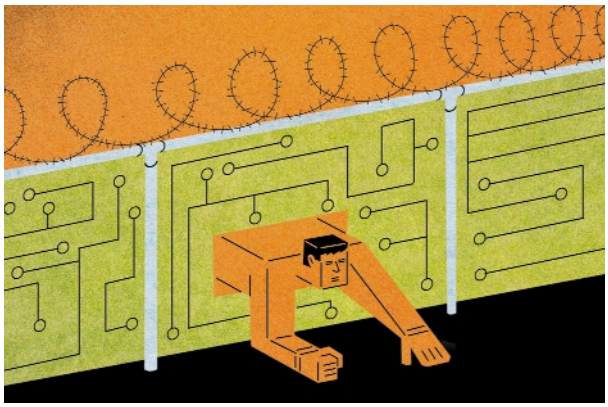
# Passport To Nowhere

## THE RADIO-TAGGED BIOMETRIC PASSPORT WON'T FAZE INDUSTRIOUS TERRORISTS

BY PHILIP E. ROSS

If you want to stop terrorists from getting at you, your first thought might be to step up surveillance at ports of entry; your second might be to exploit the modern world's technology advantage over the likes of Al Qaeda. The problem is, the proper technology is rarely chosen at first thought.



Undue haste led the U.S. government and the 27 countries in its visa-waiver pool to start a program two years ago to embed radio-tagged ICs in passports. These chips will encode the physical characteristics of the bearer, starting with the face. The U.S. initiative, included in the Enhanced Border Security and Visa Entry Reform Act of 2002, gained overwhelming support in the U.S. Congress and among the other 27 countries.

Because of foot-dragging and incompatible technologies, the system could not make its planned rollout this past October and had to be postponed for a year. But the problem goes deeper: the facial-recognition technology that companies promised would identify travelers doesn't live up to the hype. And even if the new e-passport program, at an estimated cost of more than US $1 billion a year, could make it harder to forge visa-waiver passports, it would not do much to thwart serious terrorists.

First, though, consider the embarrassing postponement. It began late last year when tests in Australia of the various visa-waiver countries' systems raised "a host of concerns," according to Barry J. Kefauver, former deputy assistant secretary of state for the U.S. Department of State's Passport Services. He is now chair of the International Organization for Standardization Task Force on New Technologies and advises the International Civil Aviation Organization (ICAO), which sets security standards. The Montreal-based ICAO began working "with crisis impetus," Kefauver says, in an effort to make different chips and readers work together and to ensure that chip packages were tough enough to last through a passport's life. But it soon became clear that the job couldn't be done in time to meet the U.S. deadline.

Last year, the ICAO laid out 22 passport improvements, centering on a few critical goals. The new passports should be harder to forge than today's versions, identify the bearer reliably, and require a traveler to spend no more than 11 seconds at the passport agent's booth.

People have been working toward these goals since the late 1980s. That's when passports began incorporating machine-readable features: two lines of 44 characters on the passport's data page that encapsulate the essential information—name, country, and passport number. The code didn't stop forgers; it

DAVID PLUNKERT

remained just as simple to cut and paste your picture into a stolen passport. So in theory at least, the new chips will provide governments with the foolproof system they need to be able to guarantee that you are who you say you are. This is the ideal scenario: a traveler presents the e-passport, with a chip laminated into its front cover, to a passport control agent. A camera takes the person's picture while the agent passes the e-passport over a radio-frequency reader and downloads the data already printed on the document and encoded in its IC—name, date and place of birth, height, weight, and code number, as well as other biometric data also encoded in the chip. The passport agent, with computer assistance, compares the page to the data downloaded from the chip, to the person standing there, and also to a central database to make sure all the attributes match.

The encrypted chip makes the forger's job nearly impossible. A few millimeters square, the chip contains 64 kilobytes of dynamic random access memory and a processor running software that communicates through a built-in antenna with the passport agent's reader. It can either be a system-on-chip, complete with a tiny antenna, or it can be packaged with a large external antenna wrapped in a spiral to lie flat in the page. It isn't easy to make—any bad guy with less funding than, say, Dr. No, would find it essentially impossible to make a comparable chip from scratch. And a stolen one isn't easy to crack. Even if the thief could decrypt the chip's stored personal and biometric data, altering its contents would require custom reverse-engineering software.

**BIOMETRICS—THE ONLY REALLY NEW TECHNOLOGY** to be incorporated into the e-passport—strives for positive identification. The ICAO is starting off by requiring only facial-recognition data, which is far from foolproof. Depending on how rigidly you standardize the photographic setting, facial biometrics still yields error rates ranging from 5 percent to 50 percent; a shot taken slightly from the left with a bright flash may not quite match the border official's shot, taken straight ahead under fluorescent lighting. Even those rates will worsen as the years roll by and faces are altered by age, sun, makeup, lighting, and changed shaving practices.

The U.S. National Institute of Standards and Technology, in Gaithersburg, Md., wants companies to demonstrate 98 percent reliability for their facial-recognition systems—a tough standard, but perhaps not tough enough to handle tens of millions of travelers per year. Consider the problem of false alarms, which even in a world of 98 percent average reliability will occasionally get much worse, angering shuffling lines of weary travelers. What's more, if every third fellow with a beard and every woman with a veil sets off the alarm and gets carted off to a secure area for "secondary questioning," it may seem as if the impersonal biometric system is just an excuse to discriminate against Muslims. On the other hand, if border guards tire of interrogating people they are convinced the system has flagged erroneously, they may get into the habit of waving such people through. The elaborate facial-recognition system would then become as useless as an oversensitive smoke alarm that has been disabled.

It all comes down to a tradeoff between efficacy and convenience. "Biometrics is a tool, not a panacea," says Kefauver. "It's meant to increase the utility of a human process."

While the ICAO is deferring the addition of other biometric markers—notably fingerprints and iris scans, which experts agree are more reliable—participating countries are free to include the additional markers. "There may have to be some minor differences between countries," says Saswato Das, spokesperson for innovation and technology at Infineon Technologies North America, in San Jose, Calif., which is vying for the U.S. government contract to produce the chips, along with Axalto, BearingPoint, and SuperCom. "All the chips we will offer will support all the requirements around the world, whatever is demanded," adds Das.

Electronic passports—with or without biometrics—will make it easier for countries to exclude small fry, such as illegal immigrants in search of work. Meanwhile, serious terrorists will just smirk. If they need passports, they can forge them from non-visa-waiver countries—recall that the difficult-to-forge e-passports are going to be issued by only the 27 visa-waiver countries—and brave the secondary questioning at the airport. Alternatively, they can apply for visa-waiver passports with faked paper documentation. Terrorist masterminds might also simply recruit agents from within visa-waiver countries, as Al Qaeda did when it got Britain's Richard Reid to try to blow up an airliner with a bomb in his shoe. Last but not least, terrorists can simply slip through poorly guarded frontiers. If Kennedy Airport in New York City is out, then they can always sneak into the Florida Keys on a cigarette boat.

The electronic passport puts up a Maginot line at the border, when what we really need is a comprehensive defense that impedes the aspiring terrorist—but not innocent travelers—at every step. But to get such a defense, we'd need something on the order of the domestic passports required in the former Soviet Union or the national ID cards now issued in Spain, France, Germany, and other countries, some of which contain biometric data. But while there is talk of requiring such domestic ID cards in more countries—including the United States, Canada, Japan, and Australia—citizens there have so far balked at what are perceived as tools of universal surveillance.

**EVEN THE RADIO-TAGGED PASSPORTS** go too far for some. They could, in principle, be read from a distance without the bearer's knowledge, says Marc Rotenberg, executive director of the Electronic Privacy Information Center, in Washington, D.C. "It allows secret disclosures, information that you can't inspect and correct, and that might not be relevant to what you're seeking: entry into a country," he says.

So what were the bureaucrats thinking? Maybe they were infatuated with similar radio frequency ID (RFID) technology, which retail giant Wal-Mart Stores Inc., in Bentonville, Ark., and other big companies will soon be using to track millions of items. But a bag of socks at Wal-Mart isn't self-propelled, intelligent, or malicious. It is checked when it enters the company's grounds and at many points on its way to the customer's car.

And if the occasional bad sock gets through, Wal-Mart will cheerfully refund the purchase, and New York City will still be standing. Terrorists are a different story. ■

## ELECTRONIC PASSPORTS

**GOAL:** To provide foolproof passport identification using a combination of biometrics and secure, radio-tagged ICs

**WHY IT'S A LOSER:** It won't stop terrorists from getting into the country

**ORGANIZATION:** The U.S. Department of State and counterparts in its 27-country visa-waiver pool

**CENTER OF ACTIVITY:** Washington, D.C., plus various research centers across the world

**NUMBER OF PEOPLE ON THE PROJECT:** Not available

**BUDGET:** A few million U.S. dollars in the research phase; up to $100 million per year in the United States, $1 billion worldwide after deployment