Human Bar Code

by Clyde Wayne Crews Jr.

November 1, 2002

Clyde Wayne Crews Jr. is director of technology studies at the Cato Institute.

http://www.cato.org/research/articles/crews-021104.html

Stock Photo Biometric technologies - such as voice prints, retina, iris and face scanners, digitized fingerprints, even implantable chips - can benefit us. Look for the technologies in cell phones, mobile computers, cars doors, doorknobs and office keys-basically everywhere. They'll bolster online commerce, help locate a lost youngster, and transmit medical information to doctors. They promise increased privacy by preventing identity theft.

But no one wants to be treated like human bar code by the authorities.

What are the benefits and concerns surrounding the further deployment of biometric identification techniques into our lives? While they promise new levels of physical security and secure commerce, they can also threaten fundamental values of privacy and liberty. We need a framework by which to judge biometric deployment, to make distinctions appropriate and inappropriate uses. The management of databases that underlie biometric applications can impact anonymity, privacy, and even authentication technology itself.

The most pressing threat to liberty is a government-mandated database containing all of us, corresponding to a National ID with biometric identifiers. This is the Big Brother scenario that would lead to the asking for ID everywhere, and devolve into a general law enforcement tool having nothing to do with the terrorism that prompted recent calls for National IDs. National IDs threaten liberty and anonymity, and, ironically, they undermine security itself by moving the locus of technological advancement in authentication technologies out of the private sector and into government.

A less sweeping biometric database is a partial one containing criminals and suspects - but not the general population. An example would be government-run face recognition cameras deployed in public places that have garnered so much attention lately. Individuals are observed, but presumably only to see if they match a face already in the underlying database. Allegedly, the information collection - that pertaining to the criminals - has already taken place under appropriate Fourth Amendment procedures, and no data is ever collected on individuals not already in the database. Nevertheless, many properly doubt governments can be trusted to discard incidental data collected on innocents. Applications of biometrics to identify and track individuals, even in "public" places, can constitute an unreasonable search and easily be abused. Stringent safeguards are required, but they do not yet exist. This will be the locus of much of the "privacy" debate in the coming years.

Finally, private, limited applications of biometrics are less worrisome. These might constitute databases of "members," as contrasted with governmental "bad guy" databases. Such tailored solutions exist where security clearances are needed, like factories and laboratories, and can offer the opportunity for extraordinary security by preventing others from posing as us. These proclaim, in effect, "You may enter my privately owned building, airplane, parking garage, neighborhood, house, etc., but only if I know who you are."

These offerings hold the most promise in the field of biometrics. However, these applications must not be allowed access to individual data gleaned by government coercion. If that happens, they will turn society against the technology and make it impossible to defend the industry from regulation. Let's keep it self-regulated.

Biometrics offers tremendous promise, but also risk. To safeguard civil liberties, there are basically three requirements. In a nutshell: (1) avoid mandatory databases or any form of National ID; (2) Ensure Fourth Amendment protections even for public surveillance, and; (3) avoid the mixing of public and private databases as new biometrics technologies emerge and proliferate: Instead of granting the private sector the use of government-mandated information, private industry must generate its own information, for purposes limited by the market's twin engines of consumer choice - and consumer rejection. Privacy, liberty, and even authentication technology will be all the better for it.

This article originally appeared on *Tech Central Station* on November 4, 2002.