IBIA

International
Biometrics+Identity
Association

IBIA Policy Platform: A Platform for Progress

Keynote Address

By John Mears, IBIA Chairman

At connect:ID

March 11, 2020

John@IBIA.org

A PLATFORM FOR PROGRESS

1. Biometrics: Fostering a truthful, secure, convenient world
2. Privacy is a good thing
3. Blanket bans are undisciplined blunt instruments
4. Biometrics are better than humans and biographics
5. “In NIST We Trust”
6. We should have a viable national identity strategy
7. We don’t support oppressive uses of biometrics
8. Advocate for STEM and inclusion
9. Support education and outreach
10. Join the IBIA

Thank you, Mark. On behalf of the International Biometrics and Identity Association, welcome to Connect:ID 2020! When Mark asked me to make a few opening remarks, I reflected on your interests and the reasons you are here. You're probably here because biometrics, identity management technologies, applications, public understanding, resulting policies and laws are all evolving rapidly, though I'd observe often not at the same pace and certainly not consistently. You're here because of this dynamic, and the information, collaboration, and connections that Connect:ID offers, which is, after all, how it got its name.

As this is a political campaign year, at least in the U.S., we know that in those campaigns, candidates try to clarify and differentiate their positions on issues of the day by creating a "platform" with "planks" representing an approach to each issue. In an analogous fashion, I'd like to posit our own "platform" <click> to navigate the diverse and often conflicting forces that sometimes impede or propel progress as we enter the third decade of the 21st century.

1. Biometrics: Fostering a truthful, secure, convenient world

I think this is an assertion that we can all support – that biometrics and identity management foster a more truthful, secure, equitable and convenient world. If you don't believe this, find me during the course of the conference and let's discuss it.

2. Privacy is a good thing

Privacy is a good thing, and we all support it. There are many definitions of privacy, but for my purposes here I define it as the right to be left alone. For instance, I feel my privacy is invaded in the evening at suppertime when those robo-calls always seem to come in. THAT is an invasion of my privacy.

However, with regard to biometrics, we feel that there is no inherent conflict between responsible uses of biometrics and privacy. Now let's talk about what constitutes responsible uses.

In the case of Governments, for example, they are required to identify people boarding planes and crossing borders. The use of biometric technology to facilitate these processes increases the level of accuracy, and can speed the flow, but doesn't change the fundamental exchange the government is having, and is required to have, with an individual.

In Commercial applications, we advocate for best practices, documented on the IBIA website. Note that in the NTIA meetings on face recognition concluded at the beginning of 2016, the IBIA best practices were the only constructive work product that resulted. Those best practices advocate for, among other things, notice for uses of face characterization, and consent for uses of biometric identification, except for security applications.

One more hot button for me on this topic. The best biometric privacy practices are only as good as the cybersecurity framework protecting the data, and the cybersecurity hygiene practices of your IT staff. We all share the responsibility of ensuring government and commercial companies invest in and continuously evaluate their cybersecurity posture.

3. Blanket bans are undisciplined blunt instruments

Blanket bans of biometrics, mostly aimed at law enforcement, are undisciplined blunt instruments with unintended consequences. Facing a more well-financed and unconstrained criminal element, law enforcement needs all the efficient tools it can get. Forensic uses of biometrics should ALWAYS be allowed. Blanket bans may bar such uses in times of crisis (like the Boston Marathon Bombing investigation).

However, real-time uses of biometrics through surveillance techniques should be subject to court order, similar to wire-taps. This keeps us from turning into a "surveillance state" while preserving measured judicious uses of the technology.

One last point on this plank. In states like Illinois where restrictions on uses of biometrics1 have been instituted, no real benefits to the public have been shown. The Illinois law has mostly served lawyers and a litigious clientele eager to benefit monetarily – as much as $1000 to $5000 per violation, which can be a lot when a class action lawsuit is involved. In the cases that have been brought, no real harm has been shown – other than to the bank accounts of the defendants. We advocate for a uniform national use-case-specific, risk-based governance framework with preemption. That is to say that Federal laws and regulations should preempt all state and local laws that apply to biometric technologies to ensure that the current patchwork of conflicting state and local legal requirements does not continue to impede technological innovation, public safety, and public understanding of the national biometric technology market.

4. Biometrics are better than humans and biographics

Biometrics are better than humans and biographic identification techniques, enabling humans to focus on the aspects of their application or mission that they are uniquely suited to do. For instance, measured accuracy of human visual passport inspection is notoriously low, determined by some to be in the range of 80% or less. In contrast, measured performance of CBP biometric exit systems is around 99%, and the system doesn't get tired or inattentive.

5. "In NIST We Trust"

In a NIST report on facial recognition as long ago as 2018, the report noted that "massive accuracy gains are consistent with an industrial revolution associated with the incorporation of convolutional neural network-based algorithms…." In fact, today, the best algorithms can be 99.9% accurate under controlled circumstances.

Algorithms aren't capable of "bias", a human trait, but they do show demographic differentials between population subsets, similar to the way that DNA probabilities of alleles vary by population subset. The best algorithms show little difference in accuracy amongst different racial demographics. Which illustrates a point. The best, most responsible biometrics algorithm providers ensure that their labeled training data reflects the demographic mix in the populations they serve. There are, however, persistent differences in accuracy rates for males vs. females, with accuracy rates for males higher than for females.

All this said, the continuing independent NIST characterization of biometric performance across industry participants is important to an objective assessment of the technology, and allows organizations to pick the best algorithms for their applications.

However, informed reading of the NIST reports is necessary, lest one falls victim to distortions of the facts. For example, Georgetown Law, in their opposition to CBP uses of facial recognition for biometric exit, cited an average of all the accuracy results of the algorithm participants in (at the time) the most recent NIST testing and associated report. By citing an average of the very worst results added to the very best results, Georgetown gave the appearance that the whole industry had inferior accuracy results. They argued that the technology wasn't ready because it was prone to error. I've personally been through biometric exit at United at Dulles, and observed biometric entry at JFK CBP primary, and I can tell you that both are accurate and fast.

Bottom line, we must do a better job of translating the NIST reports (which are technical) to make it easier for people to understand the important facts and prevent misinformation or misunderstanding.

6. We should have a viable national identity strategy

We believe that the interests of individuals, continually growing commerce, and national well-being are served by having a national strategy and implementation plan for biometrically-enabled identity, facilitating:

- Secure social security;
- Secure Medicare and Medicaid;
- Secure Green Cards;
- eVerify through secure verification of identity and work status.

We aren't the only ones to be advocating for more secure identities for all. As an example, the Business Roundtable has an initiative to address Digital Identity Policy Challenges in the U.S. The World Bank is calling on governments to work together to implement standardized, cost-effective identity management solutions. The World Bank estimates that as many as 1 billion people world-wide do not have a legal identity, and as many as 3.4 billion have some form of identity, but have limited ability to use it in the digital world. And the U.N. has published Sustainable Development goal 16.9, asking for the provision of universal legal identity by 2030, a short 10 years away. Will the developing world achieve this goal before the developed nations? I wonder.

7. We don't support oppressive uses of biometrics

We've talked so far about things we support in our platform. Let's talk about some things we DON'T support. We don't support oppressive or discriminatory uses of biometrics and identity management. To illustrate my point, let me give a contrasting GOOD example – a use case practiced by the United Nations High Commission for Refugees. UNHCR uses biometrics to ensure that food and medicine are fairly and accurately given to war refugees. And now here's the contrast – we don't support the use of biometric technology for use by oppressive governments to target those very same refugees of war. This is one of the many great reasons that the UNHCR system is separate from any national system.

We don't support the use of biometrics as an instrument of discrimination. We don't support the use of biometrics for social profiling or to curtail free speech. And last but not least, we don't support the use of biometric systems to "stalk" people. Related to this, and as I said earlier on responsible cybersecurity, we advocate for appropriate insider threat detection techniques as a part of a comprehensive cybersecurity practice. Auditing and insider threat detection can deter and detect stalking abuses of biometric systems.

8. Advocate for STEM and inclusion

We believe in advocacy for science, technology, engineering and mathematics (STEM) and diversity inclusion initiatives. Science, technology, engineering and mathematics are the critical tools of our trade, and key to our futures. Join us in advocating for STEM careers! Reach out to your local primary and secondary schools and volunteer as a STEM speaker. Go back to your colleges and universities and talk about your professional experiences. While that's an enjoyable thing to do in any case, we have other pressing motivations for these outreach activities. As the unemployment rate has dropped, so good technical staff have become harder and harder to recruit and retain, especially clearable citizens. Do your part to "fill the pipeline" with diverse talent!

9. Support education and outreach

Advocacy for education and outreach is an industry-wide responsibility. We believe in science and the scientific method. We need to help others understand the truth that this approach reveals. Reports and studies on our industry can be very technical, but we can mitigate some of the uninformed opposition we face through better advocacy and education efforts.

Take time to speak to your local and Federal representatives and their staff to better understand their positions on topics of interest to you, and help them to understand the technology. An educated person is a better legislator or government official – at all levels.

10. Join the IBIA

Every citizen in a democracy has a responsibility to be informed so we can make good choices when we exercise our rights to help determine the future directions of our societies. We look at the platforms of our potential representatives when we make these choices. Look at this platform for our industry. If you agree and want to advocate for it, join us. If you disagree, join us and help make it better. Become a responsible advocate for our industry, and help us to amplify our voices during this critical time.

We can't face this challenge alone. We must band together to ensure our voices are heard above the noise. Join the IBIA, help us make a difference – for all of us.

#identitymatters

IBIA
International
Biometrics+Identity
Association

1325 G Street, NW, Suite 500
Washington, DC 20005

202.888.0456 | IBIA.ORG