Biometrics group counters privacy fears

[WASHINGTON] A newly formed US industry group has announced a set of principles that, it says, should protect users of biometrics against privacy abuses. The move is a bid to pre-empt attacks from civil libertarians and politicians anxious to capitalize on public anxiety about data privacy.

The International Biometric Industry Association (IBIA) says its code calls for legislation to control government use of biometrics. But it would leave private industry unregulated except for voluntary adherence to the principles. "If the end-users and customers of the technology are cognizant of the [privacy] issues, this is clearly an area that can be self-regulated effectively," says Richard Norton, executive director of IBIA.

A biometric is an electronic code representing some unique physical feature — commonly a person's hand geometry, iris pattern, fingerprint or face — that is used to verify that person's identity against a reference code provided by the person and stored digitally.

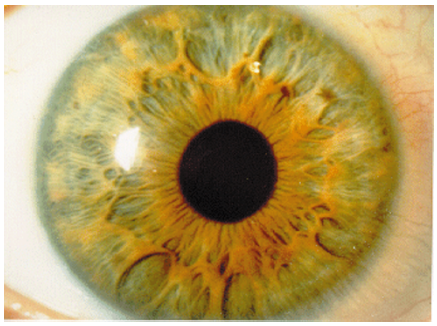
Norton says the group was motivated by about 150 privacy bills introduced in the last Congress — and 38 so far in this one — that would affect biometric technology makers and marketers, often adversely. Rather than face the consequences of such bills becoming law, or of having to deal with a patchwork of state laws in the absence of federal action, IBIA is seeking pre-emptive federal legislation limiting government use of biometrics.

Privacy advocates say that digitized identification systems are easily abused by government and industry. Computerized biometric information can be manipulated and transferred swiftly and easily. A biometric is unique and cannot be forged like a signature, stolen like a password or lost like a card. Because of its near-infallibility, they argue, industry or a 'Big Brother' state could use an individual's biometric as an all-purpose identifier that could be used to deny benefits, restrict travel, or even obliterate the individual as a state-recognized entity.

"A majority of citizens have something to fear from biometrics because information that identifies you intimately in one area of your life can easily be used to adversely score you in another," says Simon Davies, director of Privacy International, a London-based group that monitors surveillance by governments and companies.

Davies says the potential for abuse is particularly dangerous in countries with authoritarian regimes. He complains, for instance, about IBM's recent work with the Peruvian government to digitize fingerprints to prevent fraud in applications for national identity cards.

"What lies around the corner is the same biometric being used for social security, police purposes… a whole range of other purposes."



IRISCAN

Private eye, public information: security systems such as those that scan irises could be abused.

Barry Steinhardt, associate director of the American Civil Liberties Union, says biometrics present a real danger of the development of a 'surveillance state'. He says: "We have grave concerns about how [this technology] is going to be used. [Will it] make it impossible for people to go about routine business in an anonymous way without being subject to surveillance or having more and more data collected about them, either by government or by private industry?"

But the IBIA, which represents 15 companies with revenues of $35 million, says its members are being targeted by a misinformation campaign. It argues that the technology is safe, user friendly and a near-perfect defence against identity theft, cheque fraud and other privacy abuses.

If the critics understood what biometrics do, they would "see this as a tool for protecting privacy rather than running around saying the sky is falling," says John Siedlarz, IBIA vice-chairman, who is president and chief executive of IriScan, a company based in Marlton, New Jersey.

The industry says that biometrics enhance rather than undermine personal data security, providing a system that is much less vulnerable to fraud and abuse than, say, the use of PIN numbers at banks or passwords to access computer networks.

"You can't take the code that's been generated by the minutiae of a fingerprint or hand geometry and reverse-engineer that to show who I am. So it is a very secure way of locking up information," says Norton.

The IBIA principles say that biometric data must not be "released without personal consent or the authority of law". They call for industry to develop "policies that clearly set forth how biometric data will be collected, stored, accessed and used", and that preserve individuals' rights to limit the distribution of their data beyond the original purpose.

The principles say that "clear legal standards" should be developed to define and limit the conditions under which government agencies can acquire and use biometric data. And they call for public and private sectors to adopt "appropriate managerial and technical controls" to protect databases containing biometrics.

But Davies calls the principles "a Sesame Street privacy code" which, like other voluntary industry codes, is "unenforceable, illusory, counterproductive" and likely to be ignored by governments.

Similarly Robert Gellman, an independent privacy consultant in Washington, says the code is "a very casually written document without a clear understanding of privacy principles or fair information practices".

"The principles could be a lot clearer and stronger, and they're not. This is the usual American approach of saying you're going to do something about privacy, only not in a way that has any teeth." **Meredith Wadman**

Hand and eye security systems in growing use

[WASHINGTON] Biometrics have been widespread for some time in sectors such as law enforcement and the nuclear power industry, where hand geometry is used to control access to secure facilities. But they have begun in the last five years to be used in ways far more likely to be encountered by ordinary people.

Since 1995, for example, the US Immigration and Naturalization Service has enrolled more than 80,000 travellers in a system that allows them to jump lengthy queues at airports by scanning their hand geometry.

Companies are using fingerprint imaging devices to serve as passwords for computer networks. And welfare programmes from Connecticut to Los Angeles County are using biometrics to deter welfare fraud.

If privacy advocates are anxious about the implications of biometrics, some members of the public may be less concerned. In the United Kingdom, the Nationwide Building Society and NCR Corporation last year tried out an iris scanning system with 1,000 customers at Nationwide's Swindon branch.

Instead of using PIN numbers or signatures at the cash machine or bank counter, customers' irises were recognized by cameras which gave them access to their accounts. Some 91 per cent of participants favoured the system over the use of PIN numbers or signatures, according to the Pegram Walters Group, which carried out the research. **M. W.**