The Privacy Risks of New Passport Technologies
Introductory Panel Remarks
Computers, Freedom & Privacy Conference; Seattle, 13 April 2005

Kenneth Neil Cukier
Technology Correspondent, *The Economist*

The passport is a relatively new invention: the documents started coming into use only around World War I, when states began to take a greater interest in who passed through their borders. Before then, travelers didn't need any document attesting to who they were, and nations weren't in the business of providing them. An adventurous soul in Britain might simply cross the channel and try his luck in Flanders or France or Florence.

Travelers didn't need identity documents -- but they helped. And so "letters of introduction" where commonly used to attest to who the bearers were. A scholar, merchant or minor noble might solicit a letter from a man of stature in his home country, to present when in a foreign land. (For instance, the Spanish writer Cervantes traveled Europe and the Mediterranean using letters of reference. After pirates ransacked a ship he was on, the letters led them to believe he was wealthy and he was held for ransom in Algiers for five years -- and those letters spared his life when he was caught four times trying to escape).

After passports became common, other travel documents emerged. In the film *Casablanca*, the stolen "letters of transit" to leave Morocco were hidden inside Sam's piano. And the key question of the film was who would use it: would it be Ingrid Bergman with Humphrey Bogart -- or someone else? It was taken for granted that the documents would be doctored; it never mattered to whom they were actually issued.

And when you think about, the situation has not changed much from Rick's Café to today.

We know, for example, that Satam al Suqami and Abdul Aziz al Omari, who were among the hijackers on American Airlines flight 11 that crashed into the North Tower of the World Trade Center on 9/11, had passports that had been doctored. Many of the other terrorists had fraudulent official identity documents, as well. [1]

This isn't surprising. In the famous "al Qaeda Training Manual" that was recovered from a raid of a terrorist's home in Manchester, England in 2002, the book's third section is entitled "Forged Documents (Identity Cards, Records Books, Passports)." In it, the manual instructs: "All documents of the undercover brother, such as identity cards and passport, should be falsified." Among other things, it notes: "The validity of the falsified travel documents should always be confirmed." [2] Confirmed, that is, by other illegitimate documents.

The vulnerabilities of travel documents have been with us for a very long time. And it is in this context that passports are getting their biggest overhaul in their very long -- or very short -- history. Governments are incorporating new technologies. First is radio frequency identification (RFID) tags, also known as "contactless" chips. Second, is biometric identification technologies such as facial recognition, fingerprints and iris scans. The idea is to better ensure that the person bearing the passport is truly the person to whom it was issued.

The central question, perhaps, is thus not *should* this happen, but *how*?

Many people criticize the US government's plans, and the standards set by the intergovernmental body, the International Civil Aviation Organization (ICAO), as too ambitious. There is a feeling that it is too much technology, too soon, without sufficient regard for privacy protection or the vulnerabilities inherent in the technology choices that were made. In this regard, governments may be learning the lesson that businesses did in the 1990s: that throwing money and technology at a problem doesn't always work.

On the other hand, there is an argument to be made that inactivity, indeed passivity, to the problem is worse.

In this polarized environment, there is a lot of misunderstanding about what e-passports are and truly entail. Luckily, on today's panel are a number of experts to help up understand the issues. Let me introduce them now, give them a chance to make opening remarks, and then go into a discussion before opening up the floor to questions….

Notes:

1. Al Qaeda Training Manual. Section 3, points 2 and 7. Online at: http://www.usdoj.gov/ag/trainingmanual.htm

2. 9/11 Commission. "Entry of the 9/11 Hijackers into the United States Staff Statement No. 1." Page 2. Online at: http://www.9-11commission.gov

# # #