

Biometrics Data Is Vulnerable, Warn Experts

Encryption standards and data-access rules needed

EMAIL PRINT SHARE

PAGE 1 2 // VIEW ALL

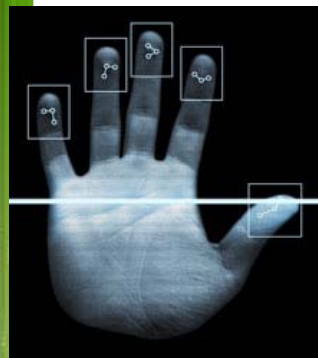


PHOTO: Andy Piatti/Stockphoto

BY MARK ANDERSON // AUGUST 2009

18 August 2009—Industry forecasters say the market for **biometric** data-collection systems will double or triple in size over the next five years. The technology, which analyzes such markers as fingerprints, voice prints, face shape, palm and finger veins, and irises, is used in applications as varied as **passports** and Disneyland passes. But storing the data on both government and privately owned computers poses an increasing threat to individual privacy and opens up new frontiers in identity theft, say security experts.

Privacy advocates are growing concerned about biometric "function creep": A company that scans your iris for an ID badge, they say, might also allow government or commercial entities to run this biometric data against their own databases—whether for legitimate or questionable purposes—without your consent. This is why encryption of biometric data is needed, argue Canadian and European biometric experts.

Ann Cavoukian, information and privacy commissioner for the Canadian province of Ontario, is an outspoken proponent of developing worldwide standards for encrypting biometric data, ensuring that the data can be used only for its original purpose, such as verifying the identity of a passport holder.

"In Europe and many countries, passports are now requiring biometrics," says Cavoukian. "I don't have a problem with that because it authenticates my identity. It says the person holding this passport is me. What I do have a problem with is those biometrics being retained in a central database that is then going to be accessed by law enforcement."

That very scenario could, in fact, be taken right out of the headlines. A new law is now being considered in the Netherlands that would aggregate every passport holder's fingerprint data and enable Dutch law enforcement to "go on fishing expeditions," as Cavoukian puts it. "This is the slippery slope," she says.

According to a report last year by American consulting company International Biometric Group, fingerprints make up two-thirds of all biometric data used today. One possible standard for fingerprint encryption comes from the Dutch company priv-ID, a spinoff of Philips Electronics.

Michiel van der Veen, the company's CEO, says that instead of storing fingerprints, priv-ID systems store only codes that are equivalent to six-digit PINs. The systems, now in use in South Africa and Swaziland, translate a fingerprint image file into code using a mathematical tool called a hash function—an algorithm that generates a small but unique set of numbers from a larger data file. Van der Veen says that even two sets of fingerprints collected from the same person under different circumstances—say, with clean hands on one occasion and dirty or greasy hands a second time—would generate the same code. But two different people would be very unlikely to generate identical codes.

"I always like to compare [priv-ID encryption] to the way we protect passwords on our computer," he says. When you log in to your laptop, it doesn't compare the password you type in to a stored copy of the password; rather, it runs the typed-in password through a hash function and compares that value to a stored copy of the hashed original password. "If your password file is stolen," van der Veen says, "then you should not be worried, because it's protected by the hash function."

Ralph Rodriguez of Boston-based Delfigo Security says the biggest problem with using biometrics for identification is that even if they are encrypted, they need only to be hacked once to be compromised forever. "I don't get another right thumb," he says.

Rodriguez instead advocates for what he calls "adaptive" biometrics: timing the way

you type in a familiar phrase or password, for instance, down to the millisecond level. The duration of each keystroke and the time between them are reliable identifiers that can compete with any biometric, he says. "The reason why is because of muscle memory. I'm effectively capturing your ability and a combination of previous injuries and the way you hold your hands, your hand-eye coordination. It's all very much tied back to the human being."

So companies or government agencies using an adaptive biometric, Rodriguez says, could still uniquely identify someone without ever needing to dabble in more personal data such as fingerprints or, someday, DNA, which if unencrypted could also be used in ways that could compromise a person's privacy.

The real threat of misused biometric data is still in the future, says Nasir Memon of New York University's Polytechnic Institute, in Brooklyn. Right now, the privacy of credit card and Social Security numbers is more important than one's biometric data.

"At this stage, it's an interesting problem," he says. "But as [biometrics] start getting deployed more, threats will emerge.

"When the Internet was first being used, people didn't worry much about security either," he says. "[Internet] security was an 'interesting problem' then too."

About the Author

Mark Anderson is a writer based in Northampton, Mass. In March 2009, he wrote about how a quirk of the [memory used in RFID tags](#) could lead to better security.

TAGS: ADAPTIVE // ETHICS // FINGERPRINT // PAGE 1 2 // VIEW ALL
BIOMEDICAL // ONTARIO // ENCRYPTION // FACE RECOGNITION // BIOMETRICS