

National Geographic Traveler Heft July/August 2002

Artikel: Smart Traveler, Seite 15

Travel tactics for a changing world
Your Body, Your Badge



The travel industry turns to biometrics to keep you safe, secure, and speeding through lines. But are these high-tech devices accurate? And what about your privacy?

BY DANA HAWKINS

In a recent cartoon-animated video produced by Japan's Narita Airport Authority, a carefree girl glides through an airport fuss-free. No waiting in long lines, and no pulling out a boarding pass and ID. Rather, the sprite pauses but a moment at an automated security checkpoint to verify her identity with a smile and a nifty multifunction device. To further shave minutes, she'd even checked in on her way to the airport via the gadget, which connects to the Internet. Sweet.

That sort of frequent-flier fantasy is closer to reality than one might think. What powers the possibility is what's embedded in the apparatus biometric identifier that links the gadget to the girl. Biometric systems measure distinctive physiological characteristics such as fingerprints, hand shape, facial structure, or iris pattern. "One day we won't leave home without our personal biometric device," says Richard Norton, executive director of the International Biometric Industry

Association. "It will be the ultimate in security and convenience for travellers.» Such a device could be integrated into everyday items cell phones, credit cards, key fobs and might also be used to securely access Your laptop car. or home.

Since the beginning of the year, dozens of airports have deployed various biometric systems. Selected frequent fliers landing at London's Heathrow, Washington's Dulles International, New York's JFK, and Amsterdam's Schiphol airports have volunteered to have their irises scanned to measure distinctive variations and patterns. The information goes into a database and is used on subsequent trips to verify that the passengers are, in fact, who they claim to be. And more airports are installing facial recognition devices at security checkpoints to scan passengers against a database of wanted felons and suspected terrorists. Airports have also placed them in public areas to monitor crowds.

But airports aren't the only venues where travellers can expect to be scanned and measured. **When guests register at Hotel Consul in Bonn, Germany, the form, pressure, and speed of their signatures are filed electronically.** Season pass holders to Disney World theme parks in Orlando enter by passing through turnstiles equipped with two-finger geometry readers, and several cruise lines are considering tightening security by adding biometric data to the photo ID on boarding passes. "It would ensure that the same people getting on are those who got off," says Ted Thompson, executive vice president of the International Council of Cruise Lines. HA gangway guard might be fooled by someone sneaking on in a baseball cap and sunglasses."

Yet biometrics experts warn that these systems are not perfect. In the Tampa entertainment district of Ybor City, local police use facial recognition technology to scan crowds for wanted felons, runaways, and sexual predators. But critics contend that the way officers covertly track pedestrians with pan and zoom camera techniques is highly invasive to privacy.

Some biometric devices are inaccurate, or won't necessarily increase security. "We don't have a database of bad people's faces, irises, or hand geometry to match against," says Jim Wayman, director of biometrics research at San Jose State University. The accuracy levels of face-scanning systems

can also be problematic. Six weeks after test subjects had "enrolled" with an initial face scan, some systems failed to recognize them nearly one-third of the time. Other devices also perform poorly. Some systems cannot collect a finger scan from up to 12 percent of users, according to recent tests conducted by the International Biometric Group. That's because their prints may be worn if subjects are elderly, or damaged if they work in construction or with harsh chemicals (hairdressers, for instance). Turns out, biometric systems are flawed, just as the human beings they verify and identify.

Can You Fool a Biometric Device?

All but the most sophisticated systems can be tricked with a well-constructed fake finger, hand, or eyeball. That's because few devices, including the two-finger readers at Disney World, check to see that the biometric sample is warm, blinks, or is otherwise alive. Gordon Levin, an engineer at Disney World, says a pass holder might conceivably create a mold of his fingers so his pals could get in free. But that's where the human element comes into play. Since operators watch the turnstiles, he claims that cheated get caught "A kid trying to get in with a fake human hand would raise some suspicion."-D.H.

Siehe auch:

(english) http://www.hesy.de/PM_BaltusII3.doc, www.hesy.de/d02687t_page36-37.pdf

(deutsch) <http://www.bonner-rundschau.de/bonn/2496364.html>

http://www.general-anzeiger-bonn.de/index4_frameset.html?/news/artikel.php?id=42773