



Your Source for Privacy Policy from a Free-market, Pro-technology Perspective

April 4, 2005

Chief, Legal Division
Office of Passport Policy, Planning, and Advisory Services
U.S. Department of State
2100 Pennsylvania Avenue, NW, 3rd Floor
Washington, D.C. 20037

**Re: Comments on RIN #: 1400-AB93
Electronic Passport**

To Whom It May Concern:

Privacilla.org is pleased to make the following comments on the proposed Electronic Passport rule.

Privacilla.org is a Web-based think-tank devoted to privacy as a public policy issue. Visitors to the Privacilla site can find hundreds of pages of information and links relating to all aspects of the privacy issue, including privacy “fundamentals;” commercial privacy including medical, financial, and online privacy; and privacy from government.

Privacilla takes a free-market, pro-technology stance towards privacy, placing it at odds, sometimes, with many other privacy advocacy organizations. The Department is likely to find unanimity among privacy advocates on this proposed regulation, however.

The proposed Electronic Passport rule is inappropriately cavalier about placing citizens’ personal information, unencrypted, on an RFID chip that must be carried in order to travel. The use of RFID rather than some other technology or even the status quo is not justified. Rather than following international bureaucratic consensus, the Department of State should lead organizations like the International Civil Aviation Organization toward standards that protect the privacy of all international travelers.

Understanding Privacy

“Privacy” has long vexed policy-makers because the term is often used casually to describe many amorphous concepts, including security, fairness, freedom from marketing, and so on. To aid in the examination of privacy issues, Privacilla has put

forward a value-neutral definition of the concept. Privacy is *the subjective condition people enjoy when they have the power to control information about themselves and when they have exercised that power consistent with their interests and values.*

Parsing this definition briefly, privacy is, first and foremost, subjective: One person cannot decide for another that he or she enjoys privacy when that person does not believe it — and no regulation can do this either. Privacy relies on having power to control personal information. This goes to whether the legal environment allows a person to take steps that protect personal information from unwanted disclosure. When people have power over personal information, privacy then comes from people’s exercise of that power consistent with interest and values. This goes to consumer awareness and market behavior.

The Department’s proposed regulation falls entirely within the “legal environment” side of this equation — whether consumers may take steps that protect personal information from unwanted disclosure. Because passport regulations condition the exercise of the liberty to travel abroad on information disclosure, travelers do not have legal power to control personal information. This makes it imperative that the Department carefully avoid disclosures and risks of disclosure that Americans find unnecessary and unacceptable.

The E-Passport Proposal

The proposed Electronic Passport regulation would establish the use of a “64 kilobyte contactless integrated circuit chip with an antenna” for storing and communicating citizen data. Though obscured by jargon, we take this to mean a Radio Frequency Identification (RFID) chip.

Because encrypted data takes longer to read, the Department intends not to encrypt the information stored on the RFID chip. As noted in the notice of proposed rulemaking, this creates risks of both eavesdropping — intercepting the communication between RFID chip and reader in border crossings — or skimming — activating and reading the RFID chip surreptitiously with a reader, which may happen anywhere a passport is carried.

The Department discounts the likelihood of eavesdropping and promises to create an “anti-skimming feature” before the new passport is implemented.

Format is Substance

The Department’s notice of proposed rulemaking is inappropriately cavalier about placing citizens’ personal information, unencrypted, on an RFID chip that must be carried in order to travel.

The Department should recognize that the format in which data is stored significantly affects the consequences of storing it. To illustrate: A financial statement delivered on paper by U.S. mail carries one set of security and privacy risks. A financial statement

delivered over the Internet carries a different set of security and privacy risks, just as a financial statement delivered via roadside billboard would have a different set.

Data on an RFID chip is more easily revealed surreptitiously than data printed on sheets of paper that are folded together. It is not appropriate to leave personal data unencrypted on an RFID chip just because “the personal data stored on the passport’s electronic chip consists simply of the information traditionally and visibly displayed on the passport data page.”

This explanation shows that the Department has not thoroughly considered the security and privacy risks of the proposed rule.

Why RFID?

RFID technologies offer many consumer benefits when used in supply chain management and logistics. With RFID, goods on trucks, in trains, and in warehouses can be inventoried without unloading and digging through pallets and packaging. Embedded in or attached to consumer products, RFID can improve customer convenience by permitting receipt-free returns and suppressing post-sale theft. As a personal identification device, RFID already enables keycard holders to quickly enter secure buildings and pass through toll gates.

All these examples are deployments of RFID where consumers either choose or acquiesce to the use of RFID. None are where RFID is legally mandated for entire populations. In most of these implementations, RFID is yet at an early stage of deployment and being used for relatively low-consequence transactions.

The notice of proposed rulemaking is singularly deficient in explaining why RFID technology has been selected for passports. A reference to “improved port of entry performance” suggests that RFID may increase the speed with which U.S. citizens are able to cross international borders.

Though efficiency improvements are always nice, the notice does not discuss the severity of the problem with border crossing speeds, nor whether difficulty with reading passport data is a cause of any such problem. The notice does not discuss what incremental time-savings would occur with chips versus present-day optical character readers.

If chips save significant time over optical character readers, the choice of a contactless RFID chip over a contact chip is not explained. This particularly needs justification in light of the security and privacy concerns that come with RFID chips that would store personal information unencrypted.

The configuration of the RFID chip and reader at border crossings would apparently require the chip to be brought within four inches of the reader, meaning that RFID holds a four-inch advantage over a contact chip. If the Department believes that not having to move passports four inches to make contact with a reader will alleviate congestion at

international borders, it should say so. If it does not believe this, it should select a non-RFID chip at most, and perhaps withdraw the proposal entirely, sticking with optical character recognition.

By no means is it satisfactory to promise an unidentified “anti-skimming feature” before electronic passports are issued. Without an anti-skimming feature already in place, planning and announcing mandatory use of RFID in passports is, at best, premature.

Exercise Leadership

The Department of State should exercise privacy leadership by withdrawing these proposed modifications to the passport. It should study more carefully what changes to passports, if any, are justified and needed to accelerate border crossings given the security and privacy risks in using RFID chips carrying personal information.

The Department should keep in mind that there is no inherent security benefit from using chips. Documents alone are fully susceptible to encryption and other techniques that make them as forgery-proof as any computer chip.

The Department of State should resist following the lead of international organizations like the International Civil Aviation Organization on machine readable document standards, or any others, if those organizations would needlessly compromise the privacy and security of international travelers.

The United States is unique in its sensitivity to the most consequential privacy concern: privacy from governments. Standards that are set in international bodies, representing the “average” international view, are not appropriate to apply to Americans, who have a unique love of freedom and privacy.

In short, the Department of State should place the privacy interests of American travelers ahead of international cooperation. This will redound not only to the benefit of Americans, but to travelers of all nations whose privacy may be put at risk by use of RFID in government-mandated identification documents.

In most applications, Radio Frequency Identification technology holds out tremendous benefits for consumers worldwide. In light of the savings and convenience that will accrue to them, consumers are likely to choose and enjoy, or at least acquiesce to, the benefits of RFID in thousands of different applications. They do not have these options when government mandates RFID, and they are right to reject having this technology forced upon them.

It is regrettable that the Department of State would consider using RFID for the tracking of individuals. This action is precipitous given the early stage for the technology and

given consumer concerns about privacy and technology overall. Appropriate reaction against this proposal will have the unfortunate effect of tarring RFID generally.

The Department should recognize that RFID is good for products, not people. It should withdraw the proposal to use RFID in passports and make use of the perfectly adequate and acceptable technologies that carry fewer security and privacy consequences and concerns.

Thank you for carefully considering these comments.

Sincerely,

James W. Harper
Editor
Privacilla.org