Confronting Biometric Detractors

Presentation at the 2006 Biometric Consortium Conference
Baltimore, MD.

Dr. Robert Atkinson
President
Information Technology and Innovation Foundation
ITIF is a non-partisan public policy think tank committed to articulating and advancing a pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Recognizing the vital role of technology in ensuring American prosperity, ITIF focus exclusively on innovation, productivity, and digital economy issues.
Detractors vs. Opponents

Detractors: raise legitimate questions that need to be asked and answer regarding the effectiveness and value proposition of biometrics.

Opponents: oppose the deployment of biometric technologies in most applications, although they often deny that they are anti-technology.
Who Are the Opponents?

On the left: some more strident privacy groups that see the spread of new IT and biometric technologies as threat to personal privacy and anonymity. (e.g., ACLU, EPIC, CASPIAN)

On the right: some conservative/libertarian organizations that distrust government (e.g., Cato Institute, Eagle Forum).
Who Are the Opponents?

- Immigration Advocates that see biometrics/stronger IDs as means of keeping out immigrants (e.g., National Council of LaRaza, National Immigration Law Center).

- Techno-Libertarians who hide their ideological opposition behind computer security expertise (e.g., Bruce Schneier)
Why Are They Opposed to Biometrics?

- They believe that biometrics is leading to (or has already led to) the loss of privacy and the rise of a totalitarian state and they are very, very committed to stopping biometrics.

- They know that demonizing the technology expands and engages their organizations’ membership.
What Arguments Do They Use?

The problem is serious, but biometrics won’t solve it.

For example, the ACLU states:

We do not dispute the government’s need to secure the borders, but policies must make sense, provide security and be effective: the WHTI fails on all three points.

Facial Recognition Is Not Effective

E-passports distract border agents and make them less effective.

Bruce Schneier states, “Biometrics such as thumbprints show some promise here, but bring with them their own set of exploitable failure modes.”
Arguments II

Biometrics “Will Create a False Sense of Security” (ACLU)
Biometrics is a threat to privacy through data breaches.

- Recent security breaches have shown that storing vast information in a single database is especially precarious and a ripe target for identity thieves.” (ACLU, 2006)

- Biometric database would be a target for identity thieves; (EPIC)

- Biometric templates can be reengineered to produce your fingerprint (Bruce Schneier)
Arguments IV

Biometrics is a threat to privacy by enabling tracking.

The ACLU opposes using biometrics for “airline passengers because it is so intrusive. To be effective, the government would have to have the iris scan or digital fingerprint of every person living in the United States and probably that of anyone traveling through America’s airways. This would be the high-tech equivalent of creating a National ID system.”

"We've reached a point where a '1984' surveillance society is technologically possible, and that trend was accelerated by the events of September 11," said Barry Steinhardt, director of technology and liberty programs at the American Civil Liberties Union. (Washington Times, 2003)

“In the future, a spychipped passport will enable [government] to scan the information and create enormous databases so people can be monitored and tracked through their travels. What happens when those databases are run by corrupt officials of foreign countries? Do we want our own government, much less some third-world dictator, having computerized records of us that include a digital photograph, biometric information, date of birth, age and any other information they decide to encode on the chip? (Katherine Albrecht)

Standardizing driver's licenses with biometrics “establishes the framework to take us even further toward a surveillance society that would significantly diminish the freedom and privacy of law-abiding people in the United States.” (Eagle Forum)
The Government Isn’t Smart Enough to Get it Right

“The State Department has done a great job addressing specific security and privacy concerns, [with the RFID passport] but its lack of technical skills is hurting it. The collision-avoidance ID is just one example of where, apparently, the State Department didn't have enough of the expertise it needed to do this right.” Bruce Schneier
And of course, “Big Brother”

“Big Brother Is Monitoring Us by Databases” (Phyllis Schlafly, Eagle Forum)

Why is the administration using RFID on the passport? “There is only one possible reason: The administration wants surreptitious access themselves. It wants to be able to identify people in crowds. It wants to surreptitiously pick out the Americans, and pick out the foreigners. It wants to do the very thing that it insists, despite demonstrations to the contrary, can't be done.” (Bruce Schneier)
Their Solution: “Smash the Machines”

Hello—we’re Luddites—and we’ve come to smash your new-fangled machine.
Actually, it’s “Don’t Deploy the Machines”

- “If all employees who oppose fingerprinting, GPS tracking, and RFID-card” quit instead of submitting to these technologies “the resulting talent drain might cause companies to reconsider such one-sided workplace surveillance mandates.” (CASPIAN)

- EPIC recommends that funding for these [biometric] systems be suspended until a comprehensive evaluation of their utility and effectiveness is completed.”
Fear of New Technology is Not New

Despite the protection against invasion of privacy afforded by the fourth Amendment to the Constitution, bugging is so shockingly widespread and so increasingly insidious that no one can be certain any longer that his home is his castle - free of intrusion. (Life Magazine, May 20, 1966)
Persuading the Detractors and Confronting the Opponents

• If possible, prove it in the private sector, then deploy to public sector.

• Build in privacy from the beginning.

• Don’t over promise.

• Realize that in most cases opponents won’t play fair.

• Realize that government officials and the media are not experts and are likely to believe the opponent’s claims, even when they are false.

• Make it clear that “could” is not the same as “will.”

• Point out that most systems are not perfect, yet they work perfectly well.

• Focus on the benefits, including safety, security and convenience.

• Keep the debate on the rules, not on the technology.

• Educate, educate, educate.
www.innovationpolicy.org
ratkinson@itif.org