INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

FOR DISCUSSION PURPOSES

IBIA Privacy Best Practice Recommendations for Commercial Biometric Use

EXECUTIVE SUMMARY

This IBIA document has two (2) parts:

- IBIA best practice recommendations for **commercial** applications of biometric technology incorporate the following essential findings:
    - Transparency and protection of data are IBIA's fundamental privacy tenets.
    - The biometric industry lacks any legal authority to impose rules of conduct on users of the technology and the industry, therefore can only **recommend** best practices.
    - Given the variety and numerous existing uses, as well as potential uses, it is not feasible or practical to develop specific /detailed practices.
    - The general guidelines are intended to provide a roadmap that will enable users and customers to tailor appropriate privacy practices to their specific contexts.
- IBIA findings and perspective on privacy risks in the digital age that form the basis for its recommended best practices. The key findings are:
    - Privacy is vulnerable to abuse by many means and methods in our digital age.
    - IBIA's primary privacy policy is that all data should be protected.
    - The level of protection should be consistent with the level of risk associated with its use and the consequences of abuse. The level of protection should also be applicable and tailored per the context of the specific biometric use.
    - The easy availability online and offline of vast amounts of detailed personal information is the greatest privacy risk.
    - The pervasive privacy risk in our society is the result of the advent of the digital age and big data and is completely independent of biometric technology, let alone a single modality.
    - As has been the case throughout human history, new methods of authenticating identity are necessary to augment existing conventions and meet current needs. Today,

biometric technologies do this and, as a major privacy-enhancing technology, preserve privacy at the same time.

- The commercial application of these best practices enhances and strengthens personal privacy protections.

These findings, coupled with the Fair Information Practice Principles[1] of transparency and protection of data and the reality of numerous and diverse biometric applications, provide the framework for implementing biometric technologies in commercial applications. Specifically, the IBIA's Privacy Best Practice Recommendations for Commercial Biometric Use incorporate general guidelines for commercial use of biometrics, leaving it to implementers and operators to determine what is most appropriate given the application, the risk and consequence of abuse, the non-biometric data used, and the purpose of the undertaking.

[1] http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf

FOR DISCUSSION PURPOSES

IBIA Privacy Best Practice Recommendations for Implementers of Commercial Biometric Identification Technology

These best practice recommendations build on the IBIA findings and perspective that are summarized below and the Fair Information Practice Principles,[2] notably transparency and protection of data. They are intended to provide core principles for how these data tools are implemented. They are built upon the premise that implementation is strictly contextual as determined by the risk and consequence of abuse, the non-biometric data used, and the purpose of the undertaking.

Please note these recommendations do not apply to law enforcement, security, intelligence or military uses, all of which are beyond the scope of this document.

General Notice

General Identity – A general notice is recommended when biometric technology is deployed but will not be used for individual identification. An example is using facial recognition technology to just detect and count people or to estimate the gender and age of a person observing a store display (for marketing research purposes).

Individual Identity – Privacy Opting-In or Out – Individual enrollment notices are application driven, taking into consideration issues such as voluntary or involuntary enrollment, type of non-biometric personal data being captured and stored, how that data will be used, the extent of notice to individuals that will be provided, and the risks and harms, if any, this process may impose on the enrollee.

To illustrate the differences that are involved, compare:

- A social media site where one can easily opt-in by clicking a box
- An office building where entering amounts to an opt-in (anything else is impractical)
- A retail establishment with a reward program or marketing campaign, where entry alone is a base requirement for its use, or where shoplifting is of concern.

Privacy Policy Notice

We recommend that implementers and operators of commercial biometric technology publish their privacy policies and that the principles listed below be included.

Collection Limitation Principle – Identification of the type of biometric that is captured/stored and its relevance to the purpose for which it is being captured/stored; identification of the non-biometric data for that individual that is being associated with the biometric data; description of the

[2] Fair Information Practice Principles, loc cit.

period of retention (preferably a defined length) or the policy that determines the period of retention.

Purpose Specification Principle – Specification of why the information is being captured and limitation on its use to those purposes.

Data Quality Principle – Maintaining the accuracy and completeness of the data; providing a mechanism for correcting the data, including a contact point (with human attendant) for re-enrollment or data removal (IBIA believes that self-service systems for initial- or re-enrollment are susceptible to fraud).

User Limitation Principle – Limitation of access to the data to certain specified individuals or applications and restricting third party access unless disclosed and necessary to the original purpose or application as stated in the Purpose Specification or in response to a legal order.

Security Safeguard Principle – Protection of any information collected or retained (whether biometric or otherwise) with good cyber-security practices; disassociating the data to the extent allowed by the applications to limit exposures if a cyber or other privacy breach does occur; encryption of data at rest and data-in-motion to limit exposures in the event of a breach.

Openness Principle – Providing a mechanism so that users for whom data is collected can request a current record of any data retained on them.

Accountability Principle – Adhering to these best practices recommendations by maintaining audit logs sufficient to the published purposes and conducting periodic audit reviews by an independent audit.

Problem Resolution and Redress – Description of the process consumers can follow if they believe that the privacy of their personal information has been compromised; publication of the contact information for the person or organization to which such concerns should be escalated, along with possible redress options, including revocation, deletion, or change of biometrics used for identification purposes.

IBIA Findings and Perspective on Privacy Risks in the Digital Age

Following is a list of the key privacy risks that should be considered:

- Privacy in our society is vulnerable to abuse by many means and methods.
- The primary privacy risk today is the ready availability online and offline of vast amounts of detailed personal information that needs to be protected. This is completely independent of biometrics (including facial recognition).
- Privacy of our personal data has been defined and limited by the rise of the digital age that incorporates big data, completely independent of biometrics.
- Anonymity and privacy are not synonymous terms. The former is forfeited if one chooses to live in society.
- Covert surveillance methods are already widely deployed, again independent of biometrics.
- Biometric identification is filling today's void in the need for security and privacy in uses throughout the government and commercial /consumer sectors; in law enforcement and national security; protection of health care records and financial records; to prevent imposters in professional and competency testing; in computers, mobile devices, and home door locks and safes; in school lunch programs and to protect child care facilities; and to make payments at retail establishments.
- In authentication applications like physical security access control and logical security access control for computers and networks, biometrics are privacy-enhancing factors that provide higher security as well as privacy.
- In both one-to-one verification and one-to-many identification applications biometrics merely provides an identity result for the questions "are you who you claim to be?" or "who are you?" These results do not necessarily diminish privacy or profile a person. Instead, these applications can enhance system integrity through positive identification, can provide a higher level of user convenience and can augment privacy.

Biometrics: A Privacy Enhancing Technology

One fact should not be lost in this discussion. As has always been the case, new methods of authenticating identity, like biometric identification, are necessary to augment existing conventions and meet current needs. Biometric technologies do this and, as a major privacy-enhancing technology, preserve privacy at the same time.

The facial template itself, like other biometric templates, provides no personal information. Indeed, protecting the non-biometric personal information is enhanced through the use of biometric verification of identity to limit data access to only authorized persons.

Biometrics can provide a unique tool to protect and enhance both identity security and privacy and to protect against fraud and identity theft, especially as a factor in identity verification.

When your personal data are protected by access mechanisms that include one or more biometric factors, it becomes much more difficult for someone else to gain access to your personal data and applications because no one else has your unique biometric attributes. This enables legitimate access and reduces the risk that a person can steal your identity and, posing as you, collect benefits; board an airplane; get a job; gain access to your personal data, etc.

The White House PCAST report[1] on privacy and big data emphasizes the importance of using privacy-enhancing technologies and supports funding for more research on the subject, singling out the work by the National Institute of Standards and Technology (NIST) in developing biometric technology to enhance privacy. Specifically with respect to facial recognition, PCAST notes "…that facial recognition technology will allow further security and convenience" and "…[is] beginning to be practical in commercial and law enforcement applications…"

Biometric identification is filling today's void in the need for security and privacy in uses throughout the government and commercial /consumer sectors; in law enforcement and national security; protection of health care records and financial records; to prevent imposters in professional testing; in computers, mobile devices, and home door locks and safes; in school lunch programs and to protect child care facilities; and to make payments at retail establishments.

As we face new social, political, security, and economic challenges in the 21st century, it is fitting that identity assurance, the underpinnings of individual and collective security, benefit from biometric identity technologies that reflect the uniqueness of the men, women and children living in societies we strive to create and improve upon.

Privacy of Personal Data is the Key Privacy Issue Facing Society

There are two (2) types of data at issue here:

- Personal biographic data (non-biometric) – such as name, address, date of birth, sex, social security number, drivers' license numbers, cell phone geolocation, passport numbers, photographs, videos, etc.

- Biometric data – a measurable biological (anatomical and physiological) and/or behavioral characteristic that can be used for automated recognition.[2]

IBIA's fundamental privacy policy is that all data should be protected. The level of protection must, however, be consistent with the risk associated with its use and potential for abuse. Further, IBIA believes that personal biographic data (not biometric data) represents the highest risk of abuse, especially in view of the advent of big data and data aggregation, and require the highest level of protection.

[1] http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

[2] National Science & Technology Council (NSTC) definition http://www.biometrics.gov/Documents/Glossary.pdf

As the Federal Trade Commission (FTC) has noted in its recent report,[3] there is a lack of transparency about the use and abuse of the individual personal data that data brokers collect and sell. Notably, the FTC was not concerned about the collection, capture, or retrieval of that data or whether the capture, storing or retrieving of that data should require an opt-in/out process. Transparency on use of personal data is their key issue.

The primacy of protecting the privacy of personal information is further supported by the National Institute of Standards and Technology Special Publication 800-122 *"Guide to Protecting the Confidentiality of Personally Identifiable Information"*[4] and the very recent report of the President's Council of Advisors on Science and Technology (PCAST) entitled *"Big Data and Privacy: A Technological Perspective,"*[5] both of which place the risk of breach of biometric data distinctly lower than the breach of personal non-biometric data.

Also, as is evident by the recent highly publicized data breaches, non-biometric personal information is that which is most prized by data thieves. The reasons are axiomatic. The breach of biometric data does not provide the ability to establish independent identities based upon that biometric data alone. However the breach of non-biometric personal biographic data enable a myriad of false identities or applications because it provides clearly identifiable attributes to an individual.

Typically, biometric data are stored in a template[6] form that requires a corresponding algorithm to read and use the template for match comparison. Non-biometric personal data however are readable and readily usable if systems containing such data are breached, and no other protective mechanisms, like encryption, were used.

IBIA believes it is good practice to maintain a separation between the biometric and associated non-biometric personal information. In fact, it is good cyber security practice to separate data of all kinds based on levels of sensitivity, classification, and/or need-to-know. Recent cyber-breaches have revealed significant vulnerabilities when a bad actor gets access to an organization's computer system, and where

[3] http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf
[4] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
[5] http://www.whitehouse.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy
[6] The word "template" is a term of art in the biometrics industry to represent the transformation of measurements (the "metrics" part of "biometrics") of physical features of a person (e.g. facial features or fingerprint minutiae) into a digitally coded form that is designed for rapid searching and matching by computer systems. Such template forms are typically unique to different vendors of the technology, and are meaningless unless used with the associated vendor search and match algorithm for which they were coded. As such, they are not easily transferred from one system to another, especially if the systems are from different vendors. In such cases, the individuals affected need to be re-enrolled, or the original raw data needs to be "re-templated" if an individual's biometric data are to be accurately transferred to another system. This leads to inherent compartmentalization of biometric data, which enhances privacy, but inhibits interoperable transitioning from one vendor to another, as is desired for technical or monetary reasons by some users of the technology. To be sure, research exists showing that it is possible to reverse engineer templates, both face and finger, to create viable finger or face images similar to the ones used to create the templates. However, whether this is a threat or not depends on the application. Such threats can be mitigated by techniques such as liveness detection and multiple factors for verification applications, and for identification applications by encryption and basic good cyber security practices, which should be in place to protect any type of personal data.

All the data are "at the same level," and therefore equally accessible without further internal checks and balances.

In other words, IBIA believes that the real privacy issue we need to address in our society is protection of personal biographic data, rather than a disproportionate focus on biometric data associated with facial recognition or other biometric technologies.

Facial Recognition, Big Data, Anonymity, Surveillance, and Privacy

The perceptions that biometrics, such as facial recognition and templates generated from facial images, need to be regulated and strongly constrained because they will destroy anonymity and increase surveillance are more imagined than real, and pale in comparison to the other electronic methods that can be exploited in the digital age in which we live.

1) There is no anonymity if we choose to live in society. Anonymity and privacy are not the same. Unless we disguise ourselves, our faces are public. In society, many services are dependent on user identity. Routinely, data are used to offer goods and services to us. Anonymity cannot be used as a means to avoid accountability. Those who choose to opt in to personal offers are simply acknowledging that they want the benefits they might gain by giving up anonymity. Privacy is a different matter and surrendering a right to anonymity is not tantamount to a surrender of privacy.

   Contrary to public statements, simply having access to a facial image or its template does not destroy the anonymity of a person walking down the street. This does not directly reveal a name, Social Security number, or any other personal information.

   It is true that tagged photos on a social media Web site could lead you to a name or address. However, that is only one of a hundred tools that can provide the very same data. With a name alone, one can find addresses and phone numbers in public phone directories and then undertake surveillance, of a person seen on the street.

2) Surveillance is a product of the digital age, not biometrics like facial recognition. Surveillance is already a part of our daily life, thanks to the digital age and tremendous increases in computational power. Facial recognition does not increase its use.

   There are two major classes of security surveillance technology in use today.[7] One class is owned and operated by commercial businesses or individual organizations, and the other is owned or operated by local, state, or federal governments.
   Commercial businesses and other non-government organizations routinely have security cameras in and around their facilities for physical security and employee/visitor safety. Contrary to their portrayal on television programs like "24" and "Person of Interest," among others, surveillance cameras owned by various businesses and organizations are NOT uniformly or even frequently interconnected and available to anyone with an Internet connection.

[7] Security surveillance in individual homes is also common, but not germane for this discussion.

They occasionally (but rarely) run "video analytics" to automatically alert security personnel to inappropriate or unsafe activities, but almost never use automated facial recognition. If an event of interest (a crime) occurs, recordings of the event can be analyzed after the fact, and are sometimes made available to police as evidence, in accordance with the law. Images extracted from such surveillance recordings can contain faces, and these can sometimes be extracted (if the image has sufficient resolution) and converted into templates for comparison against a gallery of suspects using automated facial recognition. However, this latter process is also subject to legal rules and constraints.

There are some cities where there are a great number of centrally accessible surveillance cameras. These are of great utility in traffic management, and emergent situation assessment from a central operations center. However, resolution of the video cameras is such that they can't practically be used for continuous facial recognition technology. The possible application of facial recognition technology is therefore generally confined to post-event analysis, where resources can be focused on only video captured that is germane to the event being investigated, again, according to law.

Under either class of common security surveillance video technology, it isn't practical or possible to conceive of a "face stalking" application that can be accessed and run across all the video cameras in a surveillance system. Stalking, although thankfully infrequent, occurred before the advent of facial recognition technology, and unfortunately will continue to occur, whether facial recognition becomes a factor or not. To this point, facial recognition technology has not been a factor, and likely will continue to be a non-factor for stalking.

3) Privacy in the digital age. People are entitled to privacy of their personal data. However, privacy of our personal data is constricted and defined by the digital age and big data, not by a biometric technology like facial recognition.

   Today, our ability to restrict or control all the data about you as an individual is limited. This is evidenced by the expansive notices we receive from credit card companies, insurance companies, banks, etc., regarding an individual's rights and capacity to control their personal data. Frequently, these data are used to market to the public. Order a book or product from Amazon and you will receive a number of follow up product suggestions.

   The digital data has made us all subject to the erosion of privacy. To a very large extent, we are exposed because as individuals we voluntarily give out information about ourselves on and off-line in the emerging reality of a "big data" world. This threat is compounded by lax cyber hygiene, and the myriad of hackers trying to steal our personal information on-line. Knowingly or unknowingly, much of the population has already experienced cyber-theft of personal information in addition to what we willingly share.[8]

[8] "Consumer Reports' Survey: 62 Percent of Online Consumers Do Nothing to Protect Their Internet Privacy – 1 in 7 Notified of Personal Data Breach Last Year; Victims of eMail Phishing Scams Up 22 Percent from 2012." http://www.prnewswire.com/news-releases/consumer-reports-survey-62-percent-of-online-consumers-do-nothing-to-protect-their-internet-privacy-261063761.html