The dawning of the biometric age
Ellen Gibson

Say goodbye to PINs and photo IDs. Say hello to digital fingerprints and iris scans—and to new opportunities for security businesses.

In baby steps and giant leaps, the world is moving further into digital identification and biometrics. The new technology raises concerns about privacy, of course, as well as opportunities for security companies.

The latest to join the migration: Switzerland. On May 17, Swiss voters narrowly approved a government plan to switch over to electronic passports, tied to a national fingerprint registry. The new passport will contain a microchip that stores personal data, a digital photo, and two fingerprints. At border crossings or airport checkpoints, travelers would have their fingerprints scanned and digital photos taken to make sure they match info in their e-passports.

Switzerland is actually behind much of Europe. Every nation in the European Union must institute fingerprint-enabled e-passports by next summer. Germany, France, and the Netherlands have already started issuing them.

Unhindered trip

Some locales are testing more advanced systems. For instance, at Manchester Airport in Britain, where facial-recognition devices have been installed in security gates, passengers with optional e-passports can bypass long lines and stroll right through. While travelers enjoy the unhindered trip through the airport, boosters say e-passports enable the government easily and swiftly to check anyone entering the country against international watchlists.

The digitization of personal information is a boon to companies in biometrics, or technology that can identify people based on unique physiological traits, such as fingerprints, DNA or even a person's gait or blood-vessel patterns. There are countless applications for biometrics—in border control, medical records, computing, and commercial transactions—and many experts predict it won't be long before such scans are part of everyday lives.

Lockheed Martin (LMT) is one of several companies partnering with government agencies to develop new applications in biometrics. The Bethesda (Md.) company is managing an effort by the Transportation Security Administration to give up to 1 million maritime and transportation workers access to secure areas of ports via biometric credentials, including finger and iris scans, which will be stored on biometric ID cards.

Meantime, the FBI has formed an international agency with Australia, Britain, and Canada to set up a "Server in the Sky"—a network for sharing biometric data on criminals and suspected terrorists. The group, called the International Information Consortium, asserts that a global biometric clearinghouse would help nations combat terrorism and rapidly identify victims in large-scale disasters such as Hurricane Katrina.

Resistance from privacy groups

Northrop Grumman (NOC), which is headquartered in Los Angeles, is supplying the technology, although the initiative has been met with resistance from privacy groups and has been slowed by the need for interoperability between different countries' databases.

The private sector has been experimenting with biometrics for years. Anyone who has seen CSI: Las Vegas knows that casinos use this technology. Some regional credit unions have

already piloted programs wherein members are identified by palm scans. And Walt Disney World (DIS) has been using finger scanners to ID visitors and prevent pass-sharing for years.

"Pre-9/11, the expectation was that [advances in biometrics] would percolate up from the commercial sector," says Lawrence Hornak, co-director of the National Science Foundation's Center for Identification Technology Research.

"But with the emphasis on security after 9/11, there are now major government initiatives."

Many individuals might prefer digital identification over today's security systems, which often require lengthy combinations of letters and numbers that must be changed frequently. Biometric proponents foresee a future in which body scanners replace passwords in computers and personal identification numbers at ATMs. "You always carry your physical characteristics with you," notes Hornak. "That provides a lot of convenience."

The major challenge in implementing biometric banking on a larger scale is providing the infrastructure. Institutions would need a central repository of biometric information against which to compare the scans.

Breaches are inevitable

Perhaps a bigger hurdle is opposition from civil liberties groups, which contend that biometric systems infringe on privacy and compromise individual security. Many people are wary of a future in which cameras sample their physical traits, compiling digital dossiers without their knowledge as they stroll through an airport or convenience store. And consumers fear that hackers will steal their information when it is contained in a centralized database.

Most security analysts acknowledge that data breaches are inevitable—in fact, experts have demonstrated that fingerprint scanners can be fooled with just gummy candies and a laser printer—but your biometrics are irreplaceable. "If my password security is breached, my bank and I can agree on another bit of secret information," explains John Verdi, senior counsel at the Electronic Privacy Information Center. "If I give my bank an iris scan and somebody spoofs it, I can't do anything other than poke out my eyes."

Verdi is not opposed to biometrics research, but he has a hard time believing that the advantages of current applications outweigh the risks. "If you're going to submit this truly sensitive information, you're pretty much assured that it's going to be compromised at some point," he says. "The question is: What is so important that I'm willing to put that information out there?"

GIBSON, Ellen. The dawning of the biometric age. **BusinessWeek**, New York, 20 maio 2009. Disponível em: <www.businessweek.com>. Acesso em: 28/5/2009.