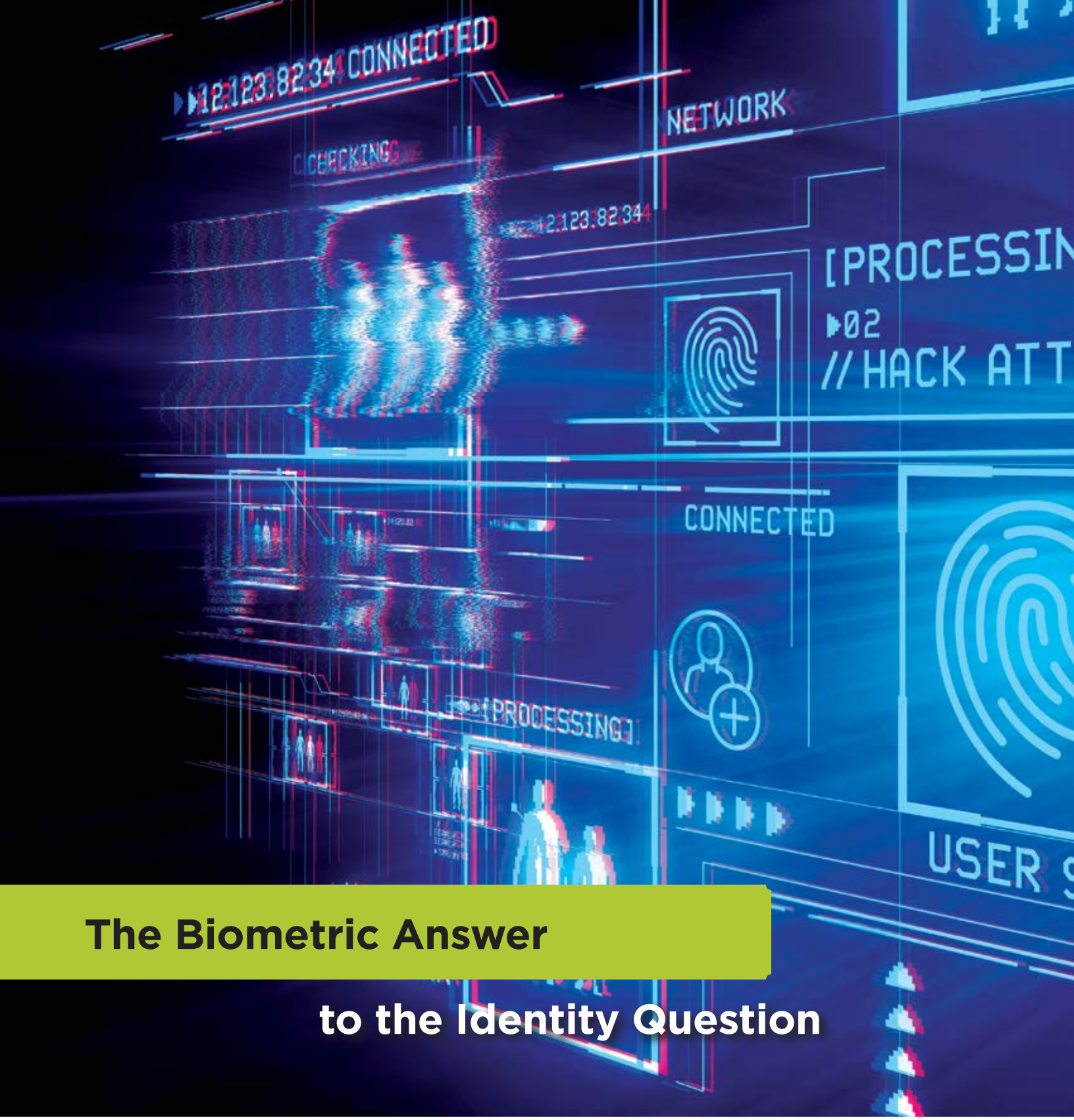

The Biometric Answer

to the Identity Question

IBIA
International
Biometrics+Identity
Association

IBIA advances the adoption and responsible use of technology-based identification solutions to enhance identity security and privacy and to facilitate convenience and productivity for government, business and consumers.

Introduction

> **"We acknowledge that many people have concerns about privacy and anonymity that are rooted in moral and legal philosophies. These are matters of opinions on which reasonable people may disagree, and should be resolved in the public sphere. Our objective in this paper is to provide facts that can help to inform conversations about biometric technology."**

As biometric technology has become more widely adopted, it has brought with it a number of questions of how the technology works. In this paper, we seek to answer those questions in a forthright manner.

We acknowledge that many people have concerns about privacy and anonymity that are rooted in moral and legal philosophies. These are matters of opinions on which reasonable people may disagree, and should be resolved in the public sphere. Our objective in this paper is to provide facts that can help to inform conversations about biometric technology.

It may be useful to address from the outset what the term biometrics means. The National Research Council, in the 2010 report "Biometric Recognition: Challenges and Opportunities," offered the definition: "Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known)—and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges)."[1]

Some historical context may also be useful. Biometrics are not a new identification technology; indeed, in a sense, biometrics are the most ancient form of identification. Since the dawn of time, human beings have recognized one another through our faces, voices, gaits, scents and so on. For thousands of years, we have known that fingerprints are a unique identifier. Before the term biometrics came into its modern usage of automated human identification, fingerprints and before that anthropometry were used by law enforcement for positive identification.

Now, as human interactions increasingly take place in cyberspace rather than face-to-face, the identity challenge has become far more vexing than it ever was to our Stone Age – and even Industrial Age – ancestors.

[1] https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities

1. Overview and Background

The Internet's Identity Problem

In the 25 years since Marc Andreessen and Eric Bina posted the Mosaic browser as a free download on the NCSA website,[2] making the Internet accessible to the general public, the way we engage with and perceive the world has in many respects changed. Before, web usage was largely confined to a colleges and universities; today 87% of U.S. adults and 40% of the world population are Internet users.[3]

Bill Gates is supposed to have originated the quote "The Internet changes everything." Perhaps he did. In any case it is true – and that includes the Internet itself. In 1993 security considerations were practically non-existent as there were few hackers, viruses, or malware, and logon was for accounting purposes if any. Yes, threats have existed since at least 1971 and the innocuous Creeper virus, but they were not regarded a significant problem.[4] Fast-forward to today and much has changed. Today our need for computer and network access control and authentication is substantial and needs no elaboration here.

In the 1960s and into the 1970s, for many systems, if you knew enough to turn on the computer, perform the bootstrap loading procedure, and operate the system you were "good to go." A written signup sheet was good enough for keeping track of users and usage. Little if anything was locked up much of anywhere. As the user population grew, and hacking evolved from humorous and mischievous to malicious and criminal, security had to be bolted on, as it had not been built in from the start. Signup sheets and (generally) professional courtesy as sole access control evolved to User ID and PIN or Password. Which worked well, and still does, for small user populations of a particular system. In May 2016 BuzzFeed News reported an Intel Security online survey of 2,000 English-speaking adults finding that the average person had 27 discrete online logons. Perhaps someone somewhere can actually remember 27 strong USERID/password combinations.[5]

[2] https://www.livinginternet.com/w/wi_mosaic.htm

[3] http://www.internetlivestats.com/internet-users/

[4] https://www.theguardian.com/technology/2009/oct/23/internet-history

[5] https://www.buzzfeed.com/josephbernstein/survey-says-people-have-way-too-many-passwords-to-remember?utm_term=.gu8E2AoJ9#.ew80N1E3m

> **"The use of biometrics by government entities is well established. What's new in just the past few years is the explosive growth of biometrics outside the governmental realm. Apple's Touch ID feature (more recently superseded by Face ID) was merely the beginning; now, companies are rolling out biometric solutions for payments, healthcare, communications, and other commercial purposes. When it comes to applying biometrics, the sky's the limit."**

Biometrics as an Answer

Enter Biometrics as a giant step forward in both convenience and security. First consider convenience. According to the same Intel Security study, 37% of people forget a password at least once a week. An April 2012 Computerworld article reported on an HDI study finding that "one-third of support centers reported that more than 30% of their tickets were related to password resets -- despite the fact that 69% of survey respondents allow customers to reset at least some of their passwords without help from the help desk."[6] Five years later there is no reason to believe that has changed. No one has ever called a help desk because they have forgotten to bring their fingerprints, face, iris, etc. to work. Use of a biometric is dramatically more convenient.

Now security. Very few people even attempt to use strong passwords. More on this later. Password cracking software can dispose of even strong passwords in seconds to minutes in most cases. So while a biometric in place of a password is not a perfect solution, it is for most a far more effective solution than a password. What has delayed adoption until recently is the cost of the biometric sensor. With introduction of the iPhone 5S in September 2013, that rapidly changed.[7] More on this topic too later. For now let it suffice that biometrically enabled access control offers greater security and dramatically improved convenience over prior practice.

Of course, biometrics are useful and used for far more that computer and network access. In law enforcement, fingerprints are used across the world for insuring the accurate association of criminal history records with the subject of the records, for wanted person apprehension, and for criminal investigation when latent fingerprint impressions are left at crime scenes. Mugshot galleries have been an element of crime investigation since at least 1857, when the New York Detective Police Office instituted a Daguerreotype Gallery[8], and today have advanced to automated face-matching systems with performance substantially superior to victims reviewing large mugshot collections. The military uses biometrics for force protection, access control, vetting contractors and vendors especially in conflict areas, and a host of other applications. Border control authorities use biometrics to speed air commerce, to confirm the identity of arriving visitors, and less frequently to deny entry to the unwelcome.

The use of biometrics by government entities is well established. What's new in just the past few years is the explosive growth of biometrics outside the governmental realm. Apple's Touch ID feature (more recently superseded by Face ID) was merely the beginning; now, companies are rolling out biometric solutions for payments, healthcare, communications, and other commercial purposes. When it comes to applying biometrics, the sky's the limit.

---

[6] https://www.computerworld.com/article/2502395/enterprise-applications/5-annoying-help-desk-calls----and-how-to-banish-them.html

[7] https://www.apple.com/newsroom/2013/09/16iPhone-5s-iPhone-5c-Arrive-on-Friday-September-20/

[8] https://timesmachine.nytimes.com/timesmachine/1857/12/05/78514460.pdf

2. Efficacy of Biometrics

> **"When it comes to efficacy, the relevant issue is not perfection but rather effectiveness compared to the alternatives, with cost of implementation an important consideration."**

When it comes to efficacy, the relevant issue is **not** perfection but rather effectiveness compared to the alternatives, with cost of implementation an important consideration.

The entertainment industry has featured surveillance activities, and also high-end access control and authorization, based upon human identification through biometric technology in ways fascinating, exciting, and frequently well divorced from reality. While not intended to mislead, but rather to entertain, this has led to a number of misconceptions and unrealistic expectations. Let's consider several such issues.

Biometrics Aren't Perfect...

No, they are not. The National Research Council's 2010 report made the point:

Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated.[9]

To put that statement into context, high-end commercial fingerprint matching systems have fully automated search reliability of 99.6% or better. Coupled with human examiners, which is typically done, the search reliability exceeds 99.99%. This is exceptional. Iris based matching accuracy

[9] See supra note 1

> **"Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated."**

is comparable to known source fingerprint matching. DNA based identification of unrelated persons is yet more accurate. Face matching systems, under **ideal** conditions, approach 98% reliability. High-resolution portrait-style capture under favorable lighting with no others in the frame lends itself to high accuracy searching. Speaker recognition systems are currently far less accurate than other common modalities. However, facial recognition systems very rarely are employed under ideal conditions. There are false negatives as well as false positives with all automated systems but depending upon the modality they can be made rare indeed. And for each modality, except for DNA, there are small segments of the public for which it is unsuitable, such as amputees for fingerprints, those with damaged eyes for iris, and so on.

...But Neither Is Anything Else

What the foregoing means in practice is that all biometric systems must make provision both for error resolution and for alternate recognition technology. Few of us encounter anything in their lives that is "perfect." In the world of physical security, banks with vaults and armed guards, as well as armored trucks, are occasionally robbed. Locks, including high security locks, can be "picked" and in any case the frames on the doors and gates and boxes they secure are readily breached. Personal Identity Verification (PIV) cards are both stolen and loaned to unauthorized persons. In cyberspace, security tokens are stolen and sometimes cloned, while passwords are notoriously vulnerable to hacking.

The most complex, high-security passwords are impossible for most people to remember and difficult to enter when copied from the list often stored close to the computer. In 2016, Keeper Security did an analysis of passwords leaked through data breaches. The findings were dismal. Each of the 25 most commonly used passwords was easily guessed and routinely checked as an early step in hacking tools. The most commonly used password, comprising a full 17% of the total, is "123456." "Password" was also quite popular.[10] The widespread requirement to provide username/password authentication for services not especially sensitive, wide variation in format, and demands to frequently change passwords often result in an insensitivity to security concerns where no password at all is used where possible, reuse of easily recalled passwords is routine, keeping a readily found written list is a common practice, and various other dodges are employed that defeat the already limited effectiveness of username/password schemes.

This increasingly troubling issue culminated in early 2015 in a level of frustration so great that the then Assistant to the President for Homeland Security and Counterterrorism, Lisa Monaco, announced a change in federal policy "*And fourth, we need to make cyberspace intrinsically more secure—replacing passwords with more secure technologies, building more resilient networks, and enhancing consumer protections online, to start with.*"[11]

[10] https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf

[11] https://obamawhitehouse.archives.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun

3. Privacy and Security of Biometrics

Biometrics Are Not Secret

Indeed not. The most reliable form of authentication is recognizing personal attributes, which are publicly revealed throughout our lives. But publicly revealed does not mean capable of duplication at a level of detail that could fool a typical human observer. It is quite difficult to fool biometric systems when human supervision is an element of the process. Nor is it so easy to fool unattended sensors as is sometimes asserted.

Biometrics Vary Depending on Context

Stories in the trade press of easily fooled fingerprint scanners, photographs, and high quality face masks used to foil facial recognition, along with less frequent references to contact lenses used to counter iris recognition, appear from time to time and spark alarm from some. Such stories are usually generic or address sensors on smartphones, and the implication is drawn that the criticism applies broadly. The 2010 National Research Council study also made the key point:

Biometric systems should be designed and evaluated relative to their specific intended purposes and contexts rather than generically. Their effectiveness depends as much on the social context as it does on the underlying technology, operational environment, systems engineering, and testing regimes.[12]

For virtually all government systems, including facility access, biometrics are captured by trained and vetted human attendants who verify "liveness" and visually check for attempts at concealment or subterfuge. It is not impossible, but very difficult, to defeat that simple but expensive precaution. More on this later. Government biometric scanners are high resolution devices with numerous technical features that make them far more difficult to defeat than the low cost consumer devices nearly all trade press articles focus upon.

[12] See supra note 1

> **"Biometric systems should be designed and evaluated relative to their specific intended purposes and contexts rather than generically. Their effectiveness depends as much on the social context as it does on the underlying technology, operational environment, systems engineering, and testing regimes."**

Smartphone Sensors Aren't As Secure – And That's Okay

The fingerprint sensor within the smart phone is, so far, a ¼" X ¼" device intended for 1:1 verification that the individual seeking access is indeed authorized. In the typical intended usage situation, where the smart phone owner seldom has the device out of immediate control and the phone can be wiped of information and deactivated in minutes if lost, this is pretty good protection. The manufacturers are fully aware these are not top of the line sensors, and that attacks exist that will defeat the protections, but make a tradeoff of cost versus effectiveness. The consumer marketplace will determine if this is good enough; and will punish those vendors that guess wrongly. Technology exists to ensure both actual liveness as well as authenticity. For example, it is feasible to verify that surface fingerprints correspond to the subdermal fingerprints. If the market dictates a need for such liveness detection, or more comprehensive authentication technology, the vendors will adopt it.

"Spoofing" A Biometric Is Possible But Unlikely

With a cooperating subject, consumer grade sensors, and no human supervision during presentation, it is relatively easy to learn how to collect the biometric and fabricate a spoof that will fool the sensor. Absent such conspiracy, spoofing will generally not be practical. The extreme case of compromise of a repository of high quality biometric images has the potential to be a counter-example. While at least one such compromise has been reported, there has been no indication of any such resulting spoofs existing. But the possibility points out the need in unattended operations where biometric authentication is NOT to a device under the owner's control (e.g. a smartphone) that additional proof of both liveness and authenticity should be included in the system design.

It is indeed possible to recover a fingerprint from a clean surface, or, if the hand is held just right from a high resolution digital image, create a mask, apply it over a finger, and spoof a low resolution device. But this is also a farfetched scenario for all but the very hardest of targets. No criminal or hacker will follow someone around in hopes of their depositing a print on a clean surface, then inconspicuously lift that print, then further follow them against the prospect they will abandon the device where it can be collected and exploited. It is simply not worthwhile for a criminal to gain access to a single phone.

Variations on the theme are equally unlikely. Uncooperative direct capture, that is high resolution photography of the friction ridge structure, can potentially be used for identification much like forensic identification from crime scene latent finger impressions. Utility of direct capture to produce materials for impersonation has yet to be demonstrated. Practically, such exploits depend on a willing confederate. Government applications are supervised and difficult to exploit. And the hard targets, government officials and the very wealthy, are accompanied by staff who would prevent gaining access to their personally owned and biometrically secured devices.

Very high quality whole hand flesh tone gloves with false fingerprints that work with both optical and capacitive sensors can be made. But this would require half a million dollars of equipment and highly specialized skills in exceedingly short supply. Nevertheless, R&D is underway to more effectively detect spoofing attempts, technically known as presentation attack detection, for incorporation into future systems. But for today the problem is in most cases one of sensationalism and hype rather than a true vulnerability.

> **"The biometrics industry cannot promise perfection. Instead, we hope to communicate to the public the benefits of convenience and security that biometrics offer compared to the available alternatives."**

Biometrics Can't Be Stolen if There's No Database

The argument is sometimes advanced that biometrics as an identification or authentication mechanism present a unique cause for concern. While it is always possible to revoke a username and password, it is not possible to revoke a biometric. While that is certainly true, it does not really address the issue of utility or effectiveness, for several reasons:

- Having a true copy of your biometric does not equate to being able to falsely present it and have it accepted. This is the issue of spoofing (presentation attack) addressed above. High-end sensors, perhaps augmented with additional modalities or other protections, make presentation attack impractical in most cases.
- Academic research has shown it practical to combine biometrics with other information, encrypt the result, and then store that as the reference "cancellable biometric." This cancellable reference can be matched in the encrypted domain, yet it remains impossible to recover the original biometric should the reference be compromised.
- For many purposes there is no need to have a centrally stored repository of reference biometrics to match against. This is the mechanism upon which the smart phone relies. The biometric remains on a device that never leaves the physical control of the owner. The user authenticates to a token (e.g. the smart phone) under their control, and the remaining details of the authentication "handshake" with distant systems do not include transmission of their biometrics.

There are governmental purposes - for example, criminal identification - for which a source reference will always be required. This is unavoidable, and the burden must be borne by the government of justifying those use cases, hardening the systems against technical attack, and vetting the humans with access to prevent disclosure. For commercial purposes, a strong case needs to be made to justify amassing a collection of reference biometrics in the first place. If uncollected they cannot be stolen.

Conclusion: Trust Through Candor

The biometrics industry cannot promise perfection. Instead, we hope to communicate to the public the benefits of convenience and security that biometrics offer compared to the available alternatives.

Identity Matters

International
Biometrics+Identity
Association

1090 Vermont Avenue, NW • 6th Floor
Washington, DC 20005

202.789.4452 x1309
IBIA.org