ACLU
AMERICAN CIVIL LIBERTIES UNION

Naked Data:

How The U.S. Ignored International Concerns and Pushed for Radio Chips In Passports Without Security

An ACLU White Paper
November 24, 2004

Introduction

Documents obtained recently by the ACLU show that the United States government ignored warnings about privacy and security while successfully pushing for an international standard for new electronic passports that will leave citizens vulnerable to identity theft, invasions of privacy, or worse.

This white paper explains the issues at stake, and offers a "guided tour" through the new documents and what they show. It has to do with a new global standard for passports that includes remotely readable "contactless" computer chips as well as a biometric. Created by an international group at the prompting of the United States, this standard was developed behind closed doors, with the ACLU and other privacy groups excluded from the process.

The major findings that emerge from the documents are that:

- During the standards-development process, there was extensive discussion of the potential privacy and security problems with leaving the electronic data on individuals' documents unprotected. Nevertheless, the standard that was adopted includes no encryption or other measures to protect that information.
- It was the United States that fought against privacy and security protections – against the advice of security experts and over the objections of other nations participating in the process.
- The U.S. is currently moving ahead with creating new U.S. passports based on this standard.
- This issue is bigger than just passports. It is about the construction of a global identity card that will likely influence the creation of national identity documents and threaten to facilitate tracking and loss of privacy around the globe.

What's wrong with the new passports?

The new passports, which the State Department is planning to begin issuing in 2005, are based on a standard developed by a little-known international group, the International Civil Aviation Organization (ICAO). Nominally sponsored by the United Nations, ICAO is made up primarily of representatives of advanced-industrial nations.

The passports contain two notable features. First, they contain a biometric – specifically, face recognition. Face recognition is not only among the least reliable biometrics currently available, but unlike others such as fingerprints, it is one that can be used from a distance to track individuals without their knowledge or consent.

Second, the passports will contain RFID (Radio Frequency Identification) tags.[1] RFID tags are tiny computer chips that, when they receive a radio signal from an RFID reader, use the energy of that signal to broadcast the data that they store. This technology is rapidly becoming familiar to Americans through such applications as toll-booth speed passes, building entry key cards, and other "contactless" applications.

The data stored in these radio chips will include all the printed information that is on a U.S. passport, including:

- name
- date of birth
- place of birth (a key to identity theft)
- a digital photograph and a digital face recognition template

RFID chips raise many serious privacy and security issues, especially when placed in identification documents. Those problems include:

1. Skimming

RFID identity documents raise the prospect that terrorists, identification thieves, government agents, marketers, or anyone else could read our identity from a distance and without our knowledge or participation, a problem known as "skimming." For example:

- A retail store or restaurant might gain the ability to capture the identities of those who walk through a portal.
- An FBI agent could covertly sweep a room to discover who is attending a political meeting, mosque, or gun show.
- A terrorist in a foreign country could take advantage of the devices to single the Americans out of a crowd. In effect, these passports would be painting giant bull's eyes on the backs of all who carry them.

2. Cloning

In addition to the problem of skimming, it appears that there exists a potential for wrongdoers to engage in "cloning" these passports – skimming the data off of a passport chip, and then copying it in its entirety onto another RFID chip. The data skimmed from a passport could also be used to forge a duplicate of the actual physical passport, since all the information needed to do so, including the subject's photograph, will be stored "free and clear" on the RFID tag.

3. Surveillance and tracking

The international standard set by ICAO has enormous potential social and political implications that go far beyond passports. What we are witnessing amounts to an effort by the U.S. government and others (whether conscious or not) to leapfrog over the politically untenable idea of adopting a national identity card, and set a course directly toward the creation of a global identity document – or, at least, toward a set of global standards for identity that can be incorporated into a wide variety of national identity documents.

- Once created, these passports will likely become either the template for standardized versions of the driver's license that amount to a de facto National Identity Card, or displace them altogether, thereby advancing government security agencies' perpetual interest in tracking and controlling the movement of citizens.
- Such documents will increasingly be demanded for more and more purposes, not only around the

world, but domestically as well. Features such as digital signatures would greatly enhance the private sector's tendency to piggyback on the perceived "trust value" of these documents – and the inclusion of a remotely readable RFID chip would make such piggybacking very easy.

- Ultimately, widespread adoption of RFID-enabled identity documents would create the potential for the constant, real-time tracking of individuals. As readers are placed in store doorways and an increasing number of other locations for reasons of security or convenience, individuals will constantly be "registering" with this system, whether they know it or not, creating a truly Orwellian result.

The idea of a global identity card is frightening enough. It is even more galling to learn that the US insisted that these new ID cards be built in the most insecure manner, blocking proposals to protect RFID chips placed in identity documents with security measures that are sufficient to protect the privacy of their bearers.

Public input excluded from secretive process

The remotely readable passports being developed by the United States follow standards set by ICAO for biometric passports, which were developed over a period of months in meetings held around the world. The ACLU and other groups concerned about privacy tried repeatedly to participate in the ICAO process, but were ignored. For example, the ACLU tried but failed to arrange attendance for a representative at a March 2004 meeting held in Cairo. An open letter to the ICAO on privacy concerns over the biometric standards met with no response.[2] And the ACLU wrote to ICAO asking to attend a May 2004 meeting in Montreal, and again received no response.

The ICAO's apparent attitude toward public input is reflected in one memo on an upcoming committee meeting obtained by the ACLU, which instructs its recipients on how to register and notes that "Only those persons registered and receiving a Confirmation of Registration/Acceptance will be permitted access to the meetings." It is not clear why a meeting to create public, global standards should be closed to the public, much less when those standards are for a set of global identity documents that have enormous potential social and political implications that should be of concern to the citizens of all nations.

Security to protect privacy was seriously considered

The most disturbing revelation in the new documents is that the State Department heard and discussed the privacy and security vulnerabilities of the new passports, and yet played the central role in fighting for – and winning – a standard that lacked any protections.

Although not reflected in the final standard because of U.S. opposition, the documents obtained by the ACLU show that during the process of creating the standard, extensive consideration was given to privacy and personal security concerns, and of potential solutions to these problems.

An example of the consideration initially given to privacy issues is an extensive, 50-page Technical Report on the "Biometrics Deployment of Machine Readable Travel Documents" from May 2003. The report recommends that "Encryption and digital signing be used to protect the data integrity and data privacy."[3] It also recommends consideration of "Contactless IC Chips with cryptographic co-processors on board," and notes that "Authenticating users before releasing data from the chip provides confidentiality for the information stored on the chip and it also makes skimming and producing duplicate chips more difficult.[4]

The centrality of the privacy issue was also apparent two months later at a July 2003 meeting in London, where ICAO participants met "to explore key issues relating to the introduction and fast-track deployment of globally interoperable machine readable passports."[5] The first day of the conference included meetings with experts from the international banking community to discuss "the securing of the data stored within the IC(s)." And the entire second day of the three-day conference was dedicated to meetings with IT security experts specifically to discuss

> the recommendations of the IT security field and the finance community experts present on the most effective way of securing the data to be recorded in Contactless IC(s) used within MRPs [Machine Readable Passports].[6]

The day's agenda indicates that participants were actively considering a "scheme" for protecting the data on passports, and were seeking the counsel of those with experience in setting up such a system. The agenda included:

- An "Overview of relevant experiences in creating and operating schemes designed to protect encoded data while ensuring global access by those authorized to access and use that data (e.g. PKI)." PKI refers to Public Key Infrastructure, a system for implementing encryption and/or digital signatures (see below).
- "Discussion of the issues to be faced by ICAO in setting up a scheme for protecting the data recorded in the Contactless IC(s) integrated into MRTDs while allowing the data to be accessed and confirmed as authentic and unchanged by a Receiving State."[7]

A slide presentation on the first day of the meeting by security experts with the smart-card vendor Gemplus International seemed to further reinforce the importance of security for participants. Declaring that "Privacy management is a key point in such a program," and the prevention of identity theft a primary goal,[8] they mentioned several ideas, including:

- Setting the system up so that "the user would get the right to check all access (authorized or not)." That way, data would be "exchanged only with trusted terminal (mutual authentication)."
- "Another approach could be the integration of a mechanical button in the contactless layer to release the transmission data, case by case, and under user control."[9]

The Gemplus experts also noted that with regards to skimming, "The specification recommends a distance of 0 to 10cm but we have to be precise [about] the maximum characteristics and measure conditions for the system reader. In fact, it's always possible to 'boost' an unauthorized reader to capture data at 20cm or more for example."[10] In fact, initial tests of the technology now being prepared for use in U.S. passports found that the data could be read from as far away as 30 feet.[11]

Another idea for securing the privacy of the passport data was mentioned in an "e-Passports Task Force" agenda document the following month. That was to use the printed "machine-readable zone" (MRZ) on the passport to encrypt the data on the chip. In other words, a printed bar code on the inside of the passport would contain a code that would be needed to unlock the data on the RFID chip. That would make it impossible to understand to data on the chip without visual access to the printed passport.

The United States weighs in

None of these concerns or the ideas for addressing them, however, were acted upon, chiefly because of opposition from the U.S. government. Despite all the evidence that was presented, and discussion that took place on the gaping security and privacy holes that an unprotected RFID chip would bring, the U.S. position is clearly reflected in a number of the documents.

A State Department memo drafted in August 2003, for example, contains a clear statement of US policy on skimming and RFIDs. On the need for encrypting data, the memo reads:

> US position: Data written to chip and data exchanged between a reader and a passport will be free and clear without the need for encryption. DHS [Department of Homeland Security] concurs with this position.

On Data skimming:

> U.S. Position: There is little risk here since we plan to store only currently collected data and a facial image which are already stored visibly on the passport. In order to facilitate travel through automated boarder crossing gates, the US will recommend against the use of pins or other methods that might be required to unlock a chip for reading. DHS concurs with this position."[12]

This U.S. position was reiterated in an October 2003 document on IC Embedded Passport PKI Requirements," which also systematically rejected the proposed security solutions that had been discussed:

- "Is Encryption Required? The U.S. position is that the data and communication should not be encrypted."
- "Use of MRZ as part of an electronic security scheme. The U.S. position is that the MRZ should not be used for this purpose."
- "Is terminal authentication required? The U.S. position is that terminal authentication should not be required. As the U.S. chip will be a write once device and the information will be free and clear, there is no current need for authentication."[13]

In fact, the only security protection of any kind supported by the United States (and incorporated into the ICAO standard) was a "digital signature" for the passports. The digital signature serves as an electronic "seal" based on an encrypted "hash" (a code generated from the data in the RFID chip) that is included on the chip. If even a single bit of the data on the chip is altered, the hash will no longer match the data, and the data will be revealed as having been altered from the original. But the digital signature is only used to detect alterations to the data in a passport; *it does nothing to protect the passport's content from being openly read and copied.*

While the digital signature protects the interests of the government in not allowing citizens to tamper with their passports, the interests of individuals (in not being tracked or having their identity revealed or stolen) are left utterly unprotected, and indeed far more exposed than ever before. As one State Department document bluntly put it, data can "be read by anyone who chooses to invest in the infrastructure to do so."[14]

And even a robust digital signature scheme does nothing to prevent another apparent vulnerability of passport RFIDs: the copying or "cloning" of a passport, computer chip and all. The U.S. breezily ignored this concern as well. "Concerns over chip copying were raised," a State Department report noted dismissively, "and the probability of such an event (low in the US position) discussed."[15]

Opposition from other countries

The U.S. stance on these issues was not greeted without resistance by the representatives of other nations. "Other countries (most notably Germany) maintain that they need to address skimming before moving

forward," according to a summary of a September 2003 ICAO working group meeting. "UK, Canada, and The Netherlands also presented concerns about skimming." Another U.S. official, reporting on another meeting the same month, wrote that

> Privacy is a big issue and several countries, led by the Germans, objected to the concept of a contact less chip that is "open". Instead they insist that there be some mechanism, such as using a PIN or reading the MRZ before data could be extracted from the chip. Since there was no agreement (we objected) it was determined that it will be an option.[16]

Unintentionally confirming the importance of institutionalizing privacy rights in the form of national privacy commissioners (a step that every advanced-industrial nation except the United States has taken), a U.S. official noted that "European nations seemed intent upon being able to show their privacy commissioners that they had taken reasonable steps to thwart skimming. Canada stated that it 'could not support doing nothing to address the issue of skimming.'"[17] Nevertheless, in a testament to the continuing power of the United States in international forums, that is exactly what the ICAO did to address the issue of skimming: nothing.

Conclusion

The documents obtained by the ACLU clearly demonstrate how international and expert concerns about the security and privacy of computer-enhanced passports were pushed aside by the United States. This at a time:

- When identity theft is at an all-time high
- When resentment of the United States, and potential interest in targeting Americans in terrorist attacks, may be at an historical high
- When "there is already a large body of technical knowledge" on attacking smart cards, as one banking industry representative told ICAO,[18] and when technical knowledge about RFID chips is certain to be democratized around the globe.
- When we are witnessing an explosion of interconnected new technologies for tracking and surveillance that threaten to change the core nature of modern life.[19]

ICAO's push for "the introduction and fast-track deployment of globally interoperable machine readable passports" got its original impetus from the United States, and as we have seen, the U.S. played a decisive role in shaping a standard that includes no security protections to preserve privacy. No American should believe that in adopting these passports their government is merely complying good-naturedly with an international consensus. If anything, ICAO is a phony fig-leaf for a truly American policy, and represents a successful U.S. effort to export that policy around the world.[20]

Because citizen input and groups such as the ACLU were excluded from the process of developing these passports, the newly obtained State Department documents represent our only window into what took place during that process. Unfortunately, it is a very disturbing picture. The State Department must release all documents related to this passport so that the public can gain an accurate, full picture of these passports and the decisions that went into making them, and include the public in further discussions, both at national and international level, about how these problems can be remedied.

Endnotes

[1] Technically, they are not RFID chips, but "Contactless Integrated Circuits". The difference is that true RFIDs can broadcast only an identification number, while the chips that will be placed in passports will contain far more data (eventually up to 514K). Nevertheless the term "RFID" is quickly becoming commonly known, so we will refer to these chips as RFIDs in this paper despite this technical difference in definition.

[2] See ACLU et. al., "An Open Letter to the ICAO," March 30, 2004; online at http://www.aclu.org/Privacy/Privacy.cfm?ID=15341&c=130.

[3] U.S. Department of State, Technical Report: Biometrics Deployment of Machine Readable Travel Documents, Version 1.9, May 19, 2003, p. 49; online at http://www.aclu.org/passports/TechnicalReport.pdf.

[4] Ibid., p. 35.

[5] "Calling Notice – Revision 2: Meeting of ICAO TAG-MRTD/NTWG and ISO/SC17-WG3, 22-24 July 2003, London (United Kingdom)," p. 1; online at http://www.aclu.org/passports/LondonAgenda.pdf.

[6] Ibid., p. 1-2, 4.

[7] "Calling Notice – Revision 2: Meeting of ICAO TAG-MRTD/NTWG and ISO/SC17-WG3, 22-24 July 2003, London (United Kingdom)," p. 1; online at http://www.aclu.org/passports/LondonAgenda.pdf.

[8] Patrice Plessus and Jean Paul Caruana, GemPlus International, "ICAO Specification: Comments on Technical reports," slide presentation, July 22, 2003, slide #2 ("Security aspects: General remarks"); online at http://www.aclu.org/passports/GemPlusSlides.pdf.

[9] Ibid., slide #5 ("Privacy"). Italics in original

[10] Ibid., slide #7 ("Fraud").

[11] Junko Yoshida, "Tests reveal e-passport security flaw," EETimes, August 30, 2004; online at http://www.eetimes.com/tech/news/showArticle.jhtml?articleID=45400010.

[12] Frank Moss, U.S. Department of State, "Special Meeting of PKI Sub-Group of ICAO New Technologies Working Group," unclassified memorandum, August 28, 2003; online at http://www.aclu.org/passports/USPolicyMemo.pdf.

[13] U.S. Department of State, "IC Embeded Passports: PKI Requirements: Version 1.1," October 20, 2003, pp. 13-15; online at http://www.aclu.org/passports/PKIRequirements.pdf.

[14] Simon Godwin and Richard McClevey, "Trip Report: ICAO NTWG PKI Subcommittee Meeting, London, England – September 4 & 5, 2003," undated, p. 3; online at http://www.aclu.org/passports/LondonMeeting.pdf.

[15] Ibid., p. 4.

[16] L. Travis Farris, "Glascow ICO NTWG Meeting," memorandum to ICAO File, November 19, 2003, p. 1; online at http://www.aclu.org/passports/GlasgowMeeting.pdf.

[17] Simon Godwin and Richard McClevey, "Trip Report: ICAO NTWG PKI Subcommittee Meeting, London, England – September 4 & 5, 2003," undated, p. 4; online at http://www.aclu.org/passports/LondonMeeting.pdf.

[18] Colin Whittaker, APACS, "EMV Security – A UK Payment Industry perspective," slide show, undated; online at http://www.aclu.org/passports/IndustrySecurity.pdf.

[19] See Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society," ACLU, January 2003; online at http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39.

[20] The ACLU calls this technique "policy laundering." Just as "money laundering" describes the cycling of illegitimate funds through outside institutions in order to enter them into legitimate circulation, so does policy laundering involve the cycling of policies that lack political legitimacy through outside institutions in order to enter them into circulation despite their lack of acceptance.