

Biometrics Bandwagon Outpacing Privacy Safeguards

Jay Cline

June 10, 2004 ([Computerworld](#))

Governments and corporations increasingly see biometrics as the primary way they'll identify people in the future. In an age of terrorism and fraud, they hope fingerprint and eye scanning will become the cheapest and most reliable means of verifying that people are who they say they are. But are we ready for this convergence of computers with our flesh and bones? I don't think so. This significant intrusion into our personal space needs a heightened level of privacy protection that most organizations have only just started to envision.

Biometric technologies have long attracted the imaginations of screenwriters and science fiction authors. *Brave New World*, the James Bond movies, *2001: A Space Odyssey* and *Minority Report* all feature fantastic scenarios of biometric tracking and verification. But high costs and accuracy problems have kept biometrics from leaving this realm of fantasy.

That is, until 9/11.

The terrorist attacks on the U.S. prompted governments around the world to start seeking better ways of monitoring the flow of people across their borders. All eyes quickly turned to biometric authentication as the solution. Now, more than 20 countries are building digital fingerprints and facial patterns into their new passports and driver's licenses ([see story](#)).

Businesses are jumping on the government's biometric bandwagon. Private industry has long sought a better way than passwords to authenticate return customers. This is because passwords are costly to reset, and users often choose weak, crackable passwords. As a result, IMS Research

predicts that the biometrics market will grow 68% per year through 2010. The dawn of the age of biometrics seems to be upon us.

But there's a problem: The public may not be ready for it. The most common reaction people have toward biometrics—once the "cool factor" has worn off—is a reluctance to allow this level of intrusion into their personal space.

It's one thing to be asked to volunteer a password. It's quite another to allow your body to be scanned and have the results be recorded and used by complete strangers. For those of us who haven't been on a reality show, our natural reaction to these scanners is one of self-protection and modesty.

I have a deeper misgiving about biometrics. Because they promise to be much more cost-effective and reliable than traditional authentication methods, I expect businesses will want to adopt biometrics-only authentication, discarding expensive traditional methods.

But would you want to live in a biometrics-only world? Imagine if you needed a fingerprint scan to board a plane, access your bank account, receive medical care or check out at the grocery store. Three types of system failures could make your life miserable: a failed match, a mistaken match and stolen biometrics.

In a failed match, the system can't confirm your identity. Without a readily available backup process, you won't be able to complete the transaction. This is an inconvenience in itself, but the bigger impact may be on your reputation. Once biometrics are a daily reality in the U.S., the public may come to have a false sense of confidence in their accuracy. So people standing around you when your credentials fail might start suspecting you as an imposter.

A worse problem in a biometrics-only world is the mistaken match, where the system thinks you're someone else. If the system matches you to a criminal or terrorist suspect, you won't just fail to complete the transaction. You could spend the rest of the afternoon in custody and really arouse the suspicions of those standing in line nearby.

But the worst biometrics failure would be endured by those whose biometric information was stolen and used for identity theft. Today's victims of ID theft have a hard enough time clearing their names of transactions made using their Social Security numbers. Imagine how much harder it'd be to convince people someone stole your fingerprints. Biometric ID theft victims may never fully clear their names.

So does this mean we should oppose all uses of biometrics? Absolutely not. With the right controls in place, society can begin to realize the benefits that biometrics offer.

Here's a checklist of the top controls customers and citizens should demand before cooperating with biometric systems:


- The organization's explanation—available on demand—of how it will collect, use or not use biometric data
- Over 99.9% matching accuracy before a biometric is used as a primary identifier
- The use of traditional methods of authentication along with biometrics
- A defined backup process based on traditional authentication for erroneous biometric readings
- Information security that's been independently certified to meet a recognized security standard
- An effective and responsive grievance process for cases of biometric ID theft

Most organizations are only starting, however, to think about this level of process discipline. And they may never go further unless their patrons start demanding it.

No Silver Bullet

Because no single biometric identifier is highly reliable, nonintrusive and low-cost, governments and businesses should plan to combine biometrics with their current, traditional methods of authentication such as passwords and PINs.

Biometric	Accurate?	Intrusive?	Costly?
Retina	99.99999%	Highly	Median
Fingerprint	99.8%	Moderately	Lowest
Facial	Largely untested	Minimally	Lowest
Voice	98%	Minimally	Median
DNA	Largely untested	Highly	Highest



Cline manages data privacy at Carlson Companies Inc., a Minnetonka, Minn.-based group of businesses in the travel, hospitality and marketing industries. Contact him at privacy@computerworld.com.