrics Watson (Finger Capture)

In early January 2012, Integrated Biometrics announced Watson, a mobile non-optical fingerprint scanner that is FBI Appendix F certified. The FBI certified that Watson meets or exceeds all requirements listed in EBTS Appendix F Mobile ID SAP 45 of the Integrated Automated Fingerprint Identification Systems Image Quality Specifications. The device weighs 115 grams and measures 70 mm by 63 mm by 33 mm. Watson offers unique operational benefits compared to existing certified scanners including IP 67 durability rating, high quality imaging in non-optimal environments, no difficulty operating in direct sunlight, and does not require latent prints to be wiped from the sensor surface. It is capable of performing

both enrollment and matching for single or multiple finger applications. Watson utilizes Integrated Biometrics' patented Light Emitting Sensor (LES) technology. LES technology utilizes a highly engineered charged polymer film that interacts with the specific properties of human skin to illuminate fingerprint images.

Technical Specifications:

- Capture Modalities: Rolled Fingerprint
- Match Modalities: Rolled Fingerprint
- Wired Connectivity: USB 2.0
- Output Image Length (Pixels): 800
- Output Image Width (Pixels): 750
- Output Image Resolution (DPI): 500
- Length (inches): 2.48
- Width (inches): 2.76
- Depth (inches): 1.26
- Weight (lbs): 0.33 Min Temp. (Degrees C): -10
- Max Temp. (Degrees C): 55
- FBI/NIST Mobile ID SAP: 45
- Ingress Protection (IP): 67
- Other Conformance/Compliance: RoHS
- Frame Rate (FPS): 15
- Technology: Other
- Finger Types: Rolled
- Resolution (DPI): 500
- Frame Rate (FPS): 15

4.3 Iris

4.3.1 MorphoTrust USA PIER 2.4 Iris)

The Pier 2.4 is a handheld iris capture device manufactured by L-1 Identity Solutions. The device weighs approximately 1lb and has a recorded battery life of 16 hours. An extended battery life helps to ensure that the device can operate during a single work shift before requiring additional power. Additionally, it has the storage capacity to hold up to 200,000 iris templates, and can transfer information between its internal hard drive to an external database via LAN lines or serial ports. The Pier 2.4 is customized for military applications

Technical Specifications:

- Dimensions (H" x W" x D"): 6 x 3.5 x 1.8
- Weight: 1.03 lbs
- Battery: 16 hours
- Fingerprint: n/a
- Face: n/a
- Iris: 1/3" CMOS sensor; 640x480, 8 bit grayscale; 15fps; focal distance 4-6"
- On-board Storage and Matching: Storage of up to 200,000 templates
- Expansion: n/a
- Communications: LAN lines and serial ports
- Interface: 240 x 320 Color Touch Screen, Built-in minimal keyboard
- Ruggedization: n/a

4.3.2 JIRIS True Eye Access (Iris)

The True Eye Access is a hand-held device that houses JIRIS's proprietary iris recognition camera for varying applications including time & attendance and physical access control. It utilizes one infrared-led CMOS camera, auto focusing, and standard iris image capturing engine to capture uniform iris images. Additionally, the device is network-enabled and scalable for up to 5,000 users with 10,000 iris templates stored during enrollment for each user; images are formatted to meet iris interchange specifications of ANSI INCITS 379-2004/IEC 19794-6.

Technical Specifications:

- Max Templates/Users: 10,000 Iris Template/5,000 users
- Camera Sensor: CMOS
- Camera Resolution: 640 x 480
- Reported Accuracy: FAR: 0.001% FRR: 0.02%
- Recognition Time: < 1 second
- Recommended Read Distance: 22cm
- Viewing Angle: +/- 25 degrees

4.4 Multimodal (Finger/Face)

4.4.1 SAFE MBS

The SAFE MBS (Mobile Biometric Enrollment System) is a case-size portable enrollment solution that can be used to capture users' fingerprints, face images, signatures, and demographic information for passport, visa, and identity card applications. It utilizes the company's biometric capture software known as BioCap to collect and quality check data required for identity card issuance. In the past, the device has been marketed to utilize various Cross Match fingerprint live-scan devices including but not limited to Cross Match's L Scan Guardian, Verifier 310 LC, and Verifier E units. This enables the SAFE ID's mobile solution to capture single, left and right hand four finger slaps, and two thumbprints. Additionally, the unit is equipped with COTS camera unit to capture face images, signature pad, and an optical and electronic document reader.

4.4.2 AMREL DA5+B

The AMREL DA5+B handheld multi-modal capturing device is designed for military applications within harsh environments. It is engineered to resist rain, dust, vibration and shock, and is capable of capturing face and fingerprint images. DA5-B operates on Microsoft Windows Mobile 5.0 and CE, and has wireless capabilities including 802.11, Bluetooth, and GPRS. The optical fingerprint scanner captures images at 500 dpi. The unit also houses a 2-megapixel camera.

Technical Specifications:

- Dimensions (H" x W" x D"): 9.3 x 3.8 x 2.8
- Weight: 1.95 lbs.
- Battery: External: Lithium-Ion 3.7V 3900 mAH rechargeable smart battery, user swappable Internal: Backup Lithium-Polymer, 80mAH for hot-swapping
- Fingerprint: 500 dpi optical sensor; 1000 dpi latent fingerprint camera
- Face: 3-megapixel camera, built-in flash
- Iris: Auto-capture iris scanner
- On-board Storage and Matching: 128 MB Flash Rom
- Expansion: Internal PCMCIA slot (Type II)
- Communications: WLAN 802.11b, g series devices, GSM/GPRS/EDGE, (850/900/1800/1900), Bluetooth 2.0 module, GPS, USB connectivity
- Interface: Display 4" (480 x 640) sunlight readable transflective TFT LCD, Touch screen and stylus; built-in speaker and microphone
- Ruggedization: IL-STD-810F

4.4.3 MorphoTrust USA IBIS (Integrated Biometric Identification System)

IBIS (Integrated Biometric Identification System) is a mobile identification unit for law enforcement applications. IBIS allows field officers to capture high quality fingerprints and facial images on a handheld device. Biometric data acquired by IBIS is transmitted wirelessly to a central site server for validation against law enforcement databases. IBIS captures photographs and fingerprint images in industry standard NIST EFTS format for searches against databases such as AFIS, WIN, MAFIN, IDENT, and NCIC. The device works with Windows Mobile PDAs using existing cellular services.

Technical Specifications:

- Platen Dimensions:1.3" Vertical x .9"
- Horizontal Image Dimensions: 1.0" Vertical x .8"
- Horizontal (500x400 Pixels)2-D Bar Code Reader Format: PDF 417 and 2-D matrix bar codes
- Temperature, Operating: 32 to 104 F (0 to 40 C)
- Operating Humidity: 10% - 90%
- Mechanical Dimensions: 9.7" L x 2.6" W x 2.5" D

- Mechanical Weight: 0.99 lb (15.8 oz)
- Operating Life: Over 500 two-finger bookings per full battery charge
- Life (Standby): Up to seven (7) days

4.4.4 MorphoTrust USA IBIS Extreme

Similar to the original single-handed fingerprint recognition device, the IBIS Extreme is built to withstand harsh environments. It links via Bluetooth to a pre-configured PDA to conduct remote searches, and can be customized to interface with various databases including L-1's ABIS system. The IBIS Extreme has been rated with a durability of IP65 for protection against dust, debris and water.

Technical Specifications:

- Capture Modalities: Flat Fingerprint, Face
- Match Modalities: Flat Fingerprint
- Cellular Connectivity: EDGE [2.5G]
- Operating System: Windows
- Output Image Length (Pixels): 500
- Output Image Width (Pixels): 400
- Output Image Bit Depth: 3
- Output Image Resolution (DPI): 500
- Length (inches): 8.25
- Width (inches): 2.20
- Depth (inches): 2.00
- Weight (lbs): 0.75
- Min Temp. (Degrees C): 0
- Max Temp. (Degrees C): 40
- Ingress Protection (IP): 54
- Other Conformance/Compliance: RoHS

4.4.5 MaxID iDL300

"The iDL300 features on-board contactless card, barcode, and optical fingerprint readers combined with a digital camera and comprehensive wireless communications. The iDL300 is the first biometric mobile computer to incorporate 3G wireless capabilities as standard, providing up to 7.2mb/s data transfer speeds. The WAN connectivity is supplemented by WiFi and Bluetooth communications. Running Microsoft Windows CE .NET 6.0, the iDL300 offers an open, flexible platform. It is supplied with a comprehensive Software Development Kit to enable application development, while MaxID also has a comprehensive range of identity management software applications specially designed to work with the iDL300. Although the iDL300 is compact, the high-impact ABS plastic case is shock tested to survive repeated drops of more than three feet to concrete and is designed to withstand ingress of water and dust.

Technical Specifications:

- Capture Modalities: Flat Fingerprint, Face
- Match Modalities: Flat Fingerprint, Face
- Card Interface: Smart Card, MicroSD
- Wired Connectivity: USB 2.0
- Wireless Connectivity: 802.11b, 802.11g, Bluetooth
- Cellular Connectivity: GSM [2G], EDGE [2.5G], UMTS [3G]
- Internal RAM (GB): 128
- Internal Storage (GB): 1
- Expandable Storage (GB): 1
- Operating System: Windows
- CPU Speed (GHz): 520

- Output Image Length (Pixels): 640
- Output Image Width (Pixels): 480 Output Image Color: Yes
- Output Image Resolution (DPI): 500
- Length (inches): 5.90
- Width (inches): 3.10
- Depth (inches): 1.40
- Weight (lbs): 1.00
- Min Temp. (Degrees C): -10
- Max Temp. (Degrees C): 55
- Ingress Protection (IP): 66
- Other Conformance/Compliance: FIPS 201
- Display Technology: LCD
- Color: Yes
- Megapixels: 1
- Technology: Optical
- Finger Types: Flat
- Resolution (DPI): 500
- Battery Life (hrs): 10.00

4.4.6 MaxID iDL3ID

The iDL3ID is MaxID's ruggedized biometric handheld device capable of verifying an individual's identity using fingerprint recognition, barcode, digital photograph and card based technologies. It is integrated with a 1D/2D barcode reader, contactless card reader that reads ISO 14443 compliant cards, and a 2 mega-pixel digital camera. The built-in optical fingerprint reader is FIPS-201 approved, and captures images at 500 dpi resolution. Its communications capabilities include quad band GPRS/EDGE and 802.11 WiFi.

4.4.7 MaxID iDL500/iDL502

The iDL500 features On-board contact card, contactless card, barcode, and an optical fingerprint reader combined with a digital camera, GPS, and wireless communications (GSM/GPRS/EDGE, 802.11b/g WiFi, and Bluetooth). Additional card reading capabilities are provided by the combined contactless & smart card reader which is FIPS-201 compliant and has iClass capabilities. Optional magnetic swipe & OCR/MRZ accessories allow the operator to screen credentials, including passports, e-passports, Transportation Worker's Identification Credentials (TWIC), Common Access Cards (CAC), First Responder Authentication Cards (FRAC), Personal Identity Verification (PIV), driver's license and other documents. The digital camera is designed to acquire FIPS-201 compliant face images under low-light levels. The iDL500 runs on Microsoft Windows CE .NET 5.0 and 6.0; an SDK is also available. The device weighs less than two pounds and is shock tested to survive repeated drops of more than three feet to concrete and is designed to withstand ingress of water and dust.

Technical Specifications:

- Capture Modalities: Flat Fingerprint
- Match Modalities: Flat Fingerprint
- Card Interface: Smart Card, Other
- Wired Connectivity: USB 2.0, Other
- Wireless Connectivity: 802.11b, 802.11g, Bluetooth
- Cellular Connectivity: GSM [2G], EDGE [2.5G]
- Internal RAM (GB): 128
- Internal Storage (GB): 1
- Expandable Storage (GB): 4
- Operating System: Windows

- CPU Speed (GHz): 520
- Output Image Length (Pixels): 480
- Output Image Width (Pixels): 320
- Output Image Color: Yes
- Length (inches): 9.25
- Width (inches): 4.25
- Depth (inches): 2.50
- Weight (lbs): 1.80
- Min Temp. (Degrees C): -10
- Max Temp. (Degrees C): 55
- Other Conformance/Compliance: FIPS 201
- Display Technology: LCD
- Color: Yes
- Diagonal Length (inches): 3.50
- Megapixels: 1
- Technology: Optical
- Finger Types: Flat
- Resolution (DPI): 500
- Battery Life (hrs): 3.00

4.4.8 MaxID iDL750

Designed for LiveScan enrollment as well as high speed biometric validation, the iDL750 offers expanded functionality of an optical fingerprint reader, dual Contact Smart Card readers, and a 2 Megapixel color camera capable of streaming video. The iDL750 is a mobile computer that includes a 32-channel GPS receiver, bar code reader, and multiple integrated wireless options. The unit's two Smart Card readers make it the perfect complement for personnel who must both be verified for a computer network as well as have the capability to validate additional Smart Cards. Onboard wireless support includes 3G, GSM/GPRS/EDGE, 802.11a/b/g WiFi, and Class 2 Bluetooth as well as additional wireless communications via optional modules. A 1.6 GHz Intel processor gives the iDL750 exceptional computing power permitting high-speed database queries and can accommodate either Solid State or mechanical hard drives, if desired. An SD expansion memory slot is included, along with two USB 2.0 host inputs, an Ethernet connection, twin mini PCI-Express slots, user-accessible SIM card slot, and audio inputs and outputs. Other capabilities, including iris acquisition cameras, are currently in development. A complete computer despite its small size, the iDL750 runs Windows XP, Windows Vista or Windows 7 operating systems. The iDL750 also features a 5.6" TFT display with 1024x600 resolution landscape display that is easily readable in sunlight. A full QWERTY backlit keyboard features 58 keys and directional arrows for navigation. Measuring 9.7" by 7.4" by 3.1", the iDL750 is powered by two hot-swappable batteries and weighs less than four pounds. The iDL750 is ruggedized, and is shock tested to survive a drop of more than four feet to concrete. The unit easily withstands ingress of water and dust, and other daily operating conditions.

4.4.9 MaxID iDLMax

MaxID's iDLMax houses a smart card reader, barcode reader, an optical fingerprint reader, and a contactless passport reader. Additionally, the device is coupled with a digital camera, GPS, and wireless communications such as GSM/GPRS, 802.11 WiFi, and Bluetooth technology. iDLMax is FIPS-201 compliant and weighs less than three pounds. Its intended application is for onsite remote identification.

Technical Specifications:

- Dimensions (H" x W" x D"): 9.2 x 4.2 x2.3
- Weight: 3 lbs
- Fingerprint: 500 dpi; Lumidigm optical sensor; 0.6" x 0.9" sensor area

- Face: Digital camera for FIPS-201 compliant images
- Expansion: FIPS-201 compliant contactless & smart card reader
- Communications: GsM/GPRS/EDGE, 802.11b/WiFi, Bluetooth, USB
- Interface: 3.5” Color TFT LCD display at 320 x 240 resolution, daylight-readable, 40 key QWERTY keyboard, Windows CE.NET 5.0
- Ruggedization: Designed to withstand water, dust and repeated drops

4.4.10 Green Bit MiScan

Green Bit’s MiScan (originally named “WLFI”) handheld fingerprint recognition device was released for deployment in February 2010 to compete against similar devices within the mobile biometrics market; competitors include Cogent Systems’ BlueCheck, L-1’s IBIS Extreme, and Cross Match’s Be.U Mobile device. The unit is designed specifically for mobile identity applications that required remote fingerprint capture and identification capabilities such as law enforcement and border patrol / inspection points. It is an FBI certified device in regards to FBI-PIV and BSI Certified optical fingerprint reader, and designed to meet requirements and recommendations outlined within the NIST “Mobile ID Device Best Practice Recommendation”. Additionally, the MiScan follows a modular and open architecture in regards to SDK and hardware.

Technical Specifications:

- Dimensions (H” x W” x D”): 8.5 x 3.9 x 1.6
- Weight: 1.32 lbs
- Battery: 7.4V, 2400 mAh removable “snap-in” Li-Ion battery pack
- Fingerprint: 500 dpi, optical sensor, single finger, 1” x 1” active area
- Face: 2 megapixel camera with LED illuminator; color auto-focus camera
- Iris: n/a
- On-board Storage and Matching: 1:N search against on-board watch list
- Expansion: Contact and contactless card reader, 2 SD slots, 1D/2D barcode, passport MRZ reader
- Communications: 802.11b, Bluetooth, GSM/GPRS/EDGE and UMTS/HSDPA, USB 1.1
- Interface: Color LCD TFT 3.5” with touch-screen and backlight; 320 x 240 resolution, 9 keys + power on/off; WinCE 5.0; single handed operation
- Ruggedization: IP65, MIL-STD-810F

4.4.11 LaserCard LaserPASS

The LaserPASS combines optical memory technology with multi-modal biometric identification and RFID technology to provide a secure electronic identity solution. Additionally, it incorporates embedded HologramHD technology to enhance authenticity of the identification card. It also features Optical IDLock that utilizes 1:1 biometric identification and digital face image display.

4.4.12 3M Cogent Mobile Ident II

Cogent Systems’ Mobile Ident II enables authorities and officials to capture fingerprint images at 500 dpi resolution and face images of individuals remotely. The device has a color LCD touch-screen, and is tailored towards identity verification programs for military, law enforcement, and other government agencies. The device has the ability to capture fingerprint images that can then be submitted in ANSI-NIST format files to remote servers or an Automated Fingerprint Identification System (AFIS) for real-time identification. It also serves as a mag-stripe reader, and is compliant with ISO 7811 standards.

Technical Specifications:

- Dimensions (H” x W” x D”): 6 x 3.2 x 1.3
- Weight: 0.85 lbs
- Battery: Rechargeable Lithium Ion 3.7V 1100mAh
- Fingerprint: 500 ppi optical sensor, 1 finger, size: 1.19” x 0.91”

- Face: 1.3 megapixel color camera
- Iris: n/a
- On-board Storage and Matching: fingerprint and card info used for matching, picture of face only stored
- Expansion: Mag-stripe reader ISO 7811, MMC/SC card
- Communications: GPS, GPRS/ Edge GSM, IEE 802.11 b/g, Bluetooth V2.0
- Interface: Linux 2.6.14 or WinCE 6.0, 3.5 in color QVGA 320 x 240 touch screen
- Ruggedization: n/a

4.4.13 3M Cogent Mobile Ident III

Cogent Systems' Mobile Ident III is a multimodal handheld identification unit that is geared towards military, law enforcement, and government applications. As a handheld unit with wireless connectivity and communications capabilities, it can serve to capture and identify individuals in remote locations. One of its primary biometrics-based features is the ability to capture forensic quality (FBI NGI Certified) fingerprints and face images. Additionally, the unit can be customized and/or fixed with modular attachments that allow it to conduct card authentication functions such as reading magnetic stripe cards, contact and contactless smart cards.

Technical Specifications:

- Internal Storage: 300,000 fingerprint templates
- Features local fingerprint matching capability
- Features local face recognition capability
- Dimensions: 7.8" x 3.5" x 2.5"
- Weight: 1.4lbs
- Expansion Slot: 8 GB / 16 GB MicroSD option
- Fingerprint Sensor: Optical Reader
- Image Quality: 500 ppi

4.5 Multimodal (Face/Iris)

4.5.1 Iris ID iCAM H100

The iCAM H100 is Iris ID's (formerly LG Iris) handheld multimodal device designed to capture an individuals' face and iris images for on-board biometric matching. Additionally, the device can be coupled to include fingerprint and smart card read capabilities.

Technical Specifications:

- Dimensions: 6.3" x 3.6" x 1.3"
- Weight: 1.23 lbs
- Communication: USB 2.0; 802.11 b/g/n WiFi
- Embedded GPS
- Operating System: Linux
- Database: SQL Lite
- Iris Matching: Daugman Algorithm

4.5.2 Iris ID iCAM TD100

The iCAM TD100 is a handheld dual iris and face capture device. Its optical system is designed for fully automatic dual iris image capture and quality analysis, and the device's face capture API allows for the capture of ISO/ICAO formatted face images.

Technical Specifications:

- Dimensions (W x H x D): 5.9" x 3.3" x 1.2"
- Weight: 0.5lb
- Power Input: 5VDC
- Iris Capture Distance: 13"
- Face Capture Distance: 30"
- Standards: Compliant to ISO/IEC 19794-6
- Face Sensor: 1600 x 1200 MP Image Sensor

4.6 Multimodal (Face/Finger/Iris)

4.6.1 AMREL DB6-B

AMREL's DB6-B is a handheld, ruggedized multimodal device capable of capturing iris, face, and fingerprint images. Features include: dual iris capture at 30 fps, 2-megapixel face camera, -500dpi capacitive single-digit fingerprint sensor, on-board matching capabilities with a database of 100,000+ files, integrated DoD Common Access Card (CAC) reader, audio record/playback.

4.6.2 Datastrip EasyVertify

DataStrip's EasyVerify multi-biometric handheld unit adds to the company's product line of mobile devices. It is designed for remote identity verification leveraging fingerprint, face, and iris recognition technology. Additionally, the EasyVerify can be customized to read contact cards, magnetic stripes and 2D barcodes.

Technical Specifications:

- Size: 6.2" x 7.3" x 2.1"
- Weight: 2.0 lbs
- Battery Life: up to 8 hours
- Operating System: Microsoft Windows CE.NET Version 5.0
- Display: 3.7" VGA LCD (640 x 480 pixels)
- 37-key QWERTY Keypad
- 802.11b/g Wireless enabled, Bluetooth, cellular GSM
- Fingerprint Sensor: UPEK TCS1 508-dpi, 8-bit grayscale
- Fingerprint Sensor Area: 12.8mm x 18.0mm
- Face Camera: 3.2 MP, 24-bit full color
- Face Image Resolution: 2048 x 1536 (maximum)
- Iris Camera: 1.3 MP, VGA
- Iris Image Resolution: 640 x 480
- Compliant to ISO 14443A/B contactless smart cards standards
- Compliant to ISO 7816 contact smart cards standards
- 1D/2D Barcode Reader
- OCR Reader

4.6.3 MaxVision BPac

The BPac is a MaxVision developed rugged handheld computer that integrates silicon-based fingerprint recognition technology. Additionally, the device is equipped with an iris camera with infrared illuminator and face recognition technology using a 3.2MP HD video camera. As a rugged ultra mobile personal computer (UMPC), it is geared towards mobile application and operating within remote and harsh locations.

Technical Specifications:

- Capture Modalities: Flat Fingerprint, Rolled Fingerprint, Iris, Face
- Match Modalities: Flat Fingerprint, Rolled Fingerprint, Iris, Face
- Card Interface: Smart Card
- Wired Connectivity: USB 2.0, Other
- Wireless Connectivity: 802.11b, 802.11g
- Cellular Connectivity: UMTS [3G]
- Internal RAM (GB): 2
- Internal Storage (GB): 64
- Expandable Storage (GB): 256
- Operating System: Windows

- CPU Speed (GHz): 1
- Length (inches): 4.50
- Width (inches): 6.80
- Depth (inches): 2.10
- Weight (lbs): 3.45 Min Temp. (Degrees C):-32
- Max Temp. (Degrees C): 50
- FBI/NIST Mobile ID SAP: 45
- Ingress Protection (IP): 67
- Other Conformance/Compliance: MIL-STD 810G, CE, RoHS, FIPS 201
- Display Technology: LED
- Color: Yes
- Diagonal Length (inches): 5.60
- Megapixels: 3
- Technology: Optical
- Finger Types: Flat
- Conformance/Compliance: Appendix F
- Battery Life (hrs): 6.00

4.6.4 Northrop Grumman BioTRAC

The unit is designed to be a flexible, scalable, and durable platform for capture of biometric data in remote applications. BioTRAC introduces an open hardware platform that integrates multiple biometric modalities allowing for the capture of fingerprints, iris, and machine readable data. BioTRAC houses four fingerprint capture sensors, a multi-function camera with 1D and 2D barcode reading capabilities, and dual iris capture cameras. Additionally, BioTRAC can be customized to include a smart card reader, GPS unit, proximity card reader, and wireless connectivity such as 802.11 and Bluetooth technology.

Technical Specifications:

- Capture Modalities: Flat Fingerprint, Iris, Face, Voice, Other
- Match Modalities: Flat Fingerprint, Iris, Face, Voice, Other
- Card Interface: Smart Card
- Wireless Connectivity: 802.11b, 802.11g, Bluetooth
- Cellular Connectivity: UMTS [3G]
- Internal Storage (GB): 120
- Operating System: Windows
- Ingress Protection (IP): 67

4.6.5 3M Cogent Fusion

Designed for military and law enforcement personnel operating in a various environments, the Fusion handheld device provides these professionals a lightweight, wireless, multimodal biometric collection and identification device. The device is built to U.S. Department of Defense MIL-STD-810F and Ingress Protection (IP) standards. The Fusion device, 3M Cogent's latest state-of-the art handheld biometric tool, can capture and store 100,000-plus (scalable) records: forensic-quality fingerprints, latent fingerprints, iris images, photos, and textual data. Other optional capabilities include searching and matching against internally-stored biometric records; 360° latent print searching; wireless connectivity via 802.11b/g, 3G cellular radio, or Bluetooth; GPS tagging of all records collected; and the lightest weight of any device of its type on the market today—just over one pound.

Technical Specifications:

- Capture Modalities: Flat Fingerprint, Latent Fingerprint, Iris, Face
- Match Modalities: Flat Fingerprint, Latent Fingerprint, Iris, Face
- Card Interface: MicroSD

- Wired Connectivity: USB 1.1, USB 2.0
- Wireless Connectivity: 802.11b, 802.11g, Bluetooth
- Cellular Connectivity: GSM [2G], EDGE [2.5G], UMTS [3G], Other
- Expandable Storage (GB): 16
- Max Watch List Size: 100000
- Operating System: Linux
- Output Image Color: Yes
- Length (inches): 8.74
- Width (inches): 4.61
- Depth (inches): 2.91
- Weight (lbs): 1.20 FBI/NIST Mobile ID SAP: 30
- Other Conformance/Compliance:MIL-STD-810F
- Display Technology: Other
- Color: Yes
- Diagonal Length (inches): 3.50
- Megapixels: 1
- Technology: Optical
- Finger Types: Flat
- Conformance/Compliance: PIV
- Battery Life (hrs): 8.00

4.6.6 MorphoTrust HIIDE Series 4

Developed with funding from the US government, and deployed in Iraq and Afghanistan, the HIIDE (Hand-held Interagency Identity Detection Equipment) Series 4 is the world's first completely handheld system featuring multimodal finger, face and iris enrollment and matching capabilities. The HIIDE provides complete functionality while connected to a host PC or when operating in the field untethered. The HIIDE offers a USB port for connecting to peripheral devices such as passport or card readers or an external keyboard and mouse.

Technical Specifications:

- Capture Modalities: Flat Fingerprint, Iris, Face
- Match Modalities: Flat Fingerprint, Iris, Face
- Wired Connectivity: USB 2.0, LAN
- Internal RAM (GB): 256
- Expandable Storage (GB): 4
- Max Watch List Size: 22000
- CPU Speed (GHz): 533
- Output Image Length (Pixels): 640
- Output Image Width (Pixels): 480
- Output Image Color: Yes
- Output Image Resolution (DPI): 500
- Length (inches): 5.00
- Width (inches): 8.00
- Depth (inches): 3.00
- Weight (lbs): 2.00 Display Technology: LCD
- Color: Yes
- Frame Rate (FPS): 15
- Focal Distance Min (Inches): 36
- Focal Distance Max (Inches): 36
- Resolution (DPI): 500
- Frame Rate (FPS): 14

- IR Type: Dual Band
- Frame Rate (FPS): 15
- Focal Distance Min (Inches): 8
- Focal Distance Max (Inches): 10
- Battery Life (hrs): 10.00

4.6.7 MorphoTrust HIIDE Series 5

The next generation HIIDE expands onboard template capacity and communications functionality from the Series 4 version.

- Technical Specifications:
- Capture Modalities: Flat Fingerprint, Rolled Fingerprint, Iris, Face
- Match Modalities: Flat Fingerprint,
- Rolled Fingerprint, Iris, Face
- Card Interface: Smart Card
- Wireless Connectivity: 802.11b, 802.11g
- Cellular Connectivity: UMTS [3G], LTE [4G]
- Satellite Connectivity: BGAN, INMARSAT, Other
- Internal RAM (GB): 2
- Internal Storage (GB): 80
- Expandable Storage (GB): 120
- Max Watch List Size: 500000
- Operating System: Windows
- CPU Speed (GHz): 1
- Output Image Length (Pixels): 500
- Output Image Width (Pixels): 400
- Output Image Resolution (DPI): 500
- Length (inches): 8.00
- Width (inches): 3.00
- Depth (inches): 5.00 Weight (lbs): 3.25
- Min Temp. (Degrees C): 0
- Max Temp. (Degrees C): 50
- Ingress Protection (IP): 54
- Other Conformance/Compliance: MIL-STD-810F, CE, RoHS, FIPS 210
- Display Technology: LCD
- Color: Yes
- Diagonal Length (inches): 5.00
- Frame Rate (FPS): 15
- Focal Distance Min (Inches): 24
- Focal Distance Max (Inches): 48
- Megapixels: 2
- Technology: Optical
- Finger Types: Flat
- Resolution (DPI): 500
- Frame Rate (FPS): 14
- Conformance/Compliance: Appendix F
- Frame Rate (FPS): 30
- Focal Distance Min (Inches): 7
- Focal Distance Max (Inches): 10
- Battery Life (hrs): 8.00
- Charging Time (hrs): 3.00

4.6.8 CrossMatch SEEK

The SEEK (Secure Electronic Enrollment Kit) is Cross Match's multimodal mobile enrollment device that can capture an individual's fingerprint, face, and iris images. Additionally, the device is capable of automated formatting of images that conform to the Electronic Biometric Transmission Specification (EBTS) and the FBI Electronic Fingerprint Transmission Specification (EFTS) transactions.

Technical Specifications:

- Built-in Optical Fingerprint Scanner: 1.6" x 1.5"
- Built-in 1.3MP IR Camera for Iris Capture

4.6.9 CrossMatch SEEK II

The SEEK (Secure Electronic Enrollment Kit) II is Cross Match's multimodal mobile enrollment device that can capture an individual's fingerprint, face, and iris images. Additionally, the device is capable of automated formatting of images that conform to the Electronic Biometric Transmission Specification (EBTS) and the FBI Electronic Fingerprint Transmission Specification (EFTS) transactions. It is the first Mobile ID Device certified to Subject Acquisition Profile (SAP) 45 by the FBI.

Technical Specifications:

- Capture Modalities: Rolled Fingerprint, Latent Fingerprint, Iris, Face
- Wireless Connectivity: 802.11b, 802.11g, Bluetooth
- Cellular Connectivity: UMTS [3G]
- Internal RAM (GB): 2
- Internal Storage (GB): 32
- Expandable Storage (GB): 64
- Max Watch List Size: 60000
- Operating System: Windows
- Output Image Resolution (DPI): 500
- Length (inches): 8.75 Width (inches): 5.50
- Depth (inches): 3.50
- Weight (lbs): 3.60
- Min Temp. (Degrees C): 35
- Max Temp. (Degrees C): 120
- FBI/NIST Mobile ID SAP: 45
- Ingress Protection (IP): 65
- Other Conformance/Compliance: MIL-STD-810F
- Color: Yes
- Megapixels: 1
- IR Frequencies: 750nm, 850nm
- Frame Rate (FPS): 7
- Battery Life (hrs): 2.40

4.7 Components and Related Technologies

4.7.1 S.I.C. Biometrics iFMID

The iFMID is plug-in fingerprint module for the iPhone developed for USG customers. iFMID interacts with an app running on the device. When accessing a protected app, the module generates a fingerprint template and submits for matching against a remote server. the module is self-powered, and is expected to provide 2000 scans between recharges.

4.7.2 Biometric Intelligence & Identification Technologies (BI2) MORIS

The Mobile Offender Recognition & Information System (MORIS) is an iris recognition prototype developed by BI2 Technologies. It is a sleeve attachment that can be attached to the iPhone, which adds an infrared camera and viewing capability to the iPhone's built-in camera. The attachment adds approximately 1.5 ounces to the total weight of the phone, and the MORIS includes access to both IRIS and SORIS, which are products of BI2 technologies. Additionally, there are plans to design a similar attachment for Blackberry devices, and support the needs of the various law enforcement agencies. Using commercial cell services that support Internet connectivity, MORIS provides users the capability to capture an individual’s iris image, transmit information to a local or central database, and conduct remote searches onsite.

4.7.3 Black Diamond SwitchBack

The SwitchBack is an ultra-rugged customizable computer that is designed to resist harsh environmental conditions and weather conditions. It sealed to meet IEC 60529IP67 rating, and meets or exceeds the requirements of MIL-STD-810F for temperature, temperature shock, vibration, shock and humidity. Additionally, it features customizable operating systems such as Windows XP Pro, Windows Vista, or Linux, hot-swappable battery with a 2-minute swap time, and wireless connectivity and optional GPS.

Technical Specifications:

- CPU: Intel 1.0 GHz Celeron M
- Operating System: Windows XP Pro (standard); Windows Vista or Linux (optional)
- Storage: up to 120 GB
- Display: 5.6” diagonal sunlight viewable LCD with 1024 x 600 resolution
- Communications: Bluetooth 2.0; WIFI with internal 2.4 GHz antenna, civilian GPS
- Power Supply: Lithium Polymer Battery
- Dimensions (W x H x D): 7.5” x 5.5” x 2”
- Weight: 3lbs

5 Data Format and Interoperability Issues

5.1 Standardization and Interoperability

Biometric standards benefit developers, deployers, and end users in different ways.

Developer- and vendor-oriented benefits of biometric standardization include simplified development of biometrically-enabled applications and products as well as reduced risk of incompatibility with emerging systems and technologies.
Biometric vendors have been central to the development of most biometric standards; such standardization benefits certain types of technology providers more than others, and not all vendors have been active participants in the standards development process. While participation in standards development is resource-intensive, and can require compromising on matters central to one's core technology, involvement in standards development has proven important to firms (1) whose products are based on utilization of multiple sensors, devices, and/or core technologies and (2) for whom government deployers are a substantial target market. By mid-2003, most standards had gained sufficient momentum such that attempts on the part of newcomers to substantially alter their direction are unlikely to be successful.

Deployer-oriented benefits of biometric standardization include ability to hold technology providers to independent measures of compatibility, capabilities, and performance; ability to specify sets of required functions without knowledge of biometric systems operations; and (where appropriate) increased ability to exchange data with other jurisdictions and entities. In addition, standardization grants legitimacy to a technology which in many quarters is seen as highly futuristic or inherently invasive, helping to overcome objections to deployment of technologies which are too cutting-edge.
Certain deployers have played substantial roles in select standards development, such as Australia's Passports in the development of ICAO's standards for machine readable travel documents and the FBI in the development of the IAFIS standard. However, most deployers' involvement with standards is limited to incorporating compliance to certain standards within RFPs.

End User-oriented benefits of biometric standardization include increased chance of interoperability when biometric data is acquired for private or public sector deployments; increased confidence that biometric data is being stored and utilized in a fashion compliant with industry best practices; and, for end user purchasing devices for personal use, decreased costs.

While standardization is generally a welcome development, efforts to standardize biometric interfaces, data formats, and processes face numerous challenges.

Effective standards development is first complicated by the variety of biometric technologies and applications. Fingerprint, facial recognition, iris recognition, hand geometry, voice verification, and other biometrics differ substantially in their core operations as well as the characteristic used for authentication, and can be deployed in applications ranging from network security to national ID to embedded systems. It is unreasonable to expect that universal standards can be developed for every biometric technology and application; such adoption may interfere with necessary functions or simply be superfluous. In particular, access control and time and attendance applications, often implemented as standalone solutions, are only impacted by standards developments in particularly large-scale applications.

In addition, the parties playing the most active roles in the development of biometric standards very often have divergent interests. Directly competing companies, as well as government entities that seek to drive the emergence of technology in a certain direction, will often be involved in the drafting and development of standards. Certain organizations may seek to inhibit the adoption of certain standards, or may look to incorporate elements that render the standard ineffective, in order to defend strategic interests. As an example, in defining standardized methods of locating and encoding minutiae details for fingerprint

images, different companies maintain different and competing approaches, such that adoption of a particular technique may provide a competitive advantage for the technical approach adopted. While the process of consensus is designed to arrive at the best possible compromise, not all participants in the voting and validation processes are sufficiently informed to determine which approach is truly the best for the industry.

Two of the most fundamental characteristics of the biometric industry pose challenges to the long-term degree of effectiveness and acceptance of biometric standards. The first characteristic is the proprietary and secret nature of central biometric functions such as distinctive feature location, template matching, and template encoding algorithms. The second characteristic is the sensitivity to questions regarding core technology capabilities, particularly as regards matching accuracy.
In the first case, as standards are adopted, certain intellectual property elements central to biometric technology firms are lost. For example, therefore unique or differentiating approaches to feature extraction or matching may be lost in order to arrive at a common standard. This may result in either less accurate solutions or in semi-standardized solutions that retain proprietary elements to provide the highest degree of effectiveness. At the same time, companies may not be motivated to place a substantial amount of their core operations into an open standard. What results in many cases is a sub-optimal compromise: what is adopted as a standard provides a lower degree of accuracy of functionality than closed systems, and the strongest biometric solutions are not standardized.
In the second case, vendors may be hesitant to have demonstrated, in an objective setting, the accuracy of their technology as deployed (as opposed to in a theoretical or ideal matching environment). Therefore it is challenging to arrive at standards related to establishing accuracy metrics that are mutually satisfying to vendors, deployers, and other interested parties.

It is similarly notable that the general expectations regarding biometric accuracy are based on performance associated with proprietary technologies and not with standardized interoperable feature location and template generation standards. Therefore real-world performance using “generic” feature location and encoding formats – which lack the proprietary elements of a core technology thought to improve accuracy – will very likely result in less accurate biometric systems.

Standards development is a time-consuming process, particularly when advancing documents for national and international certification. This is problematic for a dynamic and emerging technology such as biometrics, where there is a risk that the industry will move faster than the pace of standardization allows. Certain applications that require expedient procurement and deployment may move too rapidly to incorporate standards at early stages, such that a migration path would need to be available to avoid deployment of a large-scale, proprietary system. The U.S. VISIT program is one such biometric effort whose aggressive timelines have set it in front of biometric standards development.
One last related issue pertains to the problem of adoption: a standard is only useful inasmuch as it is widely adopted by vendors or deployers. If standards are too cumbersome to incorporate in one’s core technology; have not gained traction among deployers; are not associated with a tangible benefit to the deployer and/or the developer; or are superseded by market developments, then they will lose much of their relevance.

These challenges notwithstanding, the benefits of standardization are such that many companies and deployers have invested substantial capital and human resources in their development and adoption.

5.2 ISO/IEC JTC1 Subcommittee 37 on Biometrics

Formed in June 2002, ISO/IEC JTC11 Subcommittee 37 on Biometrics – or SC 37 – has become the central hub for most international biometric standards efforts. SC 37 was established with the following scope:

Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.

Being an ISO-level subcommittee, SC 37 representation and voting is limited to countries as opposed to private companies or other organizations. Each country's SC 37 activities are coordinated through its national standards body; e.g. U.S. activities are coordinated through the American National Standards Institute. As of February 2008, SC 37 membership consisted of 25 Participating Members and 7 Observing Members. Many SC 37 activities are driven by delegations from the U.K., the U.S., Germany, Canada, and Korea, due to the relative maturity of these countries' national biometrics standards bodies and the presence of biometric vendors and deployers in these countries.

SC 37 is an essential standards organization as it is the primary forum for coordination, advancement, and resolution of biometric issues global in scope. Because biometrics are emerging in applications with international implications, particularly as relate to financial services, travel and transportation applications, and large-scale identification systems, it is essential that countries share a common understanding of technical, operational, and interchange issues in biometrics. Without such coordination, the ability to use biometrics to intervene for the purposes of national security will be reduced. It is important to note that the use of biometrics in criminal and forensic applications has not been strongly addressed within S 37, most likely due to the relative maturity of the use of biometric in this space.

It is also worth noting that a substantial amount of work in biometric standardization had already been undertaken within other ISO/IEC JTC1 subcommittees. The scope of SC 37 is therefore limited to areas not already directly under the purview of other subcommittees. The use of biometrics in smart cards and other documents is addressed within ISO/IEC JTC1 SC 17 Cards and Personal Identification. Biometric security, including template protection, is addressed within ISO/IEC JTC1/SC 27 Information Technology Security Techniques. These organizations, in particular SC 17, were not strongly in favor of the formation of SC 37, as it was viewed as infringing on work already being executed.

Types of Biometric Interoperability Standards

Just as the use of biometrics incorporates a range of technologies and applications, biometric standards efforts have grown to encompass various technical and non-technical elements. A helpful means of viewing categories of standards efforts is as follows.

[1] **ISO:** International Organization for Standardization; **IEC:** International Electrotechnical Commission; **JTC1:** Joint Technical Committee 1 on Information Technology

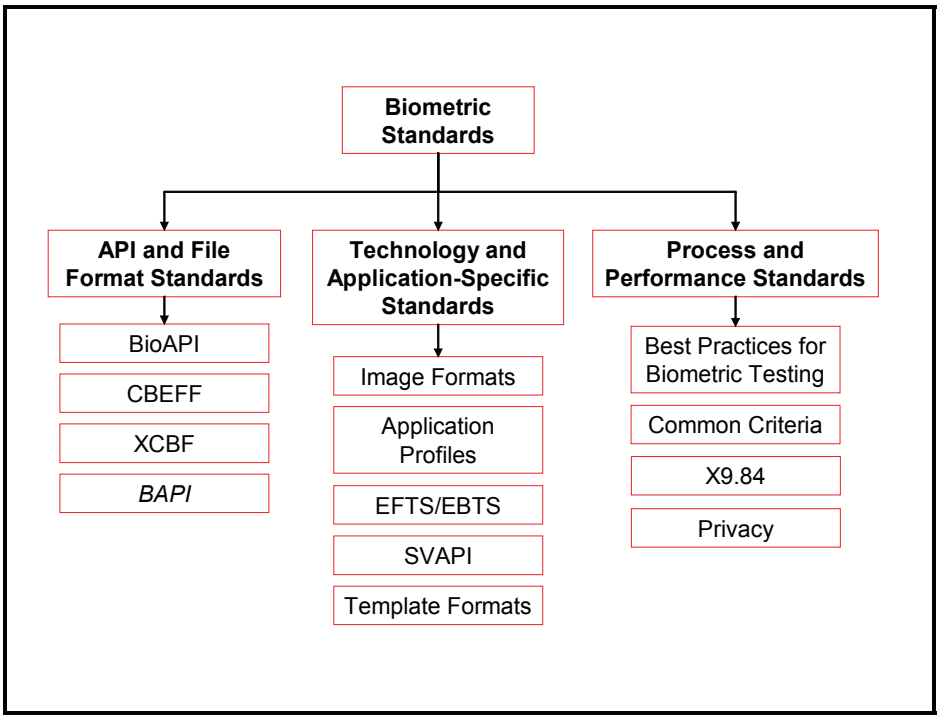

Figure 1: Types of Biometric Standards

Major categories of biometrics subject to standardization include the following:

API and File Format Standards

API and File Format Standards are generally the most well established standards efforts, providing functionality primarily of interest to biometric vendors and developers. These standards are broadly dedicated to developing technology-neutral interfaces and formats.

Application Programming Interface (API) Standards define generic protocols for communication between applications and biometric devices. BioAPI is the most widely adopted biometric API standard.

Generic File Structure and Data Format Standards define generic formats for biometric data. CBEFF (Common Biometric Exchange Format Framework) is the leading such standard, while XCBF (OASIS XML Common Biometric Format) applies specifically to biometrics and XML encoding.

Technology- and Application-Specific Standards

Technology- and Application-Specific Standards have emerged more slowly than API and file format standards, as they can impact the proprietary approaches to biometric functions held by biometric vendors and on implementations of public and private sector deployers. This category also includes highly specific standards developed for applications such as AFIS matching.

Technology-Specific Standards define formats for biometric technologies such as fingerprint and facial recognition, addressing areas such as interoperable formats for image acquisition and template structure. Technology-specific standards differ from generic formats inasmuch as the former relate to specific biometric modalities.

Application-Specific Standards define common sets of processes, functions, and normative/non-normative references for specific biometric applications.

Process and Performance Standards

Process and Performance Standards address biometric accuracy, system implementation requirements, data management, security, and policy areas. These standards are generally applicable to full biometric systems as opposed to specific system elements or interfaces.

Performance and Reporting Standards define metrics, criteria, and methodologies for evaluating biometric systems in terms of accuracy, response time, scalability, and availability.

Biometric Data Management Standards define generic protocols for transmission of biometric data. X9.84 Biometric Information Management and Security for the Financial Services Industry is the leading such standard. These standards are closely related to API and file format standards, but are categorized as process and performance standards as they incorporate discussions of preferred system architecture and matching accuracy capabilities in addition to their reference implementation.

Common Criteria is a specific type of standard, applicable to information technology security that defines the levels of security assurance associated with biometric systems and subsystems.

Privacy standards relate to collection, use, and retention of data in biometric systems.

The range of biometric technology aspects undergoing standardization has resulted in numerous complex interrelations and interdependencies between standards efforts. While certain standards efforts have grown directly from earlier efforts, others are *sui generis*, and do not necessarily build on preceding efforts. To date there is no official "suite" of standards that apply in equal measure to all deployments. However, BioAPI and CBEFF have gained enough momentum to have become widely cited in public sector procurements of biometric technology.

5.3 Technology-Specific Standards

Technology-specific standards reduce or eliminate reliance on a single supplier of imaging technology or matching algorithms; this in turn should provide migration paths to improved technologies for developers and deployers. The development of these standards is inconsistent with the interests of many hardware and algorithm developers, but is essential to ensuring that biometrics, as a whole are adopted widely. Technology-specific standards include template and image standards.

Image standards define minimum requirements for acquisition and compression of identifiable biometric images, such as fingerprints, facial images, and iris images, for use by different biometric systems. Image standards represent a basic approach to interoperability within a given technology. By mandating the size, resolution, orientation, offset, cropping, and other factors involved in image acquisition, it is possible to utilize a single biometric image – such as a fingerprint – across multiple systems. This ensures that so long as standards-compliant cameras and scanners are utilized, and the image meets quality requirements (if applicable), a stored image can be used for enrollment and verification across multiple systems. Image standards do not eliminate the need for regeneration of enrollment templates in a given system, but they do ensure that identifiable datasets can be used across multiple systems, eliminating the need to reenroll users.

Because different vendors optimize their technologies for use of specific image types, in many cases tied to a specific scanner, it can be difficult to drive consensus on what is minimally acceptable. In addition, substantial testing will be required to measure the degree of deterioration in performance when generic images are used. Format standards for data interchange have been developed within M1 for fingerprints, finger pattern spectral data, iris images, facial images, signature time series data, hand geometry silhouettes, and vascular biometric images. Format standards for interchange are currently under development within M1 for finger pattern skeletal data, signature processed dynamic data, face identity data, voice data and DNA data. Substantial work has already been conducted in fingerprint systems due to their use in forensic applications; facial image specifications are drawing on work conducted by ICAO for use in international travel documentation. Facial images are relatively unproblematic compared to

fingerprint or iris, as face matching algorithms are already designed to incorporate inputs from varying types of media and devices. Fingerprint and iris systems are more likely to be tied to a specific imaging platform.

Template standards represent a much greater challenge to the sovereignty of biometric solution providers than image standards. However, template standards are seen as a holy grail for biometrics, as the development of mature template standards would ensure that any biometric enrollment could be verified on any other biometric system based on the same behavioral or physiological characteristic.

In order to define template standards, it is necessary to gain consensus on what features or elements of the characteristic in question are necessary to effectively encode and enrollment template and perform matching. It is then necessary to gain consensus on the best way of encoding these features such that subsequent presentation of biometric data can be reconciled with the enrollment. Different vendors not only locate different types of features, but they encode and measure features' interrelations differently. Therefore a large percentage of what differentiates biometric software providers is subsumed to common functionality within template standards.

One approach to mitigate the negative impact of the loss of vendor discretion is to incorporate both a generic interoperable template and a vendor-specific template within a single biometric record. In this fashion a biometric match can utilize the native template format when it is available and revert to the generic interoperable template when using a specific device or system.

The tension involved in developing template standards is likely to continue for the foreseeable future. The firms best qualified to determine whether a given standard will be effective or deployable are the same firms with a vested interest in a core technology. As companies begin to migrate away from a focus on proprietary approaches, and seek revenues in other areas of biometrics, this should become less of an issue.

5.3.1 Fingerprint Standards

- INCITS 377: Information Technology - Finger Pattern-Based Format for Data Interchange (Approved as U.S. standard)
- ISO/IEC 19794-2:2005 Biometric Data Interchange Formats - Part 2: Finger Minutiae Data (Approved as international standard)
- INCITS 378: Information Technology - Finger Minutiae Format for Data Interchange (Approved as U.S. standard)
- ISO/IEC 19794-3:2006 Biometric Data Interchange Formats - Part 3: Finger Pattern Spectral Data (Approved as international standard)
- INCITS 381: Information Technology - Finger Image Format for Data Interchange (Approved as U.S. standard)
- ISO/IEC 19794-4:2005 Biometric Data Interchange Formats - Part 4: Finger Image Data (Approved as international standard)
- ISO/IEC DTR 29794-4, Biometric Sample Quality – Part 4: Finger image data (Current Status – DTR)

INCITS 377 and INCITS 378 represent different and non-compatible approaches to fingerprint matching.

INCITS 377 is optimized for use with low-resolution, small fingerprint sensors – particularly silicon sensors – often used in commercial or consumer applications, while the latter is designed for use with high-resolution, large fingerprint sensors, often particularly optical sensors. INCITS 377 represents the newer of the two approaches to fingerprint matching, based on "finger pattern cell" information as opposed to minutia points. A portion of the fingerprint image is divided into a grid of square cells. Within each of these cells, a small number of ridges will be present. For each cell, three parameters are calculated: ridge angle, ridge spacing, and phase offset (the distance between the lowermost ridge and the

cell border). Hundreds of cells are thus overlaid against a finger image, deriving the three aforementioned characteristics from the capture range.

Notable aspects of the standard include the following:

- *Cropping of source images to generate a small image from which patterns are derived.* Cropping allows images larger sensors to be used for matching, although there is risk that valuable data will be lost in the cropping process.
- *Specifies a minimum ppi (points per inch) of 200, as opposed to the traditionally-required 500dpi.* The specification of a 200ppi minimum resolution represents a major break with preceding fingerprint technologies, which nearly all require higher resolution to function.
- *Reference to X9.84 and Common Criteria for confidentiality of biometric data.* The standard recommends, but does not require, usage of X9.84 or Common Criteria to safeguard biometric data.

Although there is no explicit reference in the standard, INCITS 377 closely resembles Bioscrypt's proprietary pattern-matching technology. Bioscrypt leverages standards compliance as a method of differentiating itself from competitors, and as such has positioned key personnel in the standards development community to ensure that its positions are fully represented as standards are proposed, developed, and approved.

INCITS 378 leverages the traditional approach to fingerprint matching, based on the position, type, angle, and quality of minutia points present on fingerprints. Minutiae matching is the method by which fingerprints have been manually matched for decades, and is the approach that provides a "scientific" basis for the admissibility of fingerprints in legal proceedings. Standardization of this approach is simplified by preceding minutiae interoperability standards, but at the same time is complicated by the existence of numerous mature, proprietary methods of encoding and matching minutiae data in the marketplace.

Notable aspects of the standard include the following:

Open-ended approach to capture equipment standards. The only standard for fingerprint acquisition devices is Appendix F (IAFIS Image Quality Specification), which is more applicable to criminal than civil or commercial applications. 378 references Appendix F as one potential type of capture device, but also reserves space for future standards that define device performance criteria.

Focus on ridge endings and bifurcations. Most minutiae can be classified as either ridge endings or bifurcations (the point where ridges split). However there are several complex types of minutiae points that are neither ridge endings nor bifurcations. Many vendors utilize proprietary approaches to classifying and utilizing this data; the standard deals with this problem by classifying all such minutiae as "other" and allowing vendors to define the manner in which such points are defined.

INCITS 378 differs from preceding approaches in its integration with CBEFF, as alluded to above, as well as in slight changes in the way that minutiae data is encoded.

The pattern-based and minutiae-based formats for data interchange share certain common elements, including normative references to following previously-published standards:

ANSI/INCITS 358-2002, Information technology - BioAPI Specification. This standard provides a common interface and set of functions for application developers, and reduced the need to re-engineer applications as new devices and algorithms are introduced.

ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, and Scar mark and Tattoo (SMT) Information. This standard, which has since been updated to ANSI/NIST-ITL 1-2007, provides a basis for analysis and specification of fingerprint image and minutiae data.

NISTIR 6529-A-2003, Common Biometric Exchange Framework Format (CBEFF). This standard provides formats for placing biometric data into a commonly recognizable structure. CBEFF makes

accommodations for device types and algorithm versions, such that a system can process received biometric data properly.

Each standard makes accommodations for an "extended data area" that allows vendors to place additional information above and beyond standard-compliant data. In this fashion a vendor could provide a single data record that contains interoperable and proprietary data, an approach that allows vendors to balance interoperability and performance. As INCITS 378 states.

While the extended data area allows for inclusion of proprietary data within the minutiae format, this is not intended to allow for alternate representations of data that can be represented in open manner as defined in this standard.

Each standard allows for multiple fingerprints to be embedded in a single record, along with multiple "views" of each fingerprint. Each standard also makes accommodations for quality measurement, although there is as yet no standard approach to measuring quality fingerprint quality.

INCITS 377 and INCITS 378 have been advanced for consideration at the ISO/IEC level, which would improve the likelihood of large-scale interoperability on terms favorable to the parties involved in development of the standard to date. The pattern standard, whose ISO/IEC implementation is identical to INCITS 377, has met with substantial resistance from influential national bodies such as the U.K. Objections are based on the position that pattern matching approach is not sufficiently proven, either from a theoretical perspective or in the marketplace, to have been standardized, and also that alternative pattern-based approaches may be unable to comply with the standard. Granting that other approaches to pattern matching may emerge that do not utilize the cellular approach that INCITS 377 standardized, the SC37 WG3 renamed the standard to Biometric Data Interchange Formats – Part 3: Finger Pattern Spectral Data. This allows for other pattern-based standards such as ISO/IEC 19794-8 Biometric Data Interchange Formats – Part 8: Finger Pattern Skeletal Data, which is currently being developed.

INCITS 381 specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data, based on the content, format, and units of measurement for such information. The standard differs from previous fingerprint image standards in that it allows for much lower resolution images. The normal baseline for fingerprint images is 500ppi and 8-bit greyscale; INCITS 381 defines additional "Setting Levels" that allow for 125, 250, 500, and 1000 ppi, with pixel depth ranging from 1 to 8 bits. The intent of this variation in image quality is to allow for data interchange between applications or jurisdictions in which lower-resolution data has been acquired, as could be the case in non-forensic applications. The intent is that a record header would contain information such as image acquisition level, scan and image resolution (horizontal and vertical), and pixel depth, indicating to the recipient whether such data could be used for interchange purposes. Compliance with INCITS 381 requires that finger image data be implemented in a CBEFF-compliant structure. The ISO/IEC version of this standard, 19794-4 Biometric Data Interchange Formats: Part 4: Finger Image Data, maps almost directly to the INCITS version of the standard, with slight editorial modifications.

The document – ISO/IEC 29794-4 – specifies the terms and definitions that can be used in the specification, use, and testing of finger image quality metrics. Additionally, it defines the interpretation of finger image quality scores, and identifies finger image corpora for the purpose of serving as information for algorithm developers and users. Lastly, the document develops statistical methodologies targeted to finger image corporate for characterizing quality metrics, which can be used to interpret matching scores and their performance.

5.3.2 Iris Image Standards

INCITS 379: Iris Image Interchange Format (Approved as U.S. standard)

ISO/IEC 19794-6:2005 Biometric Data Interchange Formats - Part 6: Iris Image Data (Approved as international standard)

ISO/IEC 29109-6, Conformance testing methodology for biometric interchange records format – Part 6: Iris image data (Current Status – CD)

ISO/IEC 29794-6 – Biometric Sample Quality, Part 6 – Iris Image (Current Status - WD)

INCITS 379 defines two alternative formats for iris image interchange: a Cartesian/rectilinear coordinate format and a polar coordinate format. These formats are based on the technologies of the primary iris recognition developer, L1 (polar), and its Korean competitor, IriTech (rectilinear). The rectilinear format allows for compressed or uncompressed, as well as monochrome or color, iris images, and as such can require over 20kb of storage per image. The rectilinear format further defines methods for pre-processing iris images captured in dual-eye format. The polar format, which mirrors L1's approach to iris recognition, pre-processes rectilinear data such that the record requires less space (approximately 2 bytes). The polar image interchange format also makes provision to eliminate iris occlusions.

A non-normative Annex to the standard defines iris image capture best practices, and incorporates substantial guidance in the areas of grayscale density, illumination, contrast, visibility, aspect ration, scale, noise, distortion, and orientation. The Annex also defines interesting "image quality levels" associated with applications of differing security, pictured below. It will be interesting to consider the impact of differing iris diameters and resolutions on enrollment and accuracy rates.

The ISO/IEC version of this standard, 19794-6 Biometric Data Interchange Formats – Part 6: Iris Image Data, maps almost directly to the INCITS version of the standard, with slight editorial modifications. One interesting security-related objection, which resulted in the only "no" vote on the international ballot, came from the UK delegation, which holds that an iris data record must always have a capture device ID reported (or else there is no certainty regarding the origin of the data). The standard currently allows for a zero-entry in this field.

ISO/IEC 29109-6 – specifies the elements of conformance testing methodology, test assertions, and test procedures that can be applied to biometric data interchange format standard for iris images. Referencing ISO/IEC 19794, the document specifies that the testing methodology dictated in Clauses 6, 7, and 8 of ISO/IEC 29109-1 shall be applied. This includes all respective values for the requirement identifier number, level, and sub format applicability.

ISO/IEC 29794-6 – defines the terms and quantitative methodologies that are relevant to the characterization and assessment of the match-ability of iris images. It references standards ISO/IEC 19784-1 and ISO/IEC 19785-1 standards that allocate a quality field and score range that can be applied to iris images with a qualitative foundation. For ISO/IEC 29794-6, the standard establishes useful terms and definitions that can be used to specify, characterize and evaluate iris image quality, methods for assessing iris image quality, and the normative requirements of software and hardware producing iris images. Additionally, the standard establishes the normative requirements of software and hardware required to measure the utility of iris images including the requirements on covariates affecting iris recognition performance.

5.3.3 Facial Image Standards

- INCITS 385 Face Recognition Format for Data Interchange (Approved as U.S. standard)
- ISO/IEC 19794-5:2005 Biometric Data Interchange Formats - Part 5: Face Image Data (Approved as international standard)
- ISO/IEC FCD 29109-5, Conformance testing methodology for biometric interchange format records – Part 5: face image data (Current Status – FCD)
- ISO/IEC DTR 29794-5, Biometric Sample Quality – Part 5: Face image data (Current Status – DTR)

INCITS 385 provides a comprehensive approach to face recognition data interchange, encompassing specifications for different types of facial images based on the amount of face data available and the intended usage(s) of the face data. Interchange within manual, operator-based identity verification is

within the scope of the standard, in addition automated biometric identification. Functional requirements in the standard are:

- A format shall be specified with sufficient resolution to allow a human examiner to ascertain small features such as moles and scars that might be used to verify identity.
- Photographic (environment, subject pose, focus, etc.) properties of the face shall be specified for optimal one-to-many search identification using face recognition algorithms
- A face format shall be provided to satisfy requirements of a small storage footprint that can be used for both human and computer verification.
- The records shall be in a common format that can be used with non-proprietary data readers and image display programs.
- The records shall be interoperable by allowing different face recognition algorithms to undertake matching on the supplied electronic facial data.

The third and fifth of these elements are of primary interest, alluding to token-based storage and algorithm interoperability, respectively.

Four facial image types are specified in the standard:

Basic. Specifies only header and image data formats, does not address photographic or resolution requirements. The basic face record incorporates the following:

- *Facial header block*, including format identifier, version number, record length, number of facial images
- *Facial information block*, including block length, number of feature points, gender, eye color, hair color, feature mask (e.g. Glasses, beard), expression, and pose angle
- *Image information block,* including facial image type, image type (jpeg/jpeg2000), height, image color space, source type, device type, and quality

The basic image type also offers an optional "facial feature block" that specifies the type and position (in the image) facial features such as eye position, nose and nostrils, mouth. Based on the MPEG4 feature point set, this could represent a rudimentary feature-level interchange specification.

Frontal. The frontal image type incorporates all basic requirements as well as normative requirements in the following areas:

- *Scene requirements,* including purpose*,* pose *(*<+/- 5 degrees up/down, rotated left/right, and tilted left/right), and expression
- *Photographic requirements,* including exposure, focus and depth of field*,* unnatural color*,* color or grayscale enhancement*,* and radial distortion
- *Digital requirements,* including geometry and color profile

Full Frontal. The full frontal image type is based on acquisition of the entire head and the outline of the shoulders. In addition to all basic and frontal requirements, the image type incorporates normative requirements (some influenced by (AAMVA DL/ID2000) in the following areas:

- *Photographic requirements,* including centering, position of eyes (50%-70% from bottom of image), head width (minimum 4:7 relative to image width), and head length (<80% crown to chin)
- *Digital Requirements,* including resolution (180 pixels head width, 90 pixels eye to eye).

Token Face Image. The token image type incorporates the basic and frontal specifications, but is optimized for applications in which storage requirements are at a premium. The digital-only image type situates the eyes at specific points in the image for ease of use in automated facial recognition applications. Instead of requiring 90 pixels between the eyes, the token standard requires 60 pixels. The left and right eyes are placed at specific X, Y coordinates based on a 320x240 image space.

The ISO/IEC version of this standard, 19794-5 Biometric Data Interchange Formats – Part 5: Face Image Data, maps almost directly to the INCITS version of the standard, with slight editorial modifications.

ISO/IEC 29109-5 establishes the test assertions for the structure of the face image data format, which has been specified in ISO/IEC 19794-5:2005. Additionally, it asserts the internal consistency by checking the types of values that may be contained within each field.

ISO/IEC 29794-5 defines and specifies methodologies for quantitatively assessing the quality scores for facial images. Additionally, the document defines the purpose, intent, and interpretation of face quality scores. It references ISO/IEC 19794 Part 5: Biometric data interchange formats to define some facial specifications such as scene constraints, photographic properties of facial images, and digital image attributes of facial images. Though Face Image Quality can be defined in multiple ways, this standard defines it in relation to the use of facial images with automated face recognition systems with respect to the amount of defect or the degree of imperfection present in the face image.

Standard	Parent	Function	Status
SC 37 – Biometrics	Joint Technical Committee 1 (JTC1) under ISO	Global committee dedicated to standardization of biometric technologies to support interoperability and data interchange among applications and systems, including file formats; application programming interfaces; biometric templates; related profiles; methodologies for conformity assessment.	[See working groups below]
SC 37 Working Group (WG) 1 - Vocabulary	SC 37	SC 37 Working Group dedicated to a shared set of terms and definitions	
SC 37 WG 2 - Biometric Technical Interfaces	SC 37	SC 37 Working Group dedicated to developing global standards for interface-level issues such as APIs and format headers (BioAPI and CBEFF)	Developing amendments and conformance testing standards for BioAPI and additional parts to CBEFF
SC 37 WG 3 - Data Interchange Formats	SC 37	SC 37 Working Group dedicated to template and image formats standard development	Developing interchange formats for various emerging modalities; developing conformance testing methodology for data interchange records; developing biometric sample quality standards
SC 37 WG 4 - Application Profiles	SC 37	SC 37 Working Group dedicated to defining application profiles for border crossing, transportation workers, access control, etc.	Application profiles being developed for access control for airport employees, and verification and identification of seafarers; overview standard for biometric systems and profiles approved
SC 37 WG 5 - Performance and Testing	SC 37	SC 37 Working Group in which all matters related to performance testing – including test size, methods, confidence intervals, best practices, and reporting metrics – are defined and standardized	Developing standards for interoperability performance testing, access control systems and methodologies for operational evaluation

Standard	Parent	Function	Status
SC 37 WG 6 - Cross Jurisdictional and Societal Aspects	SC 37	SC 37 Working Group dedicated to national and regional issues such as privacy, perception, regional biases and preconceptions	Developing standards for jurisdictional and societal considerations for commercial applications, and pictograms, icons and symbols for use with biometric systems
ICAO 9303: Machine Readable Travel Documents	ICAO	Document deals generally with machine readable passports and visas; a section is dedicated to using biometrics with these documents	9303 a mature standard; ISO/IEC 7501 version being revised
X9.84	X9	X9.84 describes the controls and proper procedures for using biometrics as an identification and authentication mechanism for secure remote electronic access, or for local physical access control for the financial services industry	Published as American National Standard X9.84-2003 Biometric Information
Common Criteria	ISO/IEC JTC1/SC27 IT Security Techniques	Common Criteria (CC) – ISO standard 15408 – provides a common set of security functional and assurance requirements for IT security evaluations performed in different countries; based on European (ITSEC), U.S. (TCSEC - Orange Book) and Canadian (CTCPEC) evaluation criteria; results of IT security evaluations made comparable and meaningful to a wider audience.	CC is a mature standard; biometric CC evaluations an emerging area
ANSI B10.8	AAMVA	Provides a standardized method of locating and encoding fingerprint minutia for use in DL applications	Published as ANSI/NCITS/B10.8/99-001; folded into M1

Table 4: Biometric Standards and Standards Bodies Overview

6 Legal, Ethical, Cultural, and Privacy Aspects of Mobile Biometrics

6.1 Introduction: Privacy

Privacy may be a central concern of citizens or non-citizens to provide biometric samples to a mobile biometric device, particularly those who view fingerprinting as being synonymous with criminal processes. In addition, citizens may have concerns as to potential misuse of biometric data used for identity verification. It is critical that technology deployers take steps to ensure that reasonable privacy expectations are met in order to address potential resistance to use of biometrics in mobile identification applications.

There are two general categories of privacy risks posed by biometric systems: personal privacy and informational privacy. Personal privacy relates to privacy of the person, the infringement of which relates to coercion or physical or emotional discomfort when interacting with a biometric system. Informational privacy relates to the misuse of biometric data or of data associated with biometric identifiers.

6.1.1 Personal Privacy

Personal privacy impacts individuals who find the use of biometrics offensive or invasive. The percentage of the population for whom the use of biometrics is inherently problematic varies according to external factors; objections to the technology fell after 9/11/01, and can rise under other circumstances. For example, individuals may have cultural objections to being photographed, or may object to fingerprinting for religious or personal reasons. The percentage of people whose resistance to biometric systems is so strong as to increase the likelihood of non-compliance is unknown. Fears and concerns relating to privacy of the person are difficult to address through legislation or system design. Until the public at large is more familiar with biometrics, individuals objecting to the use of biometrics on the grounds of personal privacy are an inevitable component of most any biometric deployment.

6.1.2 Informational Privacy

Informational privacy is the ability to maintain control over the use and dissemination of one's personal information. It involves concepts of freedom of choice, personal control, and informational self-determination. It is well understood that threats to privacy relate to the ability of third parties to access biometric information in identifiable form and link it to other sources of information, resulting in secondary uses of the information without the consent of the data subject. Personal control of an individual over the uses of her/his information is the cornerstone of the Canadian approach to information privacy. Fears and concerns classified under informational privacy are not expressions of inherent discomfort with biometrics, but are centered on the impact of the unauthorized collection, use, retention, and disclosure of biometric data. Informational privacy is rooted in the concept that individuals have a right to control the usage of their personal information. The "Big Brother" fear of government tracking and monitoring of individuals, and of databases being used to aggregate information regarding individuals without their knowledge or consent, is one expression of fears related to informational privacy.

The fears categorized as informational privacy represent various types of *function creep*, or the expansion of a program, system or technology into areas for which it was not originally intended. The following are the primary categories of informational privacy concerns:

- *Unauthorized collection* of biometric data is a primary informational privacy concern. This is unlikely to be an issue in most mobile identification applications, as individuals are directly interacting with biometric systems. The voluntary or coercive nature of collections will impact privacy.
- *Unauthorized use* of biometric data is seen as the most severe risk biometrics pose to privacy in most applications. In this situation, it is not the *intended* uses of biometrics that are seen as problematic, but

the ways in which such data might be used for purposes broader than those originally intended. The unauthorized use of biometrics to monitor, link and track a person's activities is a commonly held fear, especially if collections occur in an environment not previously associated with strong identity verification.

- *Unauthorized retention* of biometric data, in which biometric information is stored longer than necessary, is a central concern in various biometric systems. Program requirements will likely dictate that biometric data collected be retained for a period of years. However, so long as such retention is disclosed and, by extension, authorized, the privacy impact is reduced.
- *Unauthorized disclosure* of biometric information to other public agencies or to private sector institutions undermines an individual's ability to consent to the type of data usage with which he or she is comfortable. Unauthorized disclosure increases the likelihood that biometric data will be used for purposes beyond which it was originally acquired. Disclosure of biometric data to related government agencies may become common practice, but so long as the guidelines governing such disclosure are made clear prior to data collection (and such disclosure is not arbitrary), then the system's privacy impact can be assessed from the start of operations. For mobile devices, wireless communications from un-controlled locations introduce significant security concerns related to disclosure of biometric and personal information.

6.2 Templates, Identifiable Images, and Unique Identifiers

A distinction should be drawn between the privacy impact of biometric templates and that of identifiable biometric images. Biometric templates are files derived from the unique features of a biometric sample. The template contains an extremely distinctive subset of information, but utilizes only a fraction of the information found in an identifiable biometric image such as a face image. Biometric vendors' templates are proprietary and not interoperable. Biometric systems use templates and matching algorithms to perform 1:1 and 1:N functions.

Identifiable biometric images are viewed as more problematic from a privacy perspective than templates. A biometric image, if intercepted, compromised, or copied, could be used to enroll individuals in other systems without their consent, could be used to perform 1:N searches in some circumstances, or could be used to link data from databases where the biometric resides.

The compromise of a template, though not desirable, would be less problematic. Templates cannot be reverse-engineered to render the original image because of the relative scarcity of data. Only a partial set of data exists in a template from which one could try to rebuild an identifiable image, and templates are not recognizable as biometric samples.

A major privacy fear related to misuse of biometric data is usage of biometrics as unique identifiers. A unique biometric identifier could facilitate tracking across various public and private sector databases. However, inherent characteristics of biometric templates limit the ability of biometric systems to use templates as unique identifiers. Biometric samples acquired at different times, even from sequential frames of a CCTV recording or biometric reader, generate different numerical templates. As templates change from transaction to transaction, the ability to track an individual from database to database is reduced. In order for an individual to be tracked across databases by means of a biometric, his or her identifier cannot vary.

6.3 Biometric Technology Relation to Privacy

Depending on how a biometric system is used and what protections are in place to prevent its misuse, a biometric system can be categorized in four different ways: privacy-protective, privacy-sympathetic, privacy-neutral, or privacy-invasive.

- Privacy-Protective. A privacy-protective biometric system is one is which biometric data is used to protect or limit access to personal information, or in which biometrics provide a means of an individual establishing a trusted identity.
- Privacy-Sympathetic. A privacy-sympathetic biometric system is one in which protections are established and enforced which limit access to and usage of biometric data, and in which decisions regarding design issues such as storage and transmission of biometric data are driven by privacy concerns.
- Privacy-Neutral. A privacy-neutral biometric system is one in which privacy simply is not an issue, or in which the potential privacy impact is very slight. Time and attendance systems, for example, are often seen as privacy-neutral. These are generally closed systems in which data never leaves the biometric device. These types of systems would be very difficult to misuse under any circumstance, and are not meant to enhance privacy but to deter fraud.
- Privacy-Invasive. A privacy-invasive biometric system is one used in a fashion inconsistent with generally accepted privacy principles. Privacy-invasive systems would include those that use data for purposes broader than originally intended, those that facilitate linkage of personal information without an individual's consent, and those within which biometric data is subject to compromise.

6.4 BioPrivacy Assessment: Mobile Biometric Devices

IBG has developed a privacy risk evaluation methodology known as the BioPrivacy Initiative[2]. This initiative establishes criteria for evaluating the potential privacy impact of biometric deployments and technology, and provides guidance in the form of best practices for biometric deployment. The methodology has three components:

1. Impact Framework, an application risk assessment
2. Technology Risk Ratings, a technology risk assessment
3. Best Practices, guidelines for privacy-sympathetic deployment

[2] See www.bioprovacy.org.

6.4.1 Mobile Biometrics Applications: Impact Framework

The BioPrivacy Impact Framework is comprised of ten categories which map closely to the privacy principles outlined in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

Category	Brief Description
Overt vs. Covert	Deployments in which users are aware that biometric data is being collected and used, and acquisition devices are in plain view, are less privacy-invasive than surreptitious deployments.
Opt-In vs. Mandatory	A biometric system in which enrollment is mandated, such as a public sector program or one designed to encompass a company's employees, bears a more direct relationship to privacy risks than an opt-in system. Mandatory systems come under more suspicion as they are imposed on a user as opposed to being selected by the user.
Verification vs. Identification	A system capable of performing 1:N searches can be considered more susceptible to privacy-related abuse than a 1:1 system, as individuals' records can be identified based solely on a biometric sample.
Fixed Duration vs. Indefinite Duration	The use of biometrics for a fixed duration is less likely to have a negative impact on privacy than one deployed indefinitely. When deployed for an indefinite duration, the risk of function creep increases.
Public vs. Private Sector	Public sector biometric usage can be seen as more risky than private sector due to the possibility of state or government abuse. Government collection of biometric data without proper controls and restrictions can be problematic. On the other hand, private sector companies may be more tempted to share or link personal data for marketing or profiling purposes.
Individual, Customer, Employee, Citizen	An individual's roles vary according to the people and institutions with whom they interact. A person is a citizen (or resident) in their dealings with the government or state, an employee in their dealings with an employer, a customer when party to certain types of a commercial transaction (credit issuance, for example), and a great variety of environments is an anonymous individual. Reasonable expectations of privacy are dependent on the capacity in which a person is interacting with another person or an institution.
User Ownership vs. Institutional Ownership of Biometric Data	Deployments in which the user maintains ownership over his or her biometric information are more likely to by privacy-sympathetic than those in which the public or private institution owns the data.
Personal Storage vs. Template Database	A biometric system that stores information centrally is more capable of being abused than one in which biometric information is stored on a user's PC or on a portable token (e.g. a smart card).
Behavioral vs. Physiological Biometric	Behavioral biometrics are less likely to be deployed in a privacy-invasive fashion than physiological biometrics, as technologies such as voice and signature recognition can be changed by altering a signature or using a new passphrase. Physiological biometrics are harder to mask

	or alter, and some can be collected without user compliance.
Template vs. Identifiable Data	Biometric templates, as they cannot be identified as biometric data without matching algorithms, bear fewer privacy risks than identifiable biometric data (such as fingerprints or face images).

Table 5: Mobile Biometrics Applications: Impact Framework

Assessing Mobile Identification Applications through the BioPrivacy Impact Framework illustrates the areas where greater risks are involved, such that appropriate precautions and protections can be enabled.

6.4.2 Technology Risk Ratings

Certain biometric technologies are more likely to be deployed in a privacy-invasive fashion than others. The BioPrivacy Technology Risk Ratings assess biometric technologies (e.g. fingerprint, face, iris) according to their potential for privacy-related misuse. Categories of technology-specific risk assessment are as follows:

- **Verification / Identification.** Technologies that are most capable of robust identification are more capable of privacy-invasive use; technologies that are only capable of verification are less capable of privacy-invasive use.
- **Overt / Covert.** Technologies that are capable of operating without user knowledge or consent are rated higher; technologies that only operate with user consent are rated lower.
- **Behavioral / Physiological.** Technologies that are based on unchanging physiological characteristics are rated higher; technologies that are based on variable behavioral characteristics are rated lower.
- **Give / Grab.** Technologies in which the system acquires ("grabs") user images without the user initiating a sequence are rated higher; technologies in which the user "gives" biometric data are rated lower.

Fingerprint and face recognition technology, commonly used in mobile biometric applications, are rated the most likely to be used in a privacy-invasive fashion. Fingerprint technology rates poorly due to its potential compatibility with existing databases as well as its ability to be used for 1:N searches. Face recognition rates poorly due to its ability to be acquired without user consent or compliance, as well as its ability to facilitate some types of 1:N identification. Iris recognition, the other technology suitable for use in mobile applications, is rated medium risk: its ability to facilitate 1:N searches is a negative, but the difficulty of acquisition as well as the lack of existing databases reduced the risk to some degree.

6.4.3 Best Practices Adherence

The following section presents a framework for evaluating biometric applications in terms of compliance with BioPrivacy Best Practices. BioPrivacy Best Practices are guidelines for privacy-sympathetic and privacy-protective deployment, assessing potential program compliance with the types of protections and limitations commonly implemented.

Few if any deployments can be compliant with all Best Practices; non-compliance with one or more Best Practices does not necessarily result in a privacy-invasive deployment. If a certain deployment cannot comply, for example, with Best Practices relating to *Scope and Capabilities*, that deployment may be capable of complying with Best Practices relating to *Disclosure, Auditing and Accountability* in order to counterbalance this lack of compliance.

These Best Practices provide a wide range of checks and balances against potential privacy-invasive usage, and it is strongly recommended that border security applications comply with the Best Practices so marked under “Ability to Comply”.

6.4.4 BioPrivacy Best Practices: Scope and Capabilities

Best Practice	Description	Ability to Comply
Scope Limitation	Biometric deployments should not be expanded to perform broader verification or identification-related functions than originally intended. Any expansion or retraction of scope should be accompanied by full and public disclosure, under the oversight of an independent auditing body, allowing individuals to opt-out of system usage if possible.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Establishment of a Universal Unique Identifier	Biometric information should not be used as a universal unique identifier, and sufficient protections should be in place to ensure to the degree possible that biometric information cannot under any circumstances be used as a universal unique identifier.	Watch list: N Identification: N Eligibility: Y Identity Verification: Y
Storage of Biometric Information	Biometric information should only be stored for the specific purpose of usage in a biometric system, and should not be stored any longer than necessary. Biometric information should be destroyed, deleted, or otherwise rendered useless when the system is no longer operational; specific user information should be destroyed, deleted, or otherwise rendered useless when the user is no longer expected to interact with the system.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Potential System Capabilities	When determining the risks a specific system might pose to privacy, the system's potential capabilities should be assessed in addition to risks involved in its intended usage. Systems may have latent capabilities, such as the ability to perform 1:N searches or to be used with existing databases of biometric information, which could have an impact on privacy.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Collection and Storage of Extraneous Information	Non-biometric information collected for use in a biometric system should be limited to the minimum necessary to make identification or verification possible.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y

Storage of Original Biometric Data	Biometric data in an identifiable state, such as a face image, fingerprint, or vocal recording, should not be stored or used in a biometric system other than for the initial purposes of generating a template.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y

Table 6: BioPrivacy Best Practices – Scope and Capabilities

6.4.5 BioPrivacy Best Practices: Data Protection

Best Practices related to protection of biometric data, and protection of the data resulting from biometric matches, are critical privacy-protective elements. The compromise of biometric data, even though it may not entail any actual risk, would be perceived as a major threat to privacy and would undermine confidence in the biometric system.

Best Practice	Description	Ability to Comply
Protection of Biometric Information	Biometric information should be protected at all stages of its lifecycle, including storage, transmission, and matching. The protections enacted may include encryption, private networks, secure facilities, administrative controls, and data segregation.[3]	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Protection of Post-Match Decisions	Data transmissions resulting from biometric comparisons should be protected. Although these post-comparison decisions do not necessarily contain any biometric data, their interception or compromise could result in unauthorized access being granted to personal information.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Limited System Access	Access to biometric data should be limited to certain personnel under predefined conditions, and such access should be subject to controls and strong auditing.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Segregation of Biometric Information	Biometric data should be stored separately from personal information such as name, address, and medical or financial data. Depending on the manner in which the biometric data is stored, this separation may be logical or physical.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y

[3] The protections necessary within a given deployment are determined by a variety of factors, including the location of storage, location of matching, the type of biometric used, and the capabilities of the biometric system, which processes take place in a trusted environment, and the risks associated with data compromise.

System Termination	A method should be established by which a system used to commit or facilitate privacy-invasive biometric matching, searches, or linking can be depopulated and dismantled.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y

Table 7: BioPrivacy Best Practices – Data Protection

6.4.6 BioPrivacy Best Practices: User Control of Personal Data

User control over personal information is a basic privacy principle, inasmuch as it limits a system operator's ability to abuse biometric data. Without some type of control over biometric data, individuals have only indirect recourse if they object to system usage.

Best Practice	Description	Ability to Comply
Ability to "Unenroll"	Individuals should have the right to control usage of their biometric information, and to have it deleted, destroyed, or otherwise rendered unusable upon request.	Watch list: N Identification: Depends Eligibility: Y Identity Verification: Y
Correction of and Access to Biometric-Related Information	System operators should provide a method for individuals to correct, update, and view information stored in conjunction or association with biometric information.	Watch list: N Identification: Depends Eligibility: Y Identity Verification: Y
Anonymous Enrollment	Depending on operational feasibility, biometric systems should be designed such that individuals can enroll with some degree of anonymity.	Watch list: N Identification: N Eligibility: Y Identity Verification: N

Table 8: BioPrivacy Best Practices – User Control of Personal Data

6.4.7 BioPrivacy Best Practices: Disclosure, Auditing, Accountability, and Oversight

Disclosure, auditing, accountability, and oversight are the most important types of privacy protection implemented in large-scale systems. Without the protections that result from system oversight, it becomes difficult to enforce privacy-sympathetic system usage. Because even well designed systems can be used in a fashion inconsistent with privacy principles, processes related to disclosure, auditing, accountability, and oversight must accompany all system functions.

Best Practice	Description	Ability to Comply
Third Party Accountability, Audit, and Oversight	The operators of certain biometric systems, especially large-scale systems or those employed in the public sector, should be held accountable for system use. As internal or external agents may misuse biometric systems, independent system auditing and oversight is required.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Full Disclosure of Audit Data	Individuals should have access to data generated through third-party audits of biometric systems. Data derived from system oversight should be available to facilitate public discussion on the system's privacy impact.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
System Purpose Disclosure	The purposes for which a biometric system is being deployed should be fully disclosed in order to facilitate informed assessments on the system's potential privacy impact.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Enrollment Disclosure	Ample and clear disclosure should be provided when individuals are enrolled in a biometric system. Disclosure should occur even if reference templates are not stored.	Watch list: Depends Identification: Y Eligibility: Y Identity Verification: Y
Matching Disclosure	Ample and clear disclosure should be provided when individuals are in a location or environment where biometric matching (either 1:1 or 1:N) may be taking place without their explicit consent.	Watch list: Y Identification: Y Eligibility: Y

Best Practice	Description	Ability to Comply
		Identity Verification: Y
Use of Biometric Information Disclosure	Biometric information should only be used for the purpose for which it was collected, within the system for which it was collected, unless the user explicitly agrees to broader usage.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Disclosure of Optional/Mandatory Enrollment	Ample and clear disclosure should be provided indicating whether enrollment in a biometric system is mandatory or optional. If optional, alternatives to the biometric should be made readily available.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Disclosure of Entity Responsible for System Operation and Oversight	It should be clearly stated who is responsible for system operation, to whom questions or requests for information are addressed, and what recourse individuals have to resolve grievances.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Disclosure of Enrollment, Verification and Identification Processes	Individuals should be informed of the process flow of enrollment, verification, and identification. This includes detailing the type of biometric and non-biometric information they will be asked to provide, the results of successful and unsuccessful positive verification, and the results of matches and non-matches in identification systems.	Watch list: Y Identification: Y Eligibility: Y Identity Verification: Y
Disclosure of Biometric Information Protection and System Protection	Individuals should be informed of the protections used to secure biometric information, including encryption, private networks, secure facilities, administrative controls, and data segregation.	Watch list: Depends Identification: Depends Eligibility: Y Identity Verification: Y

Best Practice	Description	Ability to Comply
Fallback Disclosure	When available, fallback authentication processes should be available for individuals to review should they be unable or unwilling to enroll in a biometric system.	Watch list: N Identification: Text-based Eligibility: Y Identity Verification: Y

Table 9: BioPrivacy Best Practices – Disclosure, Auditing, Accountability, and Oversight

6.4.8 Privacy Impact: Conclusions

Identity confirmation poses privacy risks due to mandatory enrollment and lack of anonymity. Watch list checks pose privacy risks due to the use of central databases, the retention of images, and 1:N functionality.

It will be necessary to incorporate a range of privacy protections – some relating to security of sensitive data, others relating to system oversight and accountability for system misuse – in order to ensure that biometrics in mobile applications are deployed in a privacy-sympathetic fashion. Many of these protections can be gained through adherence to international standards, such as ISO/IEC WD 29101, which focuses on focuses on requirements for managing and protecting Personally Identifiable Information (PII).

It is incumbent upon all parties with operational responsibility for collecting, transmitting, storing, and utilizing biometric data to protect this data at all stages in its lifecycle. However, the nature of mobile biometric identification is such that privacy is not an absolute. If fingerprint-based technology, for example, provides demonstrably higher security and reliability than technologies perceived as less privacy-invasive, then privacy issues must be dealt with procedurally.

6.5 Cultural Acceptability of Biometric Technology

The acceptability of biometric technologies is a consideration in functional applications. Individuals may be opposed to all biometric usage, or may be uncomfortable with a specific biometric technology.

While the association of fingerprints with criminal justice activities has negatively impacted public perception of the technology, mobile biometrics are often used in situations that are already overtly related to criminal justice. Privacy fears and lack of acceptability may be justified in the context of identifiable fingerprints where there is centralized retention. An identifiable fingerprint can act as a unique identifier that can bring together disparate pieces of personal information about the subject. This could be viewed as invasion of privacy to which some people would object.

Iris recognition encounters acceptance issues from users uncomfortable with having their eyes measured, though there is no medical basis for this objection. Face images are already a part of nearly every identity document program in the world, such that the acceptability of acquiring face images is not in question. Whether this blanket acceptability extends to use of face images for automated searches is another question: it seems that there is more resistance to face imaging as a biometric technology than to simple face imaging for the purposes of placement in a document.

6.6 Emergence of Legal Frameworks Governing Use of Biometrics

As biometrics become more commonly deployed in government programs, policy and legislature should be updated to reflect best practices and guidelines for maintaining privacy.

For applications within the Province of Ontario, the Office of the Privacy Commissioner of Ontario (IPC), has developed a list of procedural and technical safeguards that should be in place prior to the implementation of any biometric technology. The recommendations are as follows:

- The biometric sample should be encrypted.
- The use of the encrypted sample should be restricted to authentication of Eligibility, thereby ensuring that it is not used as an instrument of surveillance.
- The identifiable sample cannot be reconstructed from an encrypted instant stored in the database ensuring that a latent biometric cannot be matched to an encrypted sample stored in a database.
- The encrypted sample itself cannot be used to serve as a unique identifier.
- The encrypted sample alone cannot be used to identify an individual.
- Strict controls on who may access the biometric data and for what purposes should be established. A warrant or court order should be presented prior to granting access to external agencies.

- Any personal data of auxiliary nature (i.e., personal history / traveling patterns) should be stored separately from personal identifiers such as name or date of birth.

These guidelines have been incorporated into the Ontario government's Social Assistance Reform Act to govern the use and collection of biometrics for government welfare and benefit programs. Other Canadian provinces and agencies may use a similar approach in determining privacy-sympathetic guidelines for their respective biometric programs. To fully address any concerns of privacy advocates and Canadian citizens, the introduction of biometric language to legislation at the national level, such as The Privacy Act and PIPEDA, is advised.

7 Existing Mobile Biometric Deployments

7.1 Fingerprint-AFIS/Live-Scan

7.1.1 California: Ontario-Montclair School District-Student Fingerprint Identification[4]

Summary: In 1999, the Ontario-Montclair School District, the second largest elementary school district in California, has contracted ATSONIC to deliver their sweetFINGER for School-buses solution. Each school bus is wirelessly connected to a central server and can transmit student identification information based on fingerprint identifiers, student boarding and leaving auditing trails, exact bus location, expected arrival times, and field trip support.

Technology: Originally developed for law enforcement personnel, the ATSONIC sweetFINGER product is a fingerprint system that allows real-time fingerprint authentication, coupled with wireless transmission functionality. The product is bundled with 500 dpi image processing software as well as technology for electronically transmitting fingerprint data to remote, centralized servers. Primarily geared for use by law enforcement agents on the field, sweetFINGER enables real-time collection and verification of fingerprints. SweetFINGER is also available with integrated GPS functionality for additional tracking capabilities.

Operators/Subjects: The operators would include local school officials, teachers, bus drivers, and elementary school children. The subjects would be students in the enrolled Ontario-Montclair School District. Biometric data should not exist prior to enrolment of the program. Personally Identifiable Information (PII) will be retained for the duration the student is enrolled in a school associated with the Ontario-Montclair School District, however, PII should not be shared with other agencies due to privacy and protection concerns of minors.

Operational Constraints: Many operational constraints could exist directly related to the operational environment being on a vehicle which is outside, a reasonable amount of throughput activity that should not take need a significant time investment, degradation of the finger print sample from daily activities, etc. The article does not indicate that the sweetFINGER system will be used in conjunction with any additional biometric systems. However, it will use existing wireless communication networks and information systems to transmit and store the data back to a centralized server.

7.1.2 California: LACRIS-Mobile Fingerprint Recognition for Criminal ID[5]

Summary: The Los Angeles County Regional Identification System (LACRIS) purchased Cogent Systems' BlueCheck mobile identification devices to provide to Los Angeles Police Department patrol officers so that officers can run rapid fingerprint checks on subjects in the field.

Technology: One of the latest portable fingerprint scanners that Cogent Systems has developed, the BlueCheck is a mobile biometric device tailored toward local law enforcement use. The BlueCheck is equipped with a small, durable LCD display for real-time feedback, a 500 dpi fingerprint scanner and utilizes Cogent's SecurASIC technology for encryption and image compression. The BlueCheck enables users to perform on-the-spot fingerprint acquisition and matching against the fingerprint templates stored on the device. Additionally, using Bluetooth communication (up-to 30 feet), the BlueCheck is capable of remotely transferring captured fingerprint data to a host, such as a PDA, laptop or cellular device to allow for identification and verification of identity against a centralized database of prints. In order for this to

[4] http://bio1.com/projects/california-ontario-montclair-school-district-student-fingerprint-identification

[5] http://bio1.com/projects/california-lacris-%E2%80%93-mobile-fingerprint-recognition-criminal-id

occur, the BlueCheck connects to Cogent's BlueCheck host application, the host device can then submit ANSI-NIST format files via SMTP or FTP to a remote server or AFIS, and then the search can be conducted. Once the search is complete, the BlueCheck receives the search results from the host and displays the results on its LCD display, providing nearly real-time identification for law enforcement personnel. BlueCheck has the ability to store up-to 1200 templates (6000 with optional flash drive) and it can search up-to 500 on-device templates in 1.5 seconds.

Operators/Subjects: The operators would be trained law enforcement officers of the Los Angeles Police Department. Subjects can include any individual physically located within the Los Angeles Police Department's jurisdiction. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Operational Constraints: Operational constraints are present due to the operational environment. The patrol officer can be inside/outside or in adverse weather conditions which may influence performance. The article did not present any information suggesting the use of other biometric systems. The system will use previously established information system(s) and communication systems to connect to the remote server or AFIS. BlueCheck uses Bluetooth and USB communications.

7.1.3 Australia: New South Wales Police Force--Remote Fingerprint Identification[6]

Summary: The New South Wales Police Force in Australia has received 500 units of Sagem Sécurité's Morpho RapID 1100 mobile fingerprint terminals. These mobile devices provide police officers the ability to capture an individual's fingerprints at remote locations, and conduct real-time searches against a local or central database.

Technology: The Sagem Sécurité's Morpho RapID 1100 is a mobile fingerprint terminal. The Morpho RapID 1100 is built on the Psion Teklogix iKon, a handheld PDA rated IP54, making it resistant to adverse weather conditions such as dust and rain. The device incorporates a 2-megapixel digital camera to capture facial images in addition to its existing fingerprint acquisition capabilities, as well as a keyboard and Bluetooth wireless capabilities. The third generation Morpho RapID 1100 offers a faster data transmission than its predecessors by improving upon their wireless communication capabilities. The device, which is primarily used for capturing 500-ppi fingerprint images, can hold up to 180,000 records with its built-in watch list feature. Previous generations could only hold up to 100,000 records. Prints can be instantly checked against its vast onboard database and the results can be transmitted wirelessly to centralized AFIS systems.

Operators/Subjects: Operators include trained police officers of the New South Wales Police Force. Subjects can include any individual physically within the New South Wales Police Force jurisdiction. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

[6] http://bio1.com/projects/australia-new-south-wales-police-force-%E2%80%93-remote-fingerprint-identification

Constraints: Operational constraints exist due to the operational environment in New South Wales. Use of the device can occur indoors/outdoors and in remote locations towards the interior of the country leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors, it is has IP54 dust/water protection and is resistant to a 4 foot drop on concrete. The article does not indicate that the system would be used with any additional biometric or information systems. The system may be linked to additional information systems to run a database check but the device itself has significant capacity to function autonomously. The device uses existing WiFi, cellular (GSM, GPRS, EDGE, and 3G UMTS/WCDMA) and Bluetooth.

7.1.4 Oregon: Portland Police Bureau-Mobile AFIS Pilot[7]

Summary: The Portland, Oregon Police Bureau implemented a pilot program to deploy mobile AFIS devices. Due to budgetary constraints, the Portland Police Bureau has an extremely limited police force. Thus, with the implementation of a Mobile AFIS system more police officers can remain in the field while still being able to access local and national criminal databases. The officers will be equipped with an Identix IBIS Remote Data Terminal (Identix RDT).

Technology: IBIS (Integrated Biometric Identification System) is a mobile identification unit for law enforcement applications. IBIS allows field officers to capture high quality fingerprints and facial images on a handheld device. Biometric data acquired by IBIS is transmitted wirelessly to a central site server for validation against law enforcement databases. IBIS captures photographs and fingerprint images in industry standard NIST EFTS format for searches against databases such as AFIS, WIN, MAFIN, IDENT, and NCIC. The device works with Windows Mobile PDAs using existing cellular services.

Operators/Subjects: Operators will include law enforcement officers of the Portland, Oregon Police Bureau. Subjects can be US citizens and non-US citizens physically located in the Portland, Oregon Police Bureau jurisdiction. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match FBI NCIC database. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational constraints exist due to the operational environment. Each police officer has a large area of responsibility and cannot be overburdened with an inefficient system. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. It can operate with the EVDO/CDMA 1XRTT (Sprint/Verizon) and EDGE/GPRS (Cingular) communications systems. The device does have weather proofing (IP54 rating) that will mitigate environmental factors. The article does not indicate that the system would be used with any additional biometric systems. The device must be connected to a host PDA with Windows Mobile 2005, 32 MB RM, 64 MB Flash.

7.2 Multimodal

7.2.1 Minnesota: Bureau of Criminal Apprehension-Identix Mobile ID[8]

Summary: In 1999, the State of Minnesota Bureau of Criminal Apprehension contracted Identix Incorporated to provide an Integrated Biometric Identification System (IBIS) server and 16 IBIS mobile handheld unit, increasing the state's total deployed IBIS handheld mobile units to 80.

---

[7] http://bio1.com/projects/oregon-portland-police-bureau-mobile-afis-pilot

[8] http://bio1.com/projects/minnesota-bureau-criminal-apprehension-identix-mobile-id

Technology: IBIS is a mobile identification unit for law enforcement applications. IBIS allows field officers to capture high quality fingerprints and facial images on a handheld device. Biometric data acquired by IBIS is transmitted wirelessly to a central site server for validation against law enforcement databases. IBIS captures photographs and fingerprint images in industry standard NIST EFTS format for searches against databases such as AFIS, WIN, MAFIN, IDENT, and NCIC. The device works with Windows Mobile PDAs using existing cellular services.

Operators/Subjects: Operators include law enforcement officers from the State of Minnesota Bureau of Criminal Apprehension. Subjects include individuals who are physically located within the BCA's jurisdiction. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device is subject to a variety of environmental factors. It will be used with additional biometric and information systems to access criminal databases. It will use localized wireless networks to transmit the data to the PDA and the PDA will then transmit data to a centralized server.

7.2.2 Benin: Fingerprint and Face Imaging for 2011 Presidential Elections[9]

Summary: Gemalto delivered 3,200 Coesys mobile enrolment stations to the Republic of Benin. The Coesys enrolment solution is to manage the secure biometric registration of voters in the Republic of Benin.

Technology: The Coesys Enrolment Mobile is a portable enrolment station. The enrolment station and associated software captures citizens' demographic data, fingerprints, and digital photograph in the field.

Operators/Subjects: Operators will be individuals associated with the Republic of Benin who are sent in the field to register voters in the Presidential elections. Subjects are the citizens of the Republic of Benin who are eligible to vote in the elections. The goal is to enroll the subject with the subject's exact identity. PII will be stored; however it should not be shared for other purposes to address privacy issues. Policy constraints exist such as having all eligible citizens registered before a possible registration cutoff and/or the election occurs.

Constraints: Operational constraints exist because of anything that could decrease functionality of the Coesys Enrolment Mobile in the field e.g. a remote location with limited connectivity. It would seem that there is no existing biometric system that will be working with the Coesys Enrolment Mobile system. The system will need to use existing information systems and communications systems.

7.2.3 L-1 Receives $8.3m Order for HIIDE 4.0 from US Army's Space Program Office[10]

Summary: In 2009, The U.S. Army's Space Program Office placed an $8.3 million order for HIIDE 4.0 (Handheld Interagency Identity Detection Equipment). The HIIDE 4.0 has since been deployed to areas of conflict around the globe where the U.S. Army is conducting operations.

---

[9] http://bio1.com/projects/benin-fingerprint-and-face-imaging-2011-presidential-elections

[10] http://bio1.com/news/l-1-receives-83-million-order-hiide-40-us-army%E2%80%99s-space-program-office

Technology: Developed with funding from the US government, and deployed in Iraq and Afghanistan, the HIIDE (Hand-held Interagency Identity Detection Equipment) Series 4 is the world's first completely handheld system featuring multimodal finger, face and iris enrollment and matching capabilities. The HIIDE provides complete functionality while connected to a host PC or when operating in the field untethered. The HIIDE offers a USB port for connecting to peripheral devices such as passport or card readers or an external keyboard and mouse. HIIDE 4 creates and processes data in portfolio XML, a data format that requires conversion in order to interoperate with EFTS-based systems. HIIDE uses Neurotechnology fingerprint and SecuriMetrics iris matching (it captures but does not match faces). The device has an onboard storage and search capability of 22,000 full biometric portfolios (2 iris templates, 10 fingerprints, a facial image, and biographic data). The device use Integrated RF communications: 802.11b/g, Bluetooth, GSM/GPRS (EV-DO/EDGE optional), and USB connectivity capable.

Operators/Subjects: Operators include U.S. Army personnel deployed to areas of conflict around the globe. Subjects are anyone in the area of conflict e.g. local citizens, possible terrorists, or opposing forces. The goal is to enroll, identify, verify, and authenticate individual's exact identity. PII will be retained and possibly shared to check watch lists of known terrorists or opposing forces.

Constraints: Operational constraints exist on a case by case basis depending on the specific operational environment. Associated biometric, information, and communications networks are available to the operator depending on the operating environment.

7.2.4 MaxID's iDL520 Handheld Multimodal Capture Device Selected for US Army Contract Leveraging Lumidgm Sensor[11]

Summary: The U.S. Army has acquired and deployed the MaxID iDL520 Handheld Multimodal Capture Device. The iDL520 can be used for a variety of US Army missions including border security, law enforcement, force protection, civilian disaster assistance, and intelligence.

Technology: The iDL520 multimodal, rugged biometric mobile computer offers enhanced fingerprint reading capabilities. Featuring Lumidigm's Venus multispectral imaging fingerprint sensor, the iDL520 simultaneously reads the surface and subsurface of any finger to capture images even when surface features are absent or hard to distinguish due to age, dirt, finger pressure, and skin or environmental conditions. In addition to Lumidigm's state-of-the-art fingerprint sensor, the iDL520 integrates a smart card reader, a powerful 2D barcode reader and a 3.5 color TFT LCD sunlight-readable display at 320x240 resolution. An integrated 40-key QWERTY keyboard also includes several programmable function keys and the optional pistol grip with trigger button enables one-handed operation. Optional magnetic swipe & OCR/MRZ accessories allow the operator to screen credentials, including passports, e-passports, and a wide array of PIV cards, driver's licenses and other documents. The personal identity validation features are complemented by 3G UMTS, GSM/GPRS/EDGE, 802.11b/g WiFi, and Bluetooth wireless communications capabilities. Running Microsoft Windows CE .NET 6.0, the iDL520 offers an open, flexible platform. It is supplied with a comprehensive Software Development Kit to enable fast and easy application development. Based around MaxID's award-winning iDL500 design, the iDL520 weighs less than two pounds, the high- impact ABS plastic case is shock tested to survive repeated drops of more than three feet to concrete and is designed to withstand ingress of water and dust. The high capacity Lithium-Ion battery is designed to last a full typical shift.

Operators/Subjects: Operators include US Army personnel deployed in any capacity around the globe. Subjects can include US citizens, non-US citizens, children, adults, etc. anyone that is encompassed in the mission set. Also, the iDL 520 may be used for enrolment, identification, or verification/authentication based on the mission set. PII may or may not be shared and or retained depending on the mission set.

[11] http://bio1.com/news/maxid%E2%80%99s-idl520-handheld-multimodal-capture-device-selected-us-army-contract-leveraging-lumidigm

Constraints: Operational constraints do exist based on the operational environment. Use of the device can occur indoors/outdoors and in Environmental factors should not inhibit functionality of the fingerprint reader but may inhibit the smart card reader. The article does not indicate that the system would be used with any additional biometric or information systems. It will use 3G UMTS, GSM/GPRS/EDGE, 802.11b/g WiFi, and Bluetooth wireless communications capabilities.

7.2.5 BI2 Provides MORIS iPhone-Based Iris Recognition Technology and Animetrics' Face Technology for Plymouth County[12]

Summary: The Plymouth County Sheriff's Department (MA) and the City of Brockton Police Department (MA) have deployed Biometric Intelligence and Identification Technologies iPhone-based Wireless Multi-Modal Biometric Mobile Offender Recognition and Information device and system (MORIS).

Technology: MORIS along with the Animetric's Face technology provide iris recognition and facial recognition to the iPhone. MORIS is a sleeve attachment that attaches an infrared camera and viewing capability to the iPhone's built in camera. The Animetric's face technology provides 2D-3D facial recognition technology to the iPhone. The Mobile Offender Recognition & Information System (MORIS) is an iris recognition prototype developed by BI2 Technologies. It is a sleeve attachment that can be attached to the iPhone, which adds an infrared camera and viewing capability to the iPhone's built-in camera. The attachment adds approximately 1.5 ounces to the total weight of the phone, and the MORIS includes access to both IRIS and SORIS, which are products of BI2 technologies. Additionally, there are plans to design a similar attachment for Blackberry devices, and support the needs of the various law enforcement agencies. Using commercial cell services that support Internet connectivity, MORIS provides users the capability to capture an individual's iris image, transmit information to a local or central database, and conduct remote searches onsite.

Operators/Subjects: Operators include law enforcement officers of the Plymouth County Sheriff's Department and the City of Brockton Policy Department. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Policy and operational constraints exist when a law enforcement officer encounters/apprehends an individual. MORIS will use existing biometric, information, and communications systems/networks in order to transmit data to a central server.

7.2.6 Iris ID releases iCAM TD100 Software for the Unique Identification Authority of India (UIDAI) Project[13]

Summary: Iris ID Systems Inc. has released its AADHAAR Biometric Capture Device Software for IrisID's Iris Access iCAM TD100 system for the Unique Identification Authority of India (UIDAI) project. The Unique Identification Authority of India has envisioned the UID as a number that will make it possible for Indian residents to easily verify their identity to public and private agencies across the country.[14]

---

[12] http://bio1.com/news/bi2-provides-moris-iphone-based-iris-recognition-technology-and-animetrics%E2%80%99-face-technology-ply

[13] http://bio1.com/news/iris-id-releases-icam-td100-software-unique-identification-authority-india-uidai-project

[14] http://uidai.gov.in/UID_PDF/Front_Page_Articles/Strategy/Exclusion_to_Inclusion_with_Micropayments.pdf

Technology: IrisAccess iCAMTD100 is a portable multi modal face/iris image capturing, USB enabled device hence is suitable for bundling with mobile jump-kit used at the registration offices and sites. With its proven reliability, accuracy and high-speed image capturing, the device is fit for the UIDAI project. Fully automatic dual iris image capture and quality analysis routines are available as a part of the SDK API set for the field application of the iCAMTD100 from the Iris ID website. Iris and face capture are performed by the operator extending their arm from the face capture distance to the iris capture distance from 30 inches to 15 inches. The iris enrollment time for 2 iris captures is 8 seconds for a complete transaction.

Operators/Subjects: Operators include Indian officials employed with UIDAI. Subjects are Indian citizens. The goal is to enroll and eventually authenticate the subject's exact identity for verification and establish an access list for benefits. The subjects will not be able to opt-out of identity proofing. PII will be retained and will be shared with other agencies so the subject can verify their identity at multiple agencies.

Constraints: Operational and Policy constraints may exist but are unknown at this time. The system will be a part of the UIDAI project's jump-kit for subject enrollment. Therefore, it would seem that the system will use localized communications systems and biometric systems for enrollment of subjects. There may also be localized or centralized information systems for data storage.

7.2.7 Afghanistan: National Police Identification Project[15]

Summary: In conjunction with the U.S. Government, the Afghanistan National Police deployed Datastrip's 2DSuperscript two-dimensional bar code as the main technology in their identification document system. The 2004 initiative was implemented to improve security and manage payroll distribution by providing a counterfeit-resistant identity document.

Technology: The cards include a two-dimensional bar-code embedded with biographic and biometric data as well as security questions. The 2D barcode is able to store large amounts of data like a smartcard but at a lower cost. The data is stored in English and local languages. Mobile verification is done by trained personnel using Datastrip's DSVerify2D, a hand-held biometric identity document reader capable of decoding fingerprints, text, and photographs in a single swipe. The device has an optical fingerprint scanner, and is able to match the cardholder's live fingerprint with the stored fingerprint data on the document. This fingerprint technology was developed by SI International and is in both English and Dari. The application also provides photo and signature verification, and confirmation of the responses to the stored security questions.

Operators/Subjects: Operators include US military personnel and Afghanistan National Police personnel. Subjects will be enrolled Afghanistan National Police personnel. PII will be stored to develop an access list for future use.

Constraints: Possible operational constraints exist due to the operational environment and maintenance concerns. It is unknown whether or not the system will be operating with other biometric, information, and communications systems. The system would need to operate other wireless networks would need to be available to the user.

7.2.8 PHA Implements TWIC Program Using Datastrip's DSV2+Turbo Mobile Readers Enrolling 7000 TWIC Cardholders[16]

[15] http://bio1.com/projects/afghanistan-national-police-identification-project

[16] http://bio1.com/news/pha-implements-twic-program-using-datastrip%E2%80%99s-dsv2turbo-mobile-readers-enrolling-7000-twic-card

Summary: The Port of Houston Authority (PHA) implemented the Transportation Worker Identification Credential (TWIC) program by harnessing a handheld card reader technology solution from Datastrip and Codebench Inc. Using Datastrip's DSV2+TURBO with Codebench's PIVCheck Plus software, PHA has enrolled close to 7,000 TWIC cardholders in the Houston area to date. To comply with federal TWIC guidelines, all longshoremen, truckers, steamship line personnel, stevedores and vendors requiring access to PHA restricted areas must carry a TWIC card.

Technology: The DSV2+TURBO is Datastrip's rugged, compact handheld mobile biometric terminal. The unit is used in identity verification and biometric data collection applications including border control. The DSV2+TURBO is a FIPS 201 certified single-fingerprint capture device, and also reads contact/contactless smartcards. It can be configured to operate for up to 16 on a single battery charge using an upgraded battery option. The unit offers several expansion capabilities including the ability to read magnetic stripes or 2D barcodes, as well as connectivity through USB, CF, serial, Wi-Fi, Bluetooth or cellular technologies. The system has an IP54/MIL-STD-810F rating for ruggedization.

Operators/Subjects: Operators will include officials of the Port of Houston Authority. Subjects will include enrolled longshoremen, truckers, steamship line personnel, stevedores, and vendors. The goal is to enroll and verify the subject's exact identity and to establish an access list. After enrolment, PII will be stored. PII may be shared with other Port Authorities who have implemented the program to establish/confirm access lists.

Constraints: Operational constraints include environmental factors that would limit functionality or make the card unreadable. The device has a high ruggedization rating so it would seem the device is fairly weatherproof. The device will use existing information and communication systems to store and transmit biometric data. It is unknown if previous biometric systems are being used.

7.2.9 Port of Wilmington Deploys Datastrip's DSV2+Turbo Mobile Card Reader to Comply with TWIC Program Requirements[17]

Summary: The Port of Wilmington security officials are using Datastrip's DSV2+TURBO rugged card readers to enroll and positively identify the port's authorized workers; enabling the Port of Wilmington to be compliant with Transportation Worker Identification Credential (TWIC) program. Codebench's PIVCheck Plus software drives Datastrip's mobile readers. Port security officials have been using three Datastrip DSV2+TURBO devices with Codebench's PIVCheck Plus software at the main gate to enroll TWIC cards. Additionally, Codebench's PIVCheck Plus software has been installed on one of the port's desktop computers so that TWIC cards can be registered on-site. Port officials have future plans for mobile security patrols to use the DSV2+TURBO units to spot check workers.

Technology: The *DSV2+TURBO* is Datastrip's rugged, compact handheld mobile biometric terminal. The unit is used in identity verification and biometric data collection applications including border control. The *DSV2+TURBO*is a FIPS 201 certified single-fingerprint capture device, and also reads contact/contactless smartcards. It can be configured to operate for up to 16 on a single battery charge using an upgraded battery option. The unit offers several expansion capabilities including the ability to read magnetic stripes or 2D barcodes, as well as connectivity through USB, CF, serial, Wi-Fi, Bluetooth or cellular technologies. The system has an IP54/MIL-STD-810F rating for ruggedization. Operators/Subjects: Operators will include officials of the Port of Wilmington Authority. Subjects will include enrolled longshoremen, truckers, steamship line personnel, stevedores, and vendors. The goal is to enroll and verify the subject's exact identity and to establish an access list. After enrolment, PII should not be stored. PII may be shared with other Port Authorities who have implemented the program to establish/confirm access lists.

[17] http://bio1.com/news/port-wilmington-deploys-datastrip%E2%80%99s-dsv2turbo-mobile-card-reader-comply-twic-program-requiremen

Constraints: Operational constraints include environmental factors that would limit functionality or make the card unreadable. The device has a high ruggedization rating so it would seem the device is fairly weatherproof. The device will use existing information and communication systems to store and transmit biometric data. It is unknown if previous biometric systems are being used.

7.2.10 Intellicheck Mobilisa Announces Third Pilot Testing of IM2700 TWIC Reader at Major Seaport in North America[18]

Summary: Intellicheck Mobilisa, Inc. announced that a seaport agreed to begin pilot testing of Intellicheck Mobilisa TWIC reader handheld device. The seaport is among North America's top ten container ports and represents the company's third pilot test program for the device. The pilot program is being tested and three major North American ports.

Technology: The IM2700 is a ruggedized mobile device that is designed to read Transportation Worker Identification Credentials (TWIC) cards. It can access data stored on the contact smartcard using 1D or 2D barcodes, magnetic stripe data, or smart chip. Additionally, the reader comes with a silicon-based single fingerprint reader to capture user fingerprint data.

Operators/Subjects: Operators will include officials of the port authority officials. Subjects will include enrolled longshoremen, truckers, steamship line personnel, stevedores, and vendors. The goal is to enroll and verify the subject's exact identity and to establish an access list. After enrolment, PII should not be stored. PII may be shared with other Port Authorities who have implemented the program to establish/confirm access lists.

Constraints: Operational constraints include environmental factors that would limit functionality or make the card unreadable. Also, any additional that may limit the functionality of the silicon fingerprint scanner. It is unknown whether or not the system will be operating with other biometric systems. Local information and communication systems will need to exist in order to transmit data.

7.2.11 Fairfax County Police Deploys Datastrip DSV2+TURBO Devices to Enhance Identification Accuracy in the Field[19]

Summary: The Fairfax County (Virginia) Police Department (FCPD) deployed DSV2+TURBO handheld biometric terminal. The units were loaded with custom software to seamlessly interface with FCPD's Automatic Fingerprint Identification System (AFIS).

Technology: The DSV2+TURBO is Datastrip's rugged, compact handheld mobile biometric terminal. The unit is used in identity verification and biometric data collection applications including border control. The DSV2+TURBO is a FIPS 201 certified single-fingerprint capture device, and also reads contact/contactless smartcards. It can be configured to operate for up to 16 on a single battery charge using an upgraded battery option. The unit offers several expansion capabilities including the ability to read magnetic stripes or 2D barcodes, as well as connectivity through USB, CF, serial, Wi-Fi, Bluetooth or cellular technologies. The system has an IP54/MIL-STD-810F rating for ruggedization.

Operators/Subjects: Operators include FCPD law enforcement officers. Subjects include US citizens and non-US citizens located within Fairfax County, Virginia. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If

[18] http://bio1.com/news/intellicheck-mobilisa-announces-third-pilot-testing-im2700-twic-reader-major-seaport-north-amer

[19] http://bio1.com/news/fairfax-county-police-employs-datastrip-dsv2-turbo-units-field-identification-applications

necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational constraints include environmental factors that would limit functionality or make the card unreadable. The device has a high ruggedization rating so it would seem the device is fairly weatherproof. The device will use existing information and communication systems to store and transmit biometric data. It is unknown if previous biometric systems are being used.

7.2.12 Texas Department of Public Safety Deploys NEC Mobile Identification Solution[20]

Summary: The Texas Department of Public Safety deployed the NEC Integra-ID Mobile Identification Solution. The system will allow law enforcement officers to get real-time positive identification of an individual without having to transport them to the police station.

Technology: Integra-ID is an off-the-shelf suite of fingerprint and palmprint matching solution built on a service-oriented architecture. It uses multiple algorithms to process and manage latent fingerprints, palmprints, and tenprints. Integra-ID was designed to integrate seamlessly with third-party biometric devices.

Operators/Subjects: Operators include Texas Department of Public Safety law enforcement officers. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The article does not indicate that the system would be used with any additional biometric systems. However, it will use localized wireless networks and information systems to transmit the data.

7.2.13 Croatia: Border Management Project[21]

Summary: In September 2010, MaxID announced its sale of the iDL500 multimodal computers to IN2 and consortium partner S&T, for deployment in a Border Management application in Croatia. The iDL500 units delivered to IN2 will be used for reading, validating and recording information from passports and ePassports.

Technology: The iDL500 features On-board contact card, contactless card, barcode, and an optical fingerprint reader combined with a digital camera, GPS, and wireless communications (GSM/GPRS/EDGE, 802.11b/g WiFi, and Bluetooth). Additional card reading capabilities are provided by the combined contactless & smart card reader which is FIPS-201 compliant and has iClass capabilities. Optional magnetic swipe & OCR/MRZ accessories allow the operator to screen credentials, including passports, e-passports, Transportation Worker's Identification Credentials (TWIC), Common Access Cards (CAC), First Responder Authentication Cards (FRAC), Personal Identity Verification (PIV), driver's license and other documents. The digital camera is designed to acquire FIPS-201 compliant face images under low-light levels.

---

[20] http://www.thirdfactor.com/2012/03/29/texas-agency-deploys-nec-criminal-id-solution

[21] http://bio1.com/projects/croatia-border-management-project

Operators/Subjects: Operators would include Croatian border personnel. Subjects include any individual who is crossing the Croatian border. The goal is to enroll, identify, verify, and authenticate a subject's exact identity. Biometric data should not exist until individual has been enrolled. PII will be retained and may be shared with other Croatian authorities.

Constraints: Policy and operational constraints will exist depending on local and federal legal statutes. Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The article does not indicate that the system would be used with any additional biometric systems. The device has wired connectivity, wireless connectivity, and cellular connectivity capabilities so connectivity should be a non-issue.

7.3 Related Technologies

7.3.1 New Jersey: TRANSIT Police - BIO-Key Mobile ID[22]

Summary: In 1999, the New Jersey TRANSIT Police began a project that implemented BIO-Key PocketBlue, a handheld mobile device, and the PacketCluster Patrol, a wireless information system, to identify subjects in real time. In 2004, the TRANSIT Police, the FBI, Secret Service, and the New York Police Department (NYPD) utilized the system to enhance security and the 2004 Republican National Convention to identify individuals at Newark and Penn Station.

Technology: BIO-Key PocketBlue is a handheld software application that allows law enforcement officers to check the identity rapidly and remotely. PacketControl Patrol is a wireless information system highlighted by Real-time wireless data collection mobile device independence, wireless infrastructure independence, standards-based connectivity, efficient bandwidth management, and simplified mobile user interface.

Operators/Subjects: Operators include New Jersey TRANSIT policy, the FBI, Secret Service, and the NYPD. Subjects include individuals located within the jurisdiction of the New Jersey TRANSIT police. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational and policy constraints exist when a law enforcement officer addresses a public citizen. Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The article does not indicate that the system would be used with any additional biometric or information systems. However, it will use localized wireless networks to transmit the data.

7.3.2 Massachusetts: Brookline Police Department-BIO-Key Pocketcop Mobile ID System[23]

Summary: In 2004, the Brookline Police Department upgraded their wireless network system with BIO-Key PocketCop. Working with Verizon's CDMA wireless network, PocketCop provides law enforcement

[22] http://bio1.com/projects/new-jersey-transit-police-bio-key-mobile-id

[23] http://bio1.com/projects/massachusetts-brookline-police-department-bio-key-pocketcop-mobile-id-system

officers with the ability to access federal, state, and local criminal records as well as adding fingerprint identification, imaging, automatic vehicle location, and global positioning functionalities.

Technology: The PocketCop is a handheld software application that allows law enforcement officials to retrieve information at remote locations in real-time. Using commercially available mobile phones such as BlackBerry, the application allows officers to receive information directly from an agency's computer-aided dispatch system and send status reports to dispatch. Additionally, it can be customized to enable officers to access information from federal, state and local criminal databases.

Operators/Subjects: Operators include Brookline Police Department law enforcement officers. Subjects include US citizens and non-US citizens that are physically located within the Brookline Police Department's jurisdiction. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational and policy constraints exist when a law enforcement officer addresses a public citizen. Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The article does not indicate that the system would be used with any additional biometric or information systems. However, it will use localized wireless networks to transmit the data.

7.3.3 Texas: Collin college--BIO-Key's MobileCop to Provide Wireless Query System[24]

Summary: In 2009, the Collin College deployed the BIO-Key MobileCop solution. MobileCop allows officers the option to run fingerprint checks on individuals as well as communicate via a silent messaging system to the privacy of students involved in incidents.

Technology: The MobileCop is a wireless query and messaging system that utilizes mobile data and wireless technology to provide real-time data retrieval for law enforcement officials at remote locations. With the MobileCop, officers have the ability to retrieve motor vehicle, warrant and criminal history information.

Operators/Subjects: Operators include law enforcement officers of the Collin College Police Department. Subjects include students, staff, faculty, and other individuals located on the Collin College campus. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational and policy constraints exist when a law enforcement officer addresses a public citizen. Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The article does not indicate that the system

[24] http://bio1.com/projects/texas-collin-college-%E2%80%93-bio-key%E2%80%99s-mobilecop-provide-wireless-query-system

would be used with any additional biometric or information systems. However, it will use localized wireless networks to transmit the data.

7.3.4 Alaska: Soldotna Alaska police--PocketCop Mobile Data Solution[25]

Summary: The Soldotna Alaska Police Department has issued BIO-key's PocketCop mobile data solution for law enforcement applications to its patrol officers and command staff. As part of the mobile solution, each officer is issued a BlackBerry smartphone that provides the holder with wireless voice communications, email and Internet access. Additionally, the PocketCop enables each officer to query the Alaska Public Safety Information Network (APSIN), National Law Enforcement Telecommunications System (NLETS) and the FBI's National Crime Information Center (NCIC). Prior to the deployment of BIO-key's PocketCop, officers were required to call the regional dispatch center over the radio and wait for returned results when requesting background information on a vehicle or person of interest. PocketCop provides law enforcement officers with the ability to access federal, state, and local criminal records as well as adding fingerprint identification, imaging, automatic vehicle location, and global positioning functionalities.

Technology: The PocketCop is a handheld software application that allows law enforcement officials to retrieve information at remote locations in real-time. Using commercially available mobile phones such as BlackBerry, the application allows officers to receive information directly from an agency's computer-aided dispatch system and send status reports to dispatch. Additionally, it can be customized to enable officers to access information from federal, state and local criminal databases.

Operators/Subjects: Operators are the law enforcement officers of the Soldotna Alaska Police Department. Subjects are private citizens located within the Soldotna Alaska Police Department jurisdiction. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it is found that the subject has an outstanding warrant.

Constraints: Operational and policy constraints exist when a law enforcement officer addresses a public citizen. Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The system must be interoperable with APSIN, NLETS, and FBI NCIC systems.

7.3.5 USG: FBI- Mobile ID/RISC[26]

Summary: In the fall of 2011, the FBI CJIS[27] Division will implement the Repository for Individuals of Special Concern (RISC) Capability as part of the Next Generation Identification Increment 2. This milestone will deliver the majority of the functionality planned for the RISC Rapid Search capability. The RISC capability is a fingerprint technology that will allow law enforcement officers rapid identification of individuals and checks them against databases comprised of wanted individuals, registered sex offenders, suspected terrorists, and other persons of special interest.

---

[25] http://bio1.com/projects/alaska-soldotna-alaska-police-%E2%80%93-pocketcop-mobile-data-solution

[26] http://bio1.com/projects/usg-fbi-mobile-idrisc

[27] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/repository-for-individuals-of-special-concern-risc

Technology: Increment 2 supports both RISC rapid searches received as a Simple Mail Transfer Protocol (SMTP) Electronic Biometric Transmission Specification (EBTS) request or an Extensible Markup Language (XML) EBTS Web Services request.

Operators/Subjects: Operators include federal, state, and local law enforcement officers. Subjects can include US citizens and non-US citizens. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it be found that the subject has an outstanding warrant.

Constraints: Operational and policy constraints exist when a law enforcement officer addresses a public citizen. Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The article does not indicate that the system would be used with any additional biometric or information systems. However, it will use localized wireless networks to transmit the data and would likely be interoperable with existing FBI biometric and information systems.

7.3.6 Virginia: Virginia Law Enforcement Agencies-Remote Fingerprint Identification System[28]

Summary: Law Enforcement Agencies in Virginia plan to deploy BIO-key's software-based MobileCop application to enable patrolling officers the ability to conduct remote fingerprint searches and identification. The initial deployment of the mobile identification system will equip 110 patrol units with the appropriate hardware and BIO-key's MobileCop software. Of these units, Patrick County Sheriff's Office will be one of the first agencies to receive the technology upgrade.

Technology: The MobileCop is a wireless query and messaging system that utilizes mobile data and wireless technology to provide real-time data retrieval for law enforcement officials at remote locations. With the MobileCop, officers have the ability to retrieve motor vehicle, warrant and criminal history information. Additionally, it can be integrated with legacy devices such as computer-assisted dispatch (CAD) or records management systems (RMS).

Operators/Subjects: Operators will include law enforcement officers in the state of Virginia. Subjects include US citizens and non-US citizens that are physically in the jurisdiction of Virginia law enforcement agencies. The goal is to obtain the subject's exact identity to check it against criminal databases. The subject may be able to opt-out of identity proofing; the police bureau's policy would need to address that specific issue. Operational requirements dictate that the process be efficient to address time constraints. Biometric reference data will exist if the subject is a match in any of the criminal databases examined. PII should not be retained after the encounter. If necessary, PII can be shared with other federal, state, and local law enforcement agencies if it be found that the subject has an outstanding warrant.

Constraints: Operational and policy constraints exist when a law enforcement officer addresses a public citizen. Operational constraints exist due to the operational environment. Use of the device can occur indoors/outdoors and in remote locations leading to possible connectivity issues. The device does have weather proofing that may mitigate environmental factors. The article does not indicate that the system

[28] http://bio1.com/projects/virginia-virginia-law-enforcement-agencies-%E2%80%93-remote-fingerprint-identification-system

would be used with any additional biometric or information systems. However, it will use localized wireless networks to transmit the data.

8 Office of the Privacy Commissioner Analysis

8.1 Privacy Analysis

OPC Reference Documents

1. Data at Your Fingertips: Biometrics and the Challenges to Privacy. 2011. Available from http://www.priv.gc.ca/information/pub/gd_bio_201102_e.cfm
2. A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century. 2010. Available from http://www.priv.gc.ca/information/pub/gd_sec_201011_e.cfm
3. OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities. March 2006. Available from http://www.priv.gc.ca/information/guide/vs_060301_e.cfm
4. Guidance on Covert Video Surveillance in the Private Sector. Available from http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.cfm

8.2 Key Privacy Protection Concepts

Our reference document titled A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century provides a general analytical framework that we use when considering privacy and security issues. We suggest that this framework should also be applied in any program considering the use of portable biometrics. The framework outlines four general steps: conception, design, implementation, and evaluation. The main elements of these steps are outlined below:

1. Making the case, the Oakes test
   1.1. **Necessity**: there must be a clearly defined necessity for the use of the measure, in relation to a pressing societal concern (in other words, some substantial, imminent problem that the security measure seeks to treat),
   1.2. **Effectiveness**: the measure must be shown to be empirically effective at treating the issue, and so clearly connected to solving the problem
   1.3. **Proportionality**: the measure (or specific execution of an invasive power) must be carefully targeted and suitably tailored, so as to be viewed as reasonably proportionate to the curtailment of the privacy (or any other rights) of the individual being subject to the measure,
   1.4. **Minimal intrusiveness**: the measure must be the least invasive alternative available (in other words, ensure that all other less intrusive avenues of investigation have been exhausted).
2. Applying the Fair Information Principles
   2.1. Designing for privacy
   2.2. PIAs and TRAs
3. Ensuring compliance through effective privacy management
4. Ongoing review and oversight

We refer readers to the document for a full explanation of each of these steps. In addition, we have provided specific guidance about biometrics and privacy in our reference document titled Data at Your Fingertips: Biometrics and the Challenges to Privacy. Key points made in that document include:

- biometric data is personal information (as applied in PIPEDA and Privacy Act)
- apply the Oakes test (see above) and demonstrate how each requirement is being met

- some privacy protection principles for biometrics
    - summary information versus raw samples
    - template protection and single-purpose applications
    - verification instead of identification, when possible
    - local storage instead of central database, when possible

• other privacy issues: covert collection, cross-matching, secondary information

We refer readers to the document for a full discussion of these points.

8.3 Assumptions for this Analysis

When considering the use of portable biometric devices in the scenarios that have been described, we make the following assumptions:

- programs related to national security require special attention, see our Matter of Trust paper
- programs that use biometrics require special attention, see our Biometrics Guidance paper
- biometric characteristics are personal information that is especially sensitive because:
    - it can be a universal, permanent identifier (cannot be replaced)
    - it can be used in multiple applications with serious real-world implications, such as border control and forensics
    - solutions for safe use and storage of biometric information are in their infancy
- if a Canadian government entity collects and/or processes biometric information, then it is subject to the Privacy Act, regardless of the citizenship or status of the data subject
- large scale databases of biometric information introduce risks, such as misuses, data breaches, and decreased matching performance (false matches) that increase as the database grows. It is our view that large databases should be avoided and, instead, local storage and/or small special-purposes databases should be used wherever possible.
- portable biometric systems raise additional concerns, including: possible reduced performance due to technical limitations, security of data held in devices, security of data transmission.
- Portable biometric systems increase the risk that biometric information will be collected covertly, with the associated privacy and civil liberty risks

The following key privacy-protection issues should be considered for portable biometrics:

8.4 Key Issue: Collection

All of the scenarios involve the collection of biometric information, even if the "collection" is for the purposes of verifying identity and the collected data is immediately destroyed.

• collection of biometric information should be limited to what is absolutely necessary for the identified purpose(s)

• the purpose(s) for the collection must be disclosed to the data subject at the time of collection, and consent should be obtained

8.5 Key Issue: Safeguarding

• the program owner would have to demonstrate how any additional risks being taken through the use of portable devices, databases, and/or data transmissions are offset by benefits. An analysis should examine why any extended collection and use of biometrics is necessary and appropriate. Also, they must consider why using stationary biometric devices, perhaps housed at police stations, are not adequate for the tasks.

• normally, we would recommend that biometric information be stored in local devices instead of centralized databases, but it is not clear if this is appropriate in the scenarios that have been described. The possibility of loss or theft of the portable devices may lead one to prefer a configuration with no local storage, as long as safe (secure) transmission capabilities can be put in place.

8.6 Key Issue: Sharing

- The scenarios involve the sharing of biometric information within Canada with various agencies involved with national security (e.g., RCMP). This sharing should be limited to what is absolutely necessary and governed by appropriate agreements and procedures. The purpose and extent of the sharing must also be disclosed to the data subjects at the time of collection.
- The scenarios sometimes involve the sharing of biometric information outside of Canada with various partner countries (e.g., USA). This sharing should be limited to what is necessary and governed by appropriate agreements and procedures, including arrangements for reporting and auditing. There must be strong limits on how other countries can retain and use the information provided by Canada, and how Canada retains and uses information provided by other countries. The purpose and extent of the sharing must also be disclosed to the data subjects at the time of collection.

9 Example Use Cases and OPC Privacy Analysis

The following includes potential mobile use cases, and commentary from the Office of the Privacy Commissioner.

The material presented below should be treated as informal material for information and discussion, and not the official position of the Office of the Privacy Commissioner. Opinions or rulings from the Commission may differ depending on specific cases and facts that it might examine. The scenarios that have been described represent different legal contexts where there may be different expectations of privacy, and different laws and regulations that apply. The privacy impacts of any particular use of biometrics will depend on many factors, so deployments would have to be considered on a case-by-case basis.

9.1 Use Case 1: Afghani Biometric Collections

Use Case Name and Brief Description
Afghanistan Counter-Insurgency. The Canadian Forces (CF) joined the International Security Assistance Force (ISAF) biometric program in the war on terror, through December 2011. CF continues to support its allies and international partners through NATO Training Mission-Afghanistan.

Agency/Operators
Which agency does the mobile device operator represent?
Canadian Forces.
What is the operator's role within the agency?
Soldier.

Subjects
Which populations may be subject to identity proofing?
[ ] Canadian Citizens [ ] Legal Canadian Residents [ ] Non-Canadian Residents [X] Other Afghani Residents
What identity information is required to perform the agency's mission?
[X] Subject's exact identity. [ ] Inclusion in a "access list" or "white list" for benefits or access Describe _____ [X] Inclusion in a "watch list" or "black list" for public security Describe United States DoD maintains relevant Biometrically Enabled Watch Lists (BEWLs) [ ] Other _____

Operational Constraints
Describe the collection environment (e.g. indoors/outdoors, checkpoint/office):
Outdoors, hostile and austere environment, wide range of operating temperatures.
Describe the area of operations (e.g. room, building, city, province)
Devices are used throughout Afghanistan.
Would the device be used with any existing biometric systems?
The HIIDE and SEEK devices are used in conjunction with ISAF's biometric systems in theaters. Devices pass enrollments and searches to the US's BAT biometric system in theater.
Would the device be used with any existing information systems?
Are communications systems or networks available (e.g. LAN, WiFi, Tactical Radio)?
Tactical Radio. Devices may use comms available at Operating Bases when patrol returns.

Identity Operations
Which identity functions are required to support your mission?
[X] Enrolment/Record Retention [X] Identification (1-to-many) [ ] Verification/Authentication Do subjects claim an identity? How (e.g. ID Card)? _____
Can subjects opt-out of identity proofing?
[ ] Yes [X] No [ ] Partially (explain) _____
Are there operational or policy requirements for response time?

Data Sharing
Does biometric reference data already exist, in house or at other agencies?
[ ] Identity Document(s) _____ [X] Biometric Database(s) DoD ABIS, FBI IAFIS, DHS IDENT _____
Is any biometric or personally identifiable information (PII) retained after encounter?
[X] Encounter record includes PII [X] Biometric enrolment [X] Biographic enrolment [ ] Other _____
Is information shared with Canadian or Foreign agencies? Which? Is PII shared?
Yes, biometrics and PII are shared with ISAF, including United States.

9.1.1 OPC Commentary

In the case of the use of biometrics by the Canadian Forces, it is our understanding that while the Canadian charter may not apply during off-shore operations, the Privacy Act does apply. Anytime a Canadian federal entity collects and processes personal information we would expect that Privacy Impact Assessments (PIAs) be conducted for any new or substantially changed programs, and these PIAs would be submitted to our office.

9.2 Use Case 2: Law Enforcement Identification

Use Case Name and Brief Description
Law Enforcement – situational awareness and "most wanted" search. Biometric capability added to any current scenarios where officer may legally request proof of identity. Primary use case is Traffic Stops in accordance with federal, provincial, and local legislation.

Agency/Operators
Which agency does the mobile device operator represent?
Local or Provincial Law Enforcement
What is the operator's role within the agency?
Officer

Subjects
Which populations may be subject to identity proofing?
[X] Canadian Citizens [X] Legal Canadian Residents [X] Non-Canadian Residents [ ] Other _____
What identity information is required to perform the agency's mission?
[ ] Subject's exact identity. [ ] Inclusion in a "access list" or "white list" for benefits or access Describe _____ [X] Inclusion in a "watch list" or "black list" for public security Describe KST and "most wanted" [ ] Other _____

Operational Constraints
Describe the collection environment (e.g. indoors/outdoors, checkpoint/office):
Indoors and outdoors.
Describe the area of operations (e.g. room, building, city, province)
Anywhere within jurisdiction
Would the device be used with any existing biometric systems?
Potentially local AFIS; RCMP RTID AFIS
Would the device be used with any existing information systems?
Yes, existing identity and warrants systems
Are communications systems or networks available (e.g. LAN, WiFi, Tactical Radio)?
Tactical Radio is available; WiFi may be available; dedicated 3G may be available.

Identity Operations
Which identity functions are required to support your mission?
[ ] Enrolment/Record Retention [X] Identification (1-to-many) [X] Verification/Authentication Do subjects claim an identity? How (e.g. ID Card)? Could claim with ID card_
Can subjects opt-out of identity proofing?
[ ] Yes [X] No [ ] Partially (explain) In line with existing policies on mandatory identification
Are there operational or policy requirements for response time?
Determined by jurisdiction; generally cannot cause temporary detention to become permanent.

Data Sharing
Does biometric reference data already exist, in house or at other agencies?
[X] Identity Document(s) Provincial Driver's License (Face) [X] Biometric Database(s) RCMP RTID
Is any biometric or personally identifiable information (PII) retained after encounter?
[X] Encounter record includes PII [ ] Biometric enrolment [ ] Biographic enrolment [ ] Other
Is information shared with Canadian or Foreign agencies? Which? Is PII shared?
RCMP

Additional Comments
Traffic stops may be supported by two distinct use cases: • 1-to-few watch list searches to identify subjects with outstanding warrants (Fingerprint and Face). • 1-to-1 biometric verification against a driver's license (Face)

9.2.1 OPC Commentary

In the law enforcement scenario, which envisions the use of biometrics during traffic stops by police, there is a collection of jurisprudence and a history of charter rights concerns that should be examined. Further, the legal status of demands for proof of identity would have to be considered. Does the collection of biometrics without probable cause represent an unreasonable search that is analogous to the search of a glove compartment in a car? Since drivers already must carry license documents, why are these insufficient as a proof of identity? The possible covert collection of biometrics, such as the automatic collection of face images by cameras in police cars, also raises potential legal and privacy concerns. We have provided background documents on covert video surveillance that would be useful to review here. In general, data collection without knowledge and consent should be avoided.

9.3 Use Case 3: Transportation Access Screening

Agency/Operators
Which agency does the mobile device operator represent?
Transport Canada
What is the operator's role within the agency?

Subjects
Which populations may be subject to identity proofing?
[X] Canadian Citizens [X] Legal Canadian Residents [X] Non-Canadian Residents [ ] Other _____
What identity information is required to perform the agency's mission?
[ ] Subject's exact identity. [ ] Inclusion in a "access list" or "white list" for benefits or access Describe _____ [X] Inclusion in a "watch list" or "black list" for public security Describe Banned passengers (consolidated list does not yet exist); any relevant Watch list [ ] Other _____

Operational Constraints
Describe the collection environment (e.g. indoors/outdoors, checkpoint/office):
Indoors, Office and public transportation environments
Describe the area of operations (e.g. room, building, city, province)
Would the device be used with any existing biometric systems?
No
Would the device be used with any existing information systems?
Are communications systems or networks available (e.g. LAN, WiFi, Tactical Radio)?
WiFi is available

Identity Operations
Which identity functions are required to support your mission?
[ ] Enrolment/Record Retention [X] Identification (1-to-many) [ ] Verification/Authentication Do subjects claim an identity? How (e.g. ID Card)? No Identity System.
Can subjects opt-out of identity proofing?
[ ] Yes [ ] No [ ] Partially (explain) Not defined
Are there operational or policy requirements for response time?
Cannot impede passenger flow

Data Sharing
Does biometric reference data already exist, in house or at other agencies?
[ ] Identity Document(s) _____ [ ] Biometric Database(s) _____
Is any biometric or personally identifiable information (PII) retained after encounter?
[ ] Encounter record includes PII [ ] Biometric enrolment [ ] Biographic enrolment [ ] Other _____
Is information shared with Canadian or Foreign agencies? Which? Is PII shared?
Possible sharing with RCMP as holder of biometric database, depending on policy.

9.3.1 OPC Commentary

In the transport scenario, the actual context of use will be important. For example, would biometrics only be used for international travel, or for domestic travel? The privacy expectations and rights are very different in these two contexts. Also, would a biometric program become part of a no-fly activity or a way of checking for repeated immigration violations? Would a biometric system be used to confirm or clear people who are close matches based on names in a watch list? Also, in a border control context, will sharing of biometric information with international partners act to limit global mobility for individuals or groups? Covert collection and use would also be a concern in this context.