INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

ID News Track

IBIA is pleased to provide ID News Track to its members. This daily service is prepared by Carroll & LaDier, PLLC.

Reports from connect:ID

Public concern about private ID: Biometrics and consumer acceptance

One issue came up again and again at Connect:ID, a conference bringing together experts and companies in the fields of biometric and secure identity technology. That issue is the perception that biometrics is in some way invasive to personal privacy.

When it comes to biometrics, "One of the hardest things we have to deal with in law enforcement is the public's perception of what we do. Not the reality, but the perception," said Maj. Sean Jowell, of the Pinellas County Sheriff's Office in Florida.

To many at the conference, public unease about government and even commercial use of some biometric technologies — most recently with facial recognition, for instance — was also inexplicable, or at least irrational.

But speaker after speaker recognized that perception becomes reality, with several citing the controversy underway in Florida. Lawmakers at the state assembly in Tallahassee are pushing a bill to ban the collection of biometric data in schools. The ban would kill very helpful, successful and money-saving programs in several county school systems. The bill's backers have repeatedly — and inaccurately — cited the danger of "identity theft" as a reason for the ban, and seem determined to push ahead.

"Big Brother" fears

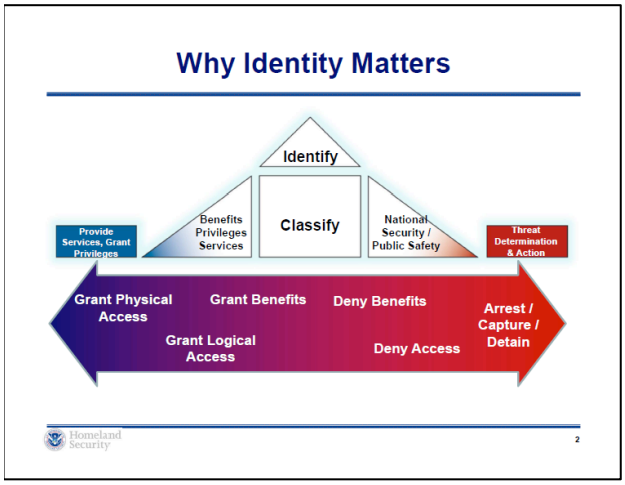
"Identity and biometrics has taken a step back" because of public concerns about privacy and government intrusiveness in other areas, said Kenneth Gantt, the acting deputy director of DHS' Office of Biometric Identity Management.

There was a fear of "Big Brother," Mr. Gantt said, in a conference keynote March 17.

"We have to do a better job of explaining the benefits, 'Here's what we want to be able to do with identity,'" he said.

"Until we really work that consumer [concern] aspect, we're not going to get there," he added, referring to public support for increased government and commercial use of biometric technologies.

Mr. Gantt displayed a slide showing the various missions in which biometric identity technologies can be used.



The right hand end of the scale, colored red, featured traditional law enforcement and national security uses, such as border control or identification of criminal suspects.

“We’ve been focused on [those interdiction missions] … I think we’re doing fairly well on the red side,” he said.

But the left hand, blue-hued, end of the scale featured other, more consumer-friendly, uses, like securing health records or bank accounts.

“It is much larger than what we do in the red if you really think about it and we have some challenges there,” he said of the blue end of the scale. “This is where identity assurance can help individuals receive better services and protection against identity theft and fraud”, says Phil Scarfo of Lumidigm.

Mr. Gantt, a retired Lt. Col. in the 3rd Infantry Division, previously headed up operations for the U.S. Army’s Biometrics Identity Management Agency.

India’s roll-out of a national biometric ID program had been successful, he said, because the government had figured out how to use it to deliver a service many citizens wanted and could not otherwise get — banking.

“They thought about the benefit first, which is awesome,” he said.

But in the United States, “We’ve got to figure out how you can help me to move us, as a country, to the blue side,” he told industry representatives.

“Because we’re not doing it right now.”

In a brief interview after his presentation, Mr. Gantt called the effort to win public support for biometrics in the US as “a public affairs war.”

“The more people know and see and understand” about the technologies, he said, “The more accepting they become.”

“That’s why IBIA has always emphasized education — telling the industry’s story and opening the public’s eyes to the benefits of this technology,” said Tovah LaDier, the association’s managing director.

Chicken and egg

Several presenters made similar points, referring to data that showed public attitudes to biometrics improving in countries where the technologies were being deployed.

In Brazil, one recent survey showed, the deployment of vein-print scanners at some banks’ ATMs had been followed by improving public attitudes to towards biometric technology.

“Where consumers are familiar with the technology,” said Terry Hartmann, vice president for security solutions and industry applications at Unisys Corp., “that drives adoption, because it takes away the suspicion and hostility that you have among some consumers who are unfamiliar with it.” Today the five largest banks in Brazil are deploying biometrics at their ATMs to provide enhanced security and user convenience.

But if familiarity drives adoption, the industry has a chicken and egg problem.

“That’s why we were all so excited about the iPhone 5S,” which can be locked with a finger or thumb print, said Ms. LaDier.

“It was the egg.”

Other industry thought-leaders concur: Apple has taken an important step by offering a consumer-facing biometric solution. Its significance is underlined by the fact that Samsung is following suit in offering a fingerprint lock on its new phones.

Gartner research recently predicted that the number of organizations requiring biometric authentication before a mobile device can access enterprise networks will increase six-fold in the next two years.

But for the consumer market, the key will be customer experience, another Connect:ID presenter said.

“If it doesn’t work, it won’t be used,” said Jay Meier, vice president of corporate development for BIO-key, of the iPhone fingerprint lock feature.

Security vs. convenience

In any biometric identity application, standards can be set either to minimize false rejections, or to minimize false acceptances. Keeping false rejections low maximizes usability, but it also increases the risk of false acceptances.

Mr. Meier suggested that Apple, concerned about consumer acceptance, might have tweaked their algorithms too far in the direction of usability.

“That’s why you had these stories, about guys enrolling with their elbows, … Or about the guy whose cat could log on.”

“Yes, the log on works every time, but it works for your cat too.”

“They’d rather have insecurity than inconvenience,” Mr. Meier concluded of Apple.

Issues with individual applications aside, there is no doubt that the ubiquity of cloud computing; and of mobile devices equipped with microphones, cameras and touch screens, creates huge opportunities for the deployment of biometric technologies.

“Your identity will be in the cloud, your phone is the lock, you are the key,” said Mr. Hartmann. Every phone on the planet is equipped to collect at least one biometric, voice, and most have cameras that can record faces, too.

“It’s all already in your pocket,” said Mr. Hartmann.

“We are not regulators”

The National Telecommunications and Information Administration (NTIA) in December asked industry, consumer groups, privacy advocates and other stakeholders to work together to develop privacy safeguards for the commercial use of facial recognition technology.

NTIA, a policy-making agency with the Department of Commerce, began a consultative process in February and has a series of public meetings planned through June.

The agency says the public consultations aim at helping interested parties reach agreement on a “voluntary, enforceable code of conduct that specifies how the [administration’s] Consumer Privacy Bill of Rights applies to facial recognition technology,” according to NTIA’s website.

That blueprint for guarding consumers’ privacy was part of a package of planned privacy measures unveiled by President Obama Feb. 23, 2012. And the NTIA multi-stakeholder process is aimed at putting those plans into action.

The NTIA has already completed one such process last July, producing — to mixed reviews — a code of conduct for disclosures about the use of personal data by mobile technology.

The codes of conduct will be enforceable, as a White House fact sheet from 2012 makes clear, because companies’ claims to abide by them will be enforceable by the Federal Trade Commission (FTC).

Officials are nonetheless keen to emphasize that they are eschewing formal rule-making.

"We are not regulators," said NTIA chief Lawrence Strickland at the first NTIA facial recognition public meeting Feb. 6. "We do not bring enforcement actions. Instead, we are in a unique position to encourage stakeholders to come together, cooperate, and reach agreement on important issues," he said.

"The biometric industry has always taken privacy seriously," said Tovah LaDier, adding that IBIA was "looking forward to engaging in the multi-stakeholder process alongside our members."

The association subscribes to the five Fair Information Practice Principles described by the FTC: notice, choice, access, security and enforcement, Ms. LaDier said.