U.S. Department of Justice's
Global Justice Information Sharing Initiative

Global Justice Information Sharing Initiative
United States Department of Justice

Privacy and Information Quality Risks: Justice Agency Use of Biometrics

Introduction

As the use of biometric technology expands and diversifies, justice agencies need to ensure that their policies regarding the collection, accuracy, use, sharing, and retention of biometric information address privacy, civil liberties, civil rights, and information quality concerns. Failure to adopt and implement appropriate policies and procedures can result in serious consequences for the agency as well as the individuals involved.

Has your justice agency adopted or is your agency considering adopting some form of biometric technology?

Are you concerned about whether your agency has adequate privacy and information quality policies that cover the collection, use, sharing, and retention of information derived through various biometric technologies?

The following information is intended for those who answered "yes" to either of these questions, are new to the subject, and who have some responsibility for overseeing the use of biometric technology. This primer introduces several of the major issues that arise in the collection and use of information derived from the use of biometric tools.

Biometric Technologies and the Justice System

Biometrics can be defined as measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition. Biometric technology is commonly used in the justice system for:

- Verification—confirmation of a person's identity (are they who they say they are?).
- Human identification—determination of a person's identity (who is this?).

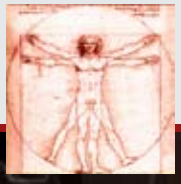
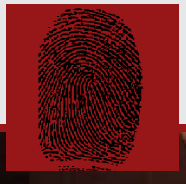
Biometric tools can be used for identification in both an administrative and an investigative capacity.

There are many types of biometric systems available for use in a justice system. The oldest and most common modalities are fingerprints and palm prints. Examples of newer forms of biometrics include DNA, facial recognition, iris recognition, retina scan, voiceprint, and hand geometry.

Although many new technologies are being developed, there are already legal precedents regarding the use of biometrics in the justice system. It is important to note that none of these systems are infallible but that implementation of proven policies and practices can reduce the risk of negative impacts as well as improve the success of your agency.

Justice Agency Framework for Understanding Privacy Risks in Biometrics

The management of biometrics information in a manner that respects privacy, civil rights, and civil liberties requires organizations to address specific questions surrounding the collection, retention, use, and sharing of biometric information. Indeed, the fact that the physical person is the source of the information creates even higher expectations for the protection of privacy. For example, the manner of collection can be pivotal. The mass collection and retention of biometric data, such as scanning all faces in a crowd without the knowledge or consent of the individuals, raises somewhat different concerns about privacy than perhaps a program that collects biometric information from individuals one at a time after obtaining their consent. In addition, mass collection and retention undertaken as a proactive preventive task—rather than as a response to a predicate criminal act—creates the potential for discovering more information than is needed, exacerbating privacy concerns. The risk is also higher for biometric data than for more traditional types of personal information because the data collected could be used for a purpose beyond that which justified the initial collection (for example, finding a suspect rather than just verifying identity).


Justice Agency Framework for Understanding

Privacy Risks in Biometrics

Justice agencies should identify and consider the range of risks and other practical considerations when developing a privacy policy for biometric-based tools. Consider the following factors when developing or evaluating a biometric technology program in your agency.

Lesser need for privacy protections		**Greater need for privacy protections**
Specific collection in response to an incident	**1. What is the purpose for the data collection?**	Generalized collection for prevention
Overt notice and collection	**2. What notice is given to those about whom information is being collected?**	Covert collection; no notice
Optional; consent required	**3. Is the collection optional or compelled?**	Compelled or consent implied
Verification of identity (one-to-one)	**4. Is the system used for identification or verification?**	Identification (one-to-many)
Collection for a fixed or finite period	**5. Is the system deployed for a fixed period of time, such as a special event?**	Ongoing or indefinite collection
Not stored or stored temporarily	**6. Where and for how long will biometric data be stored?**	Stored indefinitely
Individual, customer	**7. In what capacity is the user interacting with the system?**	Employee, citizen
Subject of the information	**8. Who is in possession of the personally identifiable information? Who maintains the information?**	Someone other than the subject
Available only to authorized users in a controlled setting	**9. Who has access to the information? How many people potentially have access?**	Available to the public generally or through a business service
Laws limiting access, use, or disclosure	**10. What restrictions are there on use of information or disclosure of information?**	No formal restrictions
Information is maintained in a secure environment	**11. How secure is the storage of the information?**	Information is maintained in an environment subject to leaks, hacking, and accidental disclosure or modification
Information is maintained in a secure format	**12. In what formats is the information stored and how secure are these formats?**	Information is maintained in an easily read format
Information is exchanged in a secure transmission	**13. How secure is the transmission of the information?**	Information is transmitted over unsecured or public channels or in unencrypted format
Representation derived from mathematical or physical analysis	**14. What type of analysis is used to generate representations of the original biometric information?**	Behavioral interpretation of original information
Only derived representations used	**15. Is the original biometric information used, or are representations derived from the original information used—or both?**	Original and derived representations

Source: Leveraging the *BioPrivacy Application Impact Framework*, developed by the BioPrivacy Initiative, International Biometric Group (IBG), GPIQWG developed justice-focused privacy and information quality risk frameworks.

Justice Agency Framework for Understanding

Information Quality Risks With Biometrics

Information quality is central to the implementation of effective biometric systems. A number of factors influence the quality of the biometrics information used within the justice system. Look at these considerations to determine to what extent your justice agency may be at risk regarding information quality issues.

Reduced risk of information quality problems		Greater risk of information quality problems
Regular and documented calibration and maintenance schedule consistent with vendor recommendations	**1. Maintenance of biometric equipment**	Inconsistent or nonexistent calibration or maintenance schedule
Standardized and effective chain-of-custody procedures with formal training programs established	**2. Collection of biometric information**	Inconsistent collection procedures, multiple levels of custody, and inadequate training
Automatic point-of-entry enrollment	**3. Enrollment of biometric data into justice systems**	Poorly edited data entry, delayed data entry, or data entry on disparate systems
Retain the original image and have standards for conversion (consistent with vendor recommendations)	**4. Conversion of a biometric into a digital format**	No standards in place for conversion or conversion is inconsistent with vendor recommendations
Documented process for confirming quality of linkage prior to linking biometric data to personal information (criteria specified)	**5. Linking biometric data with an individual's personal information**	No standards in place for biometric linking to personal information
Adequate resources, formalized audit program, and frequent recertification	**6. Staff operating the collection, retention, and sharing of biometric information**	Inadequate fiscal and personnel resources and no program certification or audits
National or industry standards, accreditation, and certification	**7. Standards for the retention, use, and transmission of biometric information**	No nationally recognized accreditation or certification standards

How Can You Reduce Privacy and Information Quality Risks?

- Identify current case law, statutes, regulations, and policies that govern the collection and use of biometric information.
- Acknowledge the social and cultural context that affect people's privacy expectations regarding the information being collected and how it will be used.
- Adopt standards and protocols for collection and maintenance of information that ensure information quality and integrity.
- Ensure that you have solutions that adequately establish and control information quality and access.
- Determine who will collect, analyze, and store biometric information.
- Determine how long your agency can retain biometric information and develop retention policies.
- Determine whether the biometric would fall under open records laws and any needed policy changes.
- Identify the circumstances, including interstate, under which you are authorized, capable, and willing to share biometric information.
- Decide whether you will allow individuals to ask whether your agency has biometric information about them and whether they can see and object to your agency's keeping the information.

CAUTION!

Do not assume that an existing policy (for example, on fingerprints) will automatically apply to other biometric technologies without a thorough assessment of similarities and differences of biometrics, regulations, etc.

Sample Scenarios

Biometric information can be very useful in identifying people and suspects. It can also lead to unfortunate failures and unintended consequences. The following examples illustrate both the benefits and problems that can arise from the use of biometric information in the justice system.

Scenario 1

Police discovered the bodies of two men who had been shot in the back of the head and left in a cemetery. One of the men had a driver's license on him, but the second man had no form of identification. Since the first 24 hours are most critical in a homicide investigation, a patrol officer with a mobile fingerprint scanner was summoned to the scene. Within a few minutes, the second man was identified. An arrest was made within days. Without the device, the second man might have gone unidentified for 36 hours while an autopsy was conducted. The appropriate use of a portable biometric device by a trained officer resulted in a quicker arrest of a suspect.

Scenario 2

A state commission approved modifications to a DNA data bank implementation plan to allow forensic laboratories to provide information to law enforcement agencies on partial DNA matches. The regulations and implementation plan were designed to ensure that the policy is applied fairly and in accordance with accepted scientific procedures and constitutional safeguards. The new regulations initially did not permit "familial searching" or singling out particular families and actively searching their DNA profiles. The care taken to develop the policy raised the credibility and legitimacy of the use of the database by local law enforcement. If the program were expanded to allow familial DNA searches, the regulations and implementation plan would have to be revised to address additional concerns raised by the expansion.

Scenario 3

A 25-year-old hospital technician was charged with the burglary of a cell phone store based on a law enforcement agency's investigation of erroneous latent fingerprint identification. Inadequate training, poor supervision, and staffing shortage (causing work overload) were given as the reasons for the misidentification. Although the automated system functioned as designed, the staff did not properly gather or analyze the evidence.

Scenario 4

A police department arrested an individual based on a pair of name-based warrants even though the subject advised the officers that a relative who had been arrested originally had supplied the subject's information to the arresting agencies. When the subject was booked with the Livescan device, the returns showed a state criminal identification number that was not the same as the one listed on the warrants. No one noticed the error, and the subject's claims of innocence were ignored. When the subject went to court, the protests were again ignored and the individual was remanded to the custody of the sheriff. When the subject again went to court, he again claimed the mistaken identity and a fingerprint examiner was called in. The examiner determined that the person in custody was not the person originally arrested. Although the equipment worked correctly and the collection was proper, the interpretation of the results was incorrect. A lawsuit is pending.

About Global

DOJ's Global serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. For more information on Global, refer to www.it.ojp.gov/global.

Additional Research and Resources

The U.S. Department of Justice (DOJ) and Global Justice Information Sharing Initiative (Global) member organizations are committed to helping you to reduce the privacy and information quality risks associated with justice agency use of biometrics. DOJ's Global Privacy and Information Quality Working Group (GPIQWG) plans to develop and make available additional biometric resources for the justice and public safety communities in an ongoing commitment to improve the collection, analysis, storage, use, and dissemination of biometric data. Additionally, biometric-related privacy resources that may be useful to your agency can be located at www.it.ojp.gov/biometricsprivacy.

www.it.ojp.gov/biometricsprivacy