

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528



The DHS Emerging Applications and Technology Subcommittee of the DHS Data Privacy and Integrity Advisory Committee is seeking comments on its draft report titled, "The Use of RFID for Human Identification."

This report will be considered by the full Committee at the June 7, 2006 public Advisory Committee meeting in San Francisco, CA.

Please provide any comments in writing to privacycommittee@dhs.gov, by postal mail, or by fax by 12:00 p.m. EST on May 22, 2006. All comments may be made public on the Privacy Committee's web site.

Data Privacy and Integrity Advisory Committee
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Telephone: 571-227-3813
Fax: 571-227-4171
Email: privacycommittee@dhs.gov

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

I. Introduction

The purposes of this paper are to: (1) address the use of Radio Frequency Identification technology (RFID) by the Department of Homeland Security (DHS) to identify and track individuals; (2) outline the potential data privacy and integrity issues implicated by this use of RFID technology; (3) offer guidance to the Secretary of DHS, program managers, and the DHS Privacy Office on deciding whether to deploy RFID technology to track individuals; and (4) offer steps to consider in order to mitigate privacy and data integrity risks when planning to use RFID to identify and track individuals.

II. Executive Summary

Automatic identification technologies¹ like RFID have valuable uses, especially in connection with tracking things for purposes such as inventory management. RFID is particularly useful where it can be embedded within an object, such as a shipping container.

There appear to be specific, narrowly defined situations in which RFID is appropriate for human identification. Miners or firefighters might be appropriately identified using RFID because speed of identification is at a premium in dangerous situations and the need to verify the connection between a card and bearer is low.

But for other applications related to human beings, RFID appears to offer little benefit when compared to the consequences it brings for privacy and data integrity. Instead, it increases risks to personal privacy and security, with no commensurate benefit for performance or national security. Most difficult and troubling is the situation in which RFID is ostensibly used for tracking objects (medicine containers, for example), but can be in fact used for monitoring human behavior. These types of uses are still being explored and remain difficult to predict.

For these reasons, we recommend that RFID be disfavored for identifying and tracking human beings. When DHS does choose to use RFID to identify and track individuals, we recommend the implementation of the specific security and privacy safeguards described herein.

¹ “Automatic identification technology” (AIT) is used here to refer to means of identifying things or individuals, collecting data about them, and automatically causing that data to be entered into a computer system, with no human interaction. Examples of AIT’s include bar codes, optical character recognition, RFID, biometrics, magnetic stripes, smart cards, and voice recognition. *See* http://en.wikipedia.org/wiki/Automated_identification_and_data_capture. *See also* RFID: APPLICATIONS, SECURITY, AND PRIVACY (Simson Garfinkel and Beth Rosenberg, Editors) (2006) at 4.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

III. Background

RFID is a leading automatic identification technology. RFID tags communicate information by radio wave through antennae on small computer chips attached to objects so that such objects may be identified, located, and tracked. The fundamental architecture of RFID technology involves a tag, a reader (or scanning device), and a database. A reader scans the tag (or multiple tags simultaneously) and transmits the information on the tag(s) to a database, which stores the information.

Transmitting identification data by radio rather than by manual transcription increases the quality, speed, and ease of that information transfer, which is the basis for the technology's appeal. RFID tags can be installed on objects such as products, cases, and pallets. They can also be embedded in identification documents and even human tissue. Both the private and public sectors are increasingly using RFID to track materiel (such as for inventory management), but RFID is also being considered and adopted by DHS and other government agencies for use in tracking people.

While RFID can demonstrably add value to manufacturing, shipping, and object-related tracking, there is an impulse at this time to deploy it for purposes to which it is not well suited. RFID's comparative low cost, invisibility, and ease of deployment in automated tracking often make it appear more attractive than the alternatives. RFID may also address some logistical or efficiency problems in human identification and tracking, but some current and contemplated uses of RFID for tracking people may be misguided. Attempts to improve speed and efficiency through using RFID to track individuals raise important privacy and information security issues.

This paper is not a tutorial on RFID technology itself.² Nor does it address the problem of developing international standards to support widespread deployment of RFID technology efficiently. Rather, this paper addresses only the privacy and data integrity issues raised by the use of RFID when explicitly designed and used for tracking people. It does not discuss the use of RFID on general objects, such as clothing or food items purchased from a store that might used to track people without their knowledge or consent. This latter practice raises far greater privacy concerns than explicit tracking and it should be rejected in all cases except when the security mission calls for tracking individuals about whom suspicion has met an appropriate legal threshold.

² We have included an Appendix to this paper listing background materials on RFID.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

IV. The Legal Basis for RFID Use in Human Identification

We know of no statutory requirement that DHS use RFID technology, specifically, to track people. The major laws, executive orders, and programs under which RFID is being considered or used are either permissive as to technology or not legally binding on the U.S. government.³

In this analysis of RFID as a generic technology, we cannot address all the rights, statutes, and regulations that may limit the use of RFID for human tracking, limit the use of information collected via RFID, or grant individuals rights pertaining to data collected via RFID. When RFID is used for human tracking, the data collected will undoubtedly comprise a “system of records” under the Privacy Act of 1974. People should have at least the rights accorded them by that law when they are identified using RFID. Systems using RFID technology are, of course, also subject to the E-Government Act’s Privacy Impact Assessment requirements.

V. RFID for Human Identification: Clarifying Incorrect Assumptions

A number of DHS programs are premised on the identification of human subjects. At the border in the US-VISIT program, at airports in the CAPPS I program, and at entrances to secure facilities of all kinds, checking identification cards is a routinely used security measure. Behind many of the current ideas for using RFID in human identification is a commonly held misperception that RFID improves the speed of identification. RFID is a rapid way to read data, but *RFID does not identify individuals*. If RFID is tied to a biometric authentication factor, it can reliably identify human beings; but tying RFID to a biometric authentication negates the speed benefit.

A. Controlling Access, Controlling Borders, and Interdicting Suspects

Checking identification is intended to achieve a number of different goals: Facilities managers use identification to control access to sensitive infrastructures that may be damaged or used to harm Americans. They use it to control access to facilities where sensitive information about other infrastructure may be kept, or where security planning or operations are carried out. The government uses identification administratively to track the border crossings of international travelers. At borders and checkpoints,

³ The REAL ID Act, about which regulations are still being formulated, calls for a “machine-readable technology” but does not specify the technology. Homeland Security Presidential Directive 12 calls for “a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).” The State Department adopted RFID technology in the e-passport to meet International Civil Aviation Organization standards, which are not legally binding on the U.S. government.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

identification can help detect and interdict undesirable entrants to the country and known or suspected terrorists.

These identification processes are intended to protect a wide variety of institutions, infrastructures, processes, and persons from a wide variety of threats, each having a different risk profile.

At base, checking identification seeks to interdict potential attackers on our institutions, infrastructure, and people. We make no effort here to determine how well the practice of identifying people achieves this mission, how well identification systems are secured against corruption and fraud, or whether the protection provided by identification-based security outweighs its costs to privacy and other interests. We only address here the difference between those identification processes using RFID and those not using RFID.

We are aware of two reasons to use RFID in identification processes: to increase the speed and efficiency of identification processes and to hinder forgery and tampering with identification documents. An RFID-chipped identification card can quickly communicate information from the card to a reader from a distance, without a line of sight or physical contact between a card and reader. With the proper use of encryption, information on an RFID chip can be rendered very difficult, if not impossible, to forge or alter.

B. RFID Can Reduce Delay at Entrances and Checkpoints

It takes some time to check a traditional identification document. The process typically includes handing the document to a verifier, who must review the information on the card and authorize the bearer to pass, record the bearer's passing, or, if appropriate, detain the bearer. The verifier must also compare the identifiers on the card with the bearer to ensure that the bearer is the person identified by the card.

The use of RFID could dispense with one of these steps by eliminating the hand-over of the card. The other two steps are not affected by RFID. The verifier must still review authorizing information and compare the identifiers on the card with the bearer.

These are distinct processes. The identification information communicated by an RFID-chipped identification card can be used to determine the bearer's authorization, but it is not authorization itself. (An RFID-chipped card, just like any card, could have a separate data element indicating authorization, of course, provided it was secure against forgery and tampering.)

In order for any document or device to accurately identify someone, it must be linked to the person in some way. This is almost always through some form of biometric — a picture, description, fingerprints, or iris scan, for example. A document that is not linked

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

to a person using a biometric is not a reliable identification document, just as someone holding a key to a house cannot be identified as the owner of the house based upon possession of that key alone. The RFID-chipped I-94 Form, for example, is not directly linked to individuals by a reliable biometric. The RFID chip in the form is useful for tracking the location of the form and correlating the form with a specific entry in a visitor database, but the form and the chip are easily transferred from one person to another. If the RFID-chipped I-94 Form were relied upon to indicate the location of a person without separate verification of identity, it would easily be used to defeat the regulation of border crossings.

In terms of speed, the use of RFID probably represents only a marginal improvement in speed over alternatives such as contact chips, 2-D bar codes, and optical character recognition. In some cases, RFID has offered no speed benefit at all. For example, to mitigate some security and privacy concerns, the State Department altered its (RFID-chipped) e-passport to require entering of a PIN number printed on the card to unlock the data on the chip.⁴ The e-passport must be swiped through an optical character reader in order to gain access to the chip. This welcome personal security measure adds back the delay and inefficiency that RFID technology was designed to overcome, obviating the utility of RFID for this application.

RFID can reduce delay at entrances and checkpoints, but typically by only a small margin. Current deployments of RFID either do not provide reliable identification (the I-94) or do not reduce delay (the e-passport).

C. RFID Can Reduce Forgery and Tampering with Identification Documents

Encryption allows information to be encoded in such a way that it is hidden from casual view and any attempt at alteration or forgery can be reliably detected. Communicating information from an identification card via RFID allows encryption to be used, suppressing potential attacks on the integrity of the identification system through forgery and alteration.

There are many technologies other than encryption that also suppress forgery and alteration. These include special inks, laminates, microtaggants, holograms, kinograms, and specialized printing techniques, including microprinting, Guilloche printing, and gradient printing. Encrypted data can be hidden in the pixels on a card, giving the same guarantee against forgery offered by encryption in an RFID chip.

The anti-forgery benefit provided by the use of RFID in identification documents is not a product of its use of radio, but rather the fact that the data is in a digital format. Any data

⁴ Department of State, Electronic Passport final rule, 70 Fed. Reg. 61553, 61554 (Oct. 25, 2005).

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

in digital format can be encrypted. Thus, RFID as such offers no anti-forgery or anti-tampering benefit over alternatives such as contact chips, bar codes, or pixelization.

D. Use of RFID Creates Risks to Individuals

While improving identification-based security by small margins, if any, the use of RFID for human identification may create a number of risks that are not found in conventional and non-radio identification processes. Individuals will likely be subject to greater surveillance in RFID identification. They will be less aware of being identified and what information is transferred during identification, concerns that necessitate transparency in the design of RFID identification systems. And, finally, the use of RFID creates security risks that are not found in non-radio identification systems. These concerns are discussed in the next section.

VI. Effects of RFID for Human Tracking on Privacy and Related Interests

Identification-based security programs create many concerns relating to privacy and related interests. We confine our analysis here to the incremental concerns created by the use of radio to communicate identity information from a card or token to a reader.

A. Increased Surveillance and Eroded Privacy, Anonymity, and Seclusion

In a visual ID-check environment, a person may be briefly identified but then forgotten, rendering them anonymous for practical purposes. In a radio ID-check environment, by contrast, a person's entry into a particular area can easily be recorded and the information permanently stored and repeatedly shared. In this way, RFID may convert identification-based security into an effective surveillance program of all people passing certain locations.

Without formidable safeguards, the use of RFID in identification cards and tokens will tend to enable the tracking of individuals' movements, profiling of their activities, and subsequent, non-security-related use of identification and derived information.

This concern exists with all automatic identification technologies that communicate identification information in digital form. The advantage of being able to easily share such digital information is part of its appeal. The concern could be minimized, however, if identity information was maintained in analog form and digital information was used only to guarantee the security of the card or token against forgery or alteration.

Advanced "identity management" systems can permit cards and tokens to communicate only the specific information relevant to a particular authorization. Early examples exist,

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

including the Clear card used in the Orlando pilot of Registered Traveler's Private Sector Known Traveler Program. This card communicates to the Transportation Security Administration that the bearer of a card is authorized to pass, but does not reveal to the TSA who the traveler is. RFID is not an obvious candidate for such implementations because the speed and efficiency it offers is not useful when travelers must stop to display a machine-readable biometric to a scanner or reader. This system appropriately uses a contact chip.

B. The Difficulty with Notice to Subjects of RFID Identification

It can be disempowering and unfair to collect certain types of information about people without their knowledge. Doing so prevents people from taking steps to conceal information they might prefer not to share. Human identification using RFID has serious potential to deprive people of notice that potentially highly specific, detailed information about them is being collected. (Here, we discuss collection of information consistent with a planned use of the RFID identification system. Unplanned collection of information by outsiders to the system is a security threat, which we will discuss separately below.)

RFID-tagged identification documents present a significant problem in terms of notice, along two dimensions. First, individuals carrying RFID-tagged documents will have a difficult time determining when they are being identified and to whom. Unless people begin carrying radio frequency detectors or purses and wallets that are impermeable to radio frequencies, they will not know when the RFID chips in their identification cards are being scanned. Designing chips to communicate over limited distances can ameliorate, but not eliminate, this problem. Technologies and both government and commercial identification policies may change over time, putting people in the position of being identified at times and places they are not aware of.

Second, people with RFID-tagged documents will have a difficult time determining what information they are sharing when they are identified using RFID. In a visual ID-check environment, people are aware that the information on the card is what is made available to a verifier. Other media make it more difficult to determine. Magnetic stripes, bar codes, and radio waves are not naturally readable to humans, though they can be interpreted by the technically savvy if they use known standards. However, when encryption is used — to defeat forgery and tampering and to secure the radio communication against outsiders — it can also deprive the individual of any way to decipher the content of the communication, rendering him or her powerless to control the use of personal information.

These concerns highlight the importance of open standards and open processes in any use of RFID for human identification. It should be possible to determine what information

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

the cards people carry actually communicate. Because RFID systems can be configured a variety of ways, it is important that the public have information about all the design standards that systems are built to. This disclosure should not be limited to their intended uses, but their maximum capabilities should also be specified. Information about the maker of the chip, the integrator, and the provider of the data system should all be made public so that the design and integration choices can be assessed by outside observers, auditors, and the affected people. Otherwise, RFID-based identification systems will invite misuse, whether they actually are misused or not.

B. Security is a Foremost Concern with Using RFID for Human Identification

Above, we discussed the concerns that exist when RFID is used for human identification as intended. Some of the greatest concerns with RFID in identification documents have to do with uses that are not intended: the security of the radio transmissions. Making identification information available via radio frequency opens up two sources of insecurity, commonly known as skimming and eavesdropping.

“Skimming” is creating an unauthorized connection with an RFID tag in order to gain access to its data. It allows someone not a part of the identification system to gather information surreptitiously. This risk can be controlled a number of ways. One is to block the transmission of radio signals to and from the chip when it is not intended to be in use. A Faraday cage or shield is a wire screen that prevents transmission of radio signals. The State Department’s new e-passport will incorporate this technology. It is more convenient in a “passbook” type document like a passport than a card for which there would have to be a wrapping.

Another way to limit skimming is to encrypt the data transmission so that identification information appears indecipherable to anyone intercepting it that is not authorized to read it. However, this is not a complete solution. Though indecipherable itself, the encrypted information can act as an identifier if it remains the same each time the card is skimmed.

“Eavesdropping” is the interception of the electronic communication session between an RFID tag and an authorized reader, again, in order to gain access to the data being transmitted. As with skimming, depending on the design of the system, an eavesdropper may be able to collect usable information from the communication between an RFID chip and reader even if the communication is encrypted.

One way to suppress eavesdropping is to limit carefully the environments in which identification cards are used. Another is to design the RFID chip so that no two communication sessions appear alike. This may require a relatively simple RFID system to migrate toward the more expensive and complicated “smart card” model.

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

The United States Government Accounting Office addressed the use of RFID technology in a May 2005 report titled *Information Security: Radio Frequency Identification Technology in the Federal Government*⁵ (GAO Report). The GAO Report identified a number of security issues that are implicated by federal (and commercial) use of RFID technology. “Without effective security controls,” the GAO Report stated, “data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users.”⁶ The GAO stated that RFID systems should be designed to:

- Ensure that only authorized readers can read the tags, and that only authorized personnel have access to the readers;
- Maintain the integrity of the data on the chip and stored in the database;
- Ensure that the critical data is fully available when necessary;
- Mitigate the risk of various attacks, such as counterfeiting or cloning (when an attacker produces an unauthorized copy of a legitimate tag); replay (when a valid transmission is repeated, either by the originator or an unauthorized person who intercepts it and retransmits it); and eavesdropping;
- Avoid electronic collisions when multiple tags and/or readers are present; and
- Mitigate the likelihood that unauthorized components may interfere or imitate legitimate system components.

We endorse these as a minimal set of measures to address the issues we have raised here about using RFID for human identification. Many additional data privacy and integrity issues would surface in a specific program that contemplated collection, storage, and use of data collected via RFID. In the next section, we draw our conclusions about the use of RFID in human tracking and suggest “best practices” for the rare case when RFID is the most appropriate technology for that purpose.

VII. Recommendation: RFID Should be Disfavored for Human Tracking.

The case for using RFID to track materiel has been made fairly well. The Department of Defense, for example, has produced a significant study showing the benefits of using

⁵ See GAO-05-551 (May 2005), available at <http://www.gao.gov/new.items/d05551.pdf>. See also Testimony of Gregory C. Wilshusen, Director, Information Security Issues, Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security, June 22, 2005, available at <http://www.gao.gov/new.items/d05849t.pdf>.

⁶ GAO Report at 19.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

RFID to tame the substantial logistical challenges it faces.⁷ We are not aware of a similarly strong case for using RFID to track humans.

RFID can reduce the delay when people pass through chokepoints that require identification. However, transmission of information from cards to verifiers is not a significant cause of the delay in such transactions compared to the authorization and verification steps.

RFID permits the use of encryption, which can control forgery and tampering with identification documents. This is not a unique characteristic of RFID, however. It is part of many digital technologies, including contact chips, bar codes, magnetic stripes, and watermarked printing.

Against these small incremental benefits of RFID are arrayed a large number of privacy concerns. RFID deployments' digitally communicated information is easier to collect, save, store, and process, and is, therefore, more easily converted to surveillance than other methods. The silent, unnoticeable operation of radio waves means that individuals will always have difficulty knowing when they are being identified and what information is being communicated, leaving them vulnerable to increased security risks such as skimming and eavesdropping.

A. Choosing Whether to Use RFID to Track Individuals

When automatic identification technology or RFID are not required or specified by law, the subcommittee recommends that program managers within the U.S. Department of Homeland Security, in consultation with the DHS Privacy Office, explore the following issues to determine if RFID will accomplish their objectives and if, on balance, using RFID technology is appropriate for tracking individuals:

- What is the specific objective of the program?
- What alternatives might accomplish these objectives? (e.g., 2D barcode, optical character recognition, or magnetic stripe)
- What are the drawbacks of these alternatives (e.g. reduced speed, efficiency, or accuracy?)
- Can one or more of these alternatives meet the objectives of the program without raising the privacy and security concerns raised by RFID?

⁷ FINAL REGULATORY FLEXIBILITY ANALYSIS OF PASSIVE RADIO FREQUENCY IDENTIFICATION (RFID), prepared by the Office of the Under Secretary of Defense for Acquisition Technology & Logistics. See full reference in appendix.

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

B. Existing Best Practices

Should they still choose RFID for human tracking, program managers should take a number of steps to protect against the adverse consequences of this technology. We would undoubtedly have specific recommendations for specific programs, but will discuss here a number of existing best practices and recommendations.

The GAO report cited above maintains that many security risks can be mitigated thorough compliance with the Federal Information Security Management Act (FISMA), which requires each agency to develop, document, and implement an agency-wide information security program. Specifically, FISMA requires agencies to:

- Engage in periodic risk assessments;
- Develop risk-based policies and procedures to reduce risks to an acceptable level;
- Develop plans for providing adequate information security for networks, facilities, systems, and groups of systems;
- Engage in security training for personnel and contractors;
- Test the information security policies at least annually, including the testing of management, operational, and technical controls for every major information system;
- Develop a process to detect and report security incidents and a remedial action process; and
- Maintain procedures for continuity of operations in light of a security incident.

As it relates to RFID, an agency can reduce the risk of unauthorized use or access through encryption and authentication.

- Encryption should include the data in the tags, in the air, and when stored in a database.
- Authentication means verifying the claimed identity of a user. It can be used between tag and reader as a way to mitigate security risks. This can help prevent the unauthorized reading and/or writing to tags.

The GAO states that the privacy issues can be mitigated by compliance with existing legislation, including compliance with:

- The Privacy Act of 1974; and
- The Privacy Impact Assessment requirements of the E-Government Act.

Other methods available to the government to reduce privacy risks include the possibilities of:

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

- Employing a deactivation mechanism, or “kill switch” (where feasible);
- Blocking technology, such as that proposed to be used by the US Department of State in its passport jackets;
- Adopting an “opt-in/opt-out” framework, where individuals would be given the choice of whether or not to participate in RFID usage. Under this proposal, people would be informed of the existence of the tags and the type of information that would be collected and then could decide whether to participate in the transaction or not; and
- Mitigating secondary use by reducing the compatibility of readers and tags with other readers and tags.⁸

C. Proposed Best Practices for Use of RFID by DHS to Identify and Track Individuals

The Committee recommends that when DHS chooses to deploy RFID technology to track individuals, it use as many of the following safeguards as possible and appropriate, given the proposed use:⁹

Notice – Individuals should know how and why RFID technology is being used, including what information is being collected and by whom. DHS should consider using standardized icons or other images to highlight the existence and use of RFID tags and the placement of readers;

Choice and Control (Consent) – Individuals should be able to turn off any RFID signal associated with tracking their presence or activities. Where possible, they also should have the option not to participate a program involving the use of RFID technology to track their movements, while maintaining the rights and privileges of other individuals who are participating in a program involving RFID technology. If a national security or other argument weighs against individual control, such an argument should be explicitly stated and debated by representative parties on both sides prior to deciding on the implementation approach.

Securing Readers and Data – To mitigate eavesdropping and skimming, DHS should ensure that only authorized readers can receive signals from DHS-authorized RFID tags.

⁸ Until recently, it was common in government environments to have systems from different vendors performing similar functions that employ incompatible data formats. Lately, such practices have fallen out of favor because of the push towards broad information sharing.

⁹ These proposed best practices draw on a number of sources, including the GAO Report, the EPCglobal Guidelines for Electronic Product Codes for Consumer Products (see http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html), and the ARTICLE 29 WORKING PARTY WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY, 10107/05/EN, WP105 (January 19, 2005) (available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf).

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

Data should be encrypted on tags, in transit, and in the database. DHS should limit carefully the environments in which identification cards are used, and design the RFID chip so that no two communication sessions appear alike. DHS should also keep databases secure and unconnected to the Internet. Access to readers and databases should be limited only to authorized DHS personnel. Overall, DHS should follow the security recommendations laid out in the GAO Report, including conducting a FISMA review of the program.

Avoid Function Creep – DHS should use data collected by RFID technology only for the stated objective. It should keep data for only as long as necessary given the objective.

Education Campaign – If it uses RFID, DHS should engage in an education campaign regarding the use of RFID, including why it is necessary and what rights and protections are afforded to individuals.

VIII. Conclusion

RFID technology may have a small benefit in terms of speeding identification processes, but it is no more resistant to forgery or tampering than any other digital technology. The use of RFID would predispose identification systems to surveillance uses. Use of RFID in identification would tend to deprive individuals of the ability to control when they are identified and what information identification processes transfer. Finally, RFID exposes identification processes to security weaknesses that non-radio-frequency-based processes do not share.

The Department of Homeland Security should consider carefully whether to use RFID to identify and track individuals, given the variety of technologies that may serve the same goals with less risk to privacy and related interests. Should DHS go forward with RFID to identify and track individuals, a number of practices and recommendations exist to guide program managers. More analysis would be needed of specific RFID-based identification programs, particularly as to collection, maintenance, and use of information collected via RFID.

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.

The Use of RFID for Human Identification
A DRAFT REPORT from DHS Emerging Applications and Technology Subcommittee
to the Full Data Privacy and Integrity Advisory Committee
Version 1.0

Appendix — Background Materials on RFID Technology

INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT, GAO-05-551 (May 2005), available at <http://www.gao.gov/new.items/d05551.pdf>

RADIO FREQUENCY IDENTIFICATION: OPPORTUNITIES AND CHALLENGES IN IMPLEMENTATION, DEPARTMENT OF COMMERCE (April 2005), available at http://www.technology.gov/reports/2005/RFID_April.doc

FINAL REGULATORY FLEXIBILITY ANALYSIS OF PASSIVE RADIO FREQUENCY IDENTIFICATION (RFID), prepared by the Office of the Under Secretary of Defense for Acquisition Technology & Logistics, available at http://www.acq.osd.mil/log/rfid/EA_08_02_05_UnHighlighted_Changes.pdf

RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS, A WORKSHOP REPORT FROM THE STAFF OF THE FEDERAL TRADE COMMISSION (March 2005), available at <http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf>

RFID: APPLICATIONS, SECURITY, AND PRIVACY (Simson Garfinkel and Beth Rosenberg, Editors) (2006);

ARTICLE 29 WORKING PARTY WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY, 10107/05/EN, WP105 (January 19, 2005), available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

CDT Working Group Set of Best Practices for the commercial use of RFID, May 1, 2006, available at <http://www.cdt.org/privacy/20060501rfid-best-practices.php>.

This report has not been considered or approved by the Full Data Privacy and Integrity Advisory Committee and has not yet been provided to the Secretary or the Chief Privacy Officer of the Department of Homeland Security as a formal recommendation.