

Biometrics and the Prevention of Identity Theft

Testimony of
Dennis Carlton
Director of Washington Operations
International Biometric Group, LLC

To the

Senate Special Committee on Aging
July 18, 2002

My name is Dennis Carlton and I am the Director of Washington Operations for International Biometric Group of New York City. On behalf of our company, I'd like to thank the committee for the opportunity to talk to you about the technology called biometrics and describe how it can be used to combat the problem of identity theft.

Let me begin with a brief description of International Biometric Group so that you better understand who we are and our unique position in the world of biometrics. International Biometric Group, or IBG, provides independent consulting services to government and private industry customers interested in biometric technology. Our organization focuses on three primary functions: (1) evaluating and reporting on biometric products and vendors, as well as the markets in which they compete, (2) advising clients on how to implement biometric systems, and (3) integrating a wide range of biometric hardware and software to meet the security needs of our customers. We take a practical, hands-on approach toward biometrics. We have conducted extensive comparative performance testing of more than thirty different biometric solutions so that we know how they're likely to perform in the real world. IBG holds to a strict vendor-neutral policy, which enables us to maintain close relationships with biometrics vendors while ensuring that our clients receive accurate and independent advice on which biometric systems can best meet their needs.

Let me take a few moments to review some of the basics of biometrics. A technical definition of biometrics is the automated measurement of behavioral or physiological characteristics of a human being to determine or authenticate their identity. In other words, it's the use of computers to confirm who a person is by matching a behavior or a permanent physical characteristic with similar records in a database. Research has shown that behaviors such as the way we speak, the way we sign our names, and even the way we type on a keyboard are distinct and unique enough that they can be quantified and compared by computers to existing samples. In a similar way, physical characteristics of the human body such as the friction ridges on the pads of our fingers, the geometry of our hands, the shape of our face, and the patterns of our irises and retinas can be measured and matched against computerized databases. A wide range of products in the market can acquire and match a person's biometric data in order to quickly and accurately identify who they are. Time permitting, I hope to be able to demonstrate some examples of these technologies to you later.

To effectively describe how biometrics can be used to combat identity theft and protect senior citizens, I think it's important to address some issues that often confuse the dialog about biometrics. First, it's important to set practical expectations of what biometrics can and can't do. To date, we have not seen a biometric product that will work accurately 100% of the time. Whether it's wrongly identifying one person as somebody else, failing to identify someone it should have recognized, or preventing someone from initially enrolling in the system, all biometric systems make errors. A properly designed system needs to employ biometrics as just one of a number of interlocking layers within a security solution, and must also include a quick, efficient exception handling process. Secondly, no one biometric technology is right for every application. For instance, while a finger-scan technology may be an excellent solution for replacing passwords to gain access to a desktop computer system, it isn't of much help trying to pick a potential terrorist out of a crowd in an airport terminal. And finally, people should not automatically conclude that the use of biometrics is an invasion of our personal privacy or a violation of our civil liberties. Biometrics themselves are privacy neutral – it's the way they are employed, and the protections put in place to limit misuse, that make biometrics either privacy-invasive or privacy-protective. What is essential is that individuals are fully informed on how their data is shared, used, collected, and secured. For more information about biometrics and privacy I commend to you an IBG-sponsored website dedicated exclusively to the subject, www.BioPrivacy.org.

Biometric technology has been employed to prevent fraud and identity theft for several years now. I personally managed a pilot program that began in 1998 to evaluate the use of finger-scan technology in a retail grocery store for confirming the identity of people who paid for their purchases by personal or payroll check. Reaction to the system by those who used it was universally positive. People found it much easier and faster to identify themselves with their index finger rather than digging through a pocket or purse for an ID, and the store found the incidence of loss due to check fraud reduced to zero. Most interestingly, senior citizens were some of the most enthusiastic proponents of the system. They recognized that no one could steal their checkbook and drain their bank account if a system like this was widely deployed. Several companies have now commercialized the concept of identification at the point of sale; I've brought some current examples of these technologies for demonstration purposes.

To properly serve the needs of elderly citizens, it may be necessary to make some adjustments to standard biometric systems. For example, the aging process can reduce the suppleness of a person's skin, which can present problems for finger-scan technology. The use of certain moisturizers and specially designed sensors can significantly reduce this problem. Another problem commonly associated with the aging process, decreased visual acuity, can make it difficult for people to properly position themselves for a facial-scan or iris-scan system. To overcome this challenge, vendors can offer more sophisticated camera systems that automatically locate the subject's face or eyes with little user effort. As I mentioned earlier, for citizens who are physically unable to interact with the biometric system, an efficient and transparent exception handling process is essential.

In conclusion, biometric technologies have already been shown to be powerful tools for combating the growing scourge of identity theft that afflicts Americans young and old. Thank you for your time and I welcome the opportunity to demonstrate some of this technology to you.