Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport

Marci Meingast
Dept. of Electrical Engineering and Computer Science
University of California
Berkeley, CA
marci@eecs.berkeley.edu

Jennifer King
Boalt Hall School of Law
University of California
Berkeley, CA
jenking@law.berkeley.edu

Deirdre K. Mulligan
Boalt Hall School of Law
University of California
Berkeley, CA
dmulligan@law.berkeley.edu

***Abstract*— New applications for Radio Frequency Identification (RFID) technology include embedding transponders in everyday things used by individuals, such as books, payment cards, and personal identification. While RFID technology has existed for decades, these new applications carry with them substantial new privacy and security risks for individuals. These risks arise due to a combination of aspects involved in these applications: 1) The transponders are permanently embedded in objects individuals commonly carry with them 2) Static data linkable to an individual is stored on these transponders 3) The objects these transponders are embedded in are used in public places where individuals have limited control over who can access data on the transponder. In 2002, the U.S. Department of State proposed the adoption of an "electronic passport," which embedded RFID transponders into U.S. passports for identification and document security purposes. In this paper, we use the U.S. Government's adoption process for the electronic passport as a case study for identifying the privacy and security risks that arise by embedding RFID technology in "everyday things." We discuss the reasons why the Department of State did not adequately identify and address these privacy and security risks, even after the government's process mandated a privacy impact assessment. We conclude with recommendations to assist government as well as industry in early identification and resolution of relevant risks posed by RFID technology embedded in everyday things.**

I. INTRODUCTION

Radio Frequency Identification (RFID) technology has existed for decades. The term RFID is generally used to describe any technology that uses radio signals for identification purposes which, in practice,"means any technology that transmits specific identifying numbers using radio [1]." Over the years, RFID has been used in in a variety of applications, such as inventory management, anti-theft monitoring of consumer merchandise, and the tagging of livestock [2]. In these applications, it is difficult to link information stored on an RFID transponder to a specific individual due to a variety of factors. In anti-theft monitoring and inventory management, the transponder is not permanently embedded in an object but externally applied, and thus easily removed if an individual desires. The transponders in these situations are meant to be of temporary use which the user can control.

Today, new applications for RFID embed RF technology in common objects, or "everyday" things used by individuals, such as library books, payment tokens, and identification cards [3]. Contactless smart cards, used in some public transportation and other electronic purse applications, contain an embedded chip which uses RF induction technology to communicate identifying data to the card reader. While these new applications of RFID can offer benefits, such as decreasing transaction time, they also pose new privacy and security risks for individuals which are not present with more traditional RFID applications. These risks arise out of a combination of factors. First, the transponders are permanently embedded into objects individuals commonly carry with them, making the transponder ever-present, or ubiquitous. Second, the data stored on these transponders is static and can be linked to an individual. Third, the user may be unaware of the presence of the transponder, or the transponder may not clearly signal to the user when and by whom it is being read. Fourth, the objects in which these transponders are embedded are used in public places where unauthorized entities may be able to access the data on the transponder without an individual's knowledge due to the transponder's remote readability and lack of signaling to the individual that any access has transpired. The combination of these factors opens the door to a variety of security and privacy risks, including tracking and hotlisting. In these new applications, the individuals who carry these objects have little if no control over the operation of the transponders. Thus, addressing the privacy and security concerns of individuals these applications pose is dependent on those procuring and designing the system.

The e-Passport is an important example of these new applications of RFID. The project began in 2002, when the U.S. Department of State (DOS) proposed adopting an "electronic passport," or "e-Passport," with an RF transponder embedded in the cover. As the DOS moved forward with this project, it was met with objections regarding the privacy and security risks for passport holders that were unidentified and unaddressed by the DOS's proposal [4]. In 2006, the

This work was sponsored by the Samuelson Law, Technology and Public Policy Clinic at Boalt Hall School of Law, U.C. Berkeley. It was funded in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Qualcomm, Pirelli, Sun and Symantec.

DOS issued the first e-Passports, which were substantially changed from the original proposal, incorporating measures to address some of the criticisms leveled against the project.

In this paper, we discuss the risks posed to individuals by embedding RFID in everyday things using the e-Passport project as a case study. We discuss the privacy and security concerns for individuals and analyze how these concerns were handled in the procurement and development of the e-Passport. In Section II, we provide an overview of the adoption process of the e-Passport. Section III presents an analysis of the security and privacy risks with embedded RF devices in everyday objects and for the e-Passport specifically. Here we identify reasons for the DOS's failure to identify and address these risks even after the government's process mandated a Privacy Impact Assessment. In Section IV, we present both recommendations to improve the adoption process, in order to earlier identify and resolve risks posed by embedded RF technology, as well as analyze the rationale for integrating embedded RF technology into everyday objects. Conclusions are presented in Section V.

II. THE E-PASSPORT AND RFID

A. Timeline of the e-Passport Project

> "Using an embedded electronic chip in the passport to store the information from the passport data page will enhance the security of the document and is expected to benefit travelers by improving the ability of border officials to verify personal identities. The Department plans to use this format because of the enhanced security features and improved port of entry performance provided by the electronic chip technology." - Federal Register Proposed Rule, p. 8305 [5]

The e-Passport project began with the passage of the Enhanced Border Security and Visa Entry Reform Act of 2002 [6]. This act required nations whose citizens are allowed to enter the U.S. under the provisions of the Visa Waiver Program to have a project in place by October 26, 2004 to "incorporate biometric and document authentication identifiers that comply with applicable biometric and document identification standards established by the International Civil Aviation Organization (ICAO) [6]." The legislation neither explicitly directed the DOS to adopt the ICAO standard in the passport, nor directed the DOS to engage in any form of rulemaking if it decided to do so. As a member of the ICAO, the United States in its Visa Waiver Program opted to follow directive 9303 and adopt contactless smart card technology for the e-Passport. According to the ICAO, the key considerations in selecting this technology were global interoperability, reliability, durability, and practicality. While ICAO had originally moved to standardize the use of two-dimensional barcodes for optional capacity expansion, 2-D barcodes have relatively low storage capacity and cannot be reprogrammed. Thus, 2-D barcodes would have difficulty storing biommetric data and other types of information.

The first "Sources Sought Notice" to requisition materials for the e-Passport project was published in a DOS request for proposal in July of 2003 with an original target issuance date for the e-Passport of December 2004. In February 2005, the DOS published a proposed rulemaking for "electronic passports" in the Federal Register soliciting public comment [5]. The rule stated the agencies intention to "introduce an enhanced version of the traditional passport, using an embedded electronic chip to digitally carry the information printed on the data page, a biometric version of the bearer's photo, and coding to prevent any digital data from being altered or removed." The comment period closed on March 4, 2005, and a summary of the comments was published along with the Final Rule in the Federal Register on October 25, 2005. Of the 2,335 comments received, 98.5% were negative, with over 86% expressing security or privacy concerns [4].

The actual issuance date was delayed approximately one year, to December 2005, to a restricted number of U.S. Government employees. Full issuance to the public by all sixteen U.S. passport issuance authorities was expected by the end of 2006. This delay was due in part to revisions made to the project mid-stream after negative reaction from the public to the lack of attention given to the privacy and security concerns of passport holders in the new design. The revisions included the incorporation of an anti-skimming material in the cover of the passport, as well as Basic Access Control (BAC), which derives an unlock code from a physical scan of the machine-readable portion of the data page of the passport [4]. BAC also allows the transmission between the passport and reader to be encrypted. The Final Rule also mentioned that passport readers would incorporate shielding to minimize eavesdropping. Documents we received, pursuant to a Freedom of Information Act request from the DOS, demonstrate that while discussion about security concerns with the e-Passport (specifically skimming attacks) occurred as early as January 2003, tests to examine the e-Passport's vulnerability to skimming and eavesdropping attacks were not requisitioned until February 2005. [1]

B. Technical Requirements

The e-Passport contains an RF transponder, implemented as a contactless smart card, embedded in the cover of each passport. This transponder contains the information currently on the data page of the passport—name, birthdate, country of citizenship, passport number etc.—with the image of the individual stored as a JPEG file. The chosen technology is a passive International Organization for Standardization (ISO) 14443 A & B compliant RF transponder with 64kB of on-board memory. The chip is passive and contains no power source, as it receives power from the RF fields produced by the reader. The standard does not explicitly address the read range of the chip, but it is generally accepted that the read range will be a maximum of 4 inches (10cm) from reader to chip. Changes implemented with the Final Rule included adding a metallic shield (a Faraday cage) to the cover of the passport to prevent skimming, as well as implementing

[1] The results of those tests, performed by the National Institute of Standards and Technology (NIST), have not been released to the public at the time of writing.

Basic Access Control to prevent unauthorized readers from accessing the chip [7].

FOIA documents establish that US officials were dismissive of passport data skimming vulnerabilities and resisted incorporating physical security measures until nearly two years into the development of the e-Passport project. Frank Moss, the Deputy Assistant Secretary for Passport Services, also admitted at that time that the e-Passport's read range was higher than previously stated; 14443 compliant readers could read the e-Passport chip at a range of a meter or more, substantially higher than the ten centimeter range originally stated [8].

III. Security and Privacy Risks With the e-Passport

By design, RFID transponders are remotely readable. This opens up RFID transponders to security and privacy risks such as skimming and eavesdropping by unauthorized users who have an RF reader [9]. Skimming occurs when the data on the RF transponder is read without the owner's knowledge or consent. The unauthorized reader interacts with the transponder to obtain the data. Eavesdropping is the opportunistic interception of information on the chip while the chip is accessed by a legitimate reader. While similar to skimming, eavesdropping may be feasible at longer distances, given that eavesdropping is a passive operation.

While skimming and eavesdropping are possible in any sort of RFID application, they create more of a risk in the new applications of RFID where transponders storing identifying information are embedded in everyday things. Unlike temporary RFID tags that are externally applied to an item, transponders that are permanently embedded in everyday things cannot be easily removed or disabled by an individual, if desired, to avoid skimming or eavesdropping. Since these embedded tags store some form of static data, whether it is the identifying number of the transponder or personally identifiable information, this data can be affiliated with the individual carrying the object. Since the data generally will not change throughout the life of the object, once this data is linked to an individual, it can be used repeatedly as a means of identifying the individual. These objects, from payment cards to passports, are such that they will often be carried or used in public places. This creates greater opportunities for unauthorized entities to access the data. Without security safeguards, the individual carrying the item will neither be unable to limit who accesses the data in public places nor know who is accessing it both due to the remote readability of RFID, and the lack of signaling transponders give to the user that access occured.

While skimming and eavesdropping are problems in their own right, these vulnerabilities can lead to additional risks such as the tracking of individuals, hotlisting, and identity theft. By reading the static information on a transponder, storing it, and following its signal, an unauthorized user can track the transponder and in return, track the individual. For example, with RFID transponders embedded in library books, an entity can track the movement of a book or the person carrying it. On their own, the movements of an individual may not be particularly interesting, but when combined with additional information, it can yield insight into a particular persons movements.

This information becomes more useful if additional information is aggregated. With hotlisting, an unauthorized entity builds a database taking static data from transponders and linking it to other individual identifiers. This data can be used to track an individual or identify a group of people. Whenever the identifier is observed, then the unauthorized entity can identify the individual. For example, the unique identifying number of a transponder in a passport may by linked to a photo of the passport holder and combined with the person's nationality. Thus, whenever that unique identifying number is observed, the unauthorized entity already knows the nationality and image of the person carrying the passport. An unpleasant example given in Halfhill [10] is that of an "RFID-enabled bomb," an explosive device that is keyed to explode at the time of a particular individuals RFID reading. In the case of e-Passports, this might be keyed on the collision avoidance UID. Finally, identity theft is an additional risk. If personally identifiable information is stored on a transponder, such as a name or credit card number, an unauthorized entity can steal this personal data and use it for identity theft.

While incorporating RFID technology in the e-Passport may have made sense to DOS officials from the perspective of managing physical passport security, the DOS did not adaquately consider how adding an RF transponder to the passport transformed it from an inert identification document to a remotely readable technological artifact. Furthermore, because the original design lacked any features that protected the data from undetected reads of the chip or encrypted the data to protect the passport holder's privacy, it undermined the passport holder's personal agency over their identifying data. In fact, the original Proposed Rule for implementation of the e-Passport stated that e-Passport data did not merit encryption 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," and because it would delay port entry processing time and be expensive and complicated due to interoperability issues [5].

An adversary would not only have access to the passport holder's name and birth date, but also to their digital photograph. Using any type of personal data on the passport, from the owner's name to the unique identifying number of the passport, an adversary can track the movements of the passport holder by repeatedly querying the passport. As the Business Travel Coalition explained, a passport could be read by an adversary while "walking down a hotel corridor," allowing him to determine in which guest rooms Americans were staying [11]. Information from the passport obtained through skimming combined with other information gathered from the passport holder's actions and aggregated over time could open up further avenues for crimes against the passport holder, such as stalking, assault, and theft.

Using the remote capabilities of RFID to store and broadcast personally identifiable information has inherent privacy and security risks to passport holders that must be taken into account. As ubiquitous computing researcher Victoria Bellotti notes, "new . . . computing technology is potentially much more intrusive than traditional information technology because of its power to collect even more kinds of information about people, even when they are not directly aware that they are interacting with or being sensed by it [12]." The changes in data format and transmission introduced by the e-Passport increases opportunities for data capture and reuse. Without measures to counteract these threats, the identifying data contained on passports is vulnerable to anyone who purchases an off-the-shelf compliant reader that can read ISO 14443 standard transponders. Armed with such a reader, a skimmer can surreptitiously learn the name, nationality, passport number and other data about the passport holder [9]. As Greely Koch, the Association of Corporate Travel Executives President stated, "[t]he thought that your travel documents could be broadcasting your nationality to those with an interest in harming U.S. citizens is bad enough, but it could also be pinpointing likely targets for pickpockets, thieves, and even providing information to steal [13]."

A. The e-Passport project Failed to Address Security and Privacy Risks to Passport Holders

When the DOS decided to add RF transponders to the U.S. passport, one of the primary considerations was that of document security; the DOS considered RF-enabled passports to be more secure and harder to copy than traditional passports [7]. As the 2004 procurement notice for the e-Passport stated, "including [integrated circuit] chips in passports could provide the border inspection community with a tool that could have significant security benefits [14]." The "significant security benefits" mentioned refer to the tamper-resistance of the documents, and not to any features of the e-Passport that would improve the security of the passport holders. As discussed earlier, risks from embedding RF transponders must be addressed in the design of the system, otherwise the implementation puts the security and privacy of the user in jeopardy. In this section, we examine the DOS's adoption process and how it failed to meet these requirements and evaluate the concerns of its users: the passport holders.

1) Privacy Impact Assessment: In theory, a process exists to discover and address the risks discussed in the previous section: the "Privacy Impact Assessment," or PIA. The eGovernment Act of 2002 requires agencies to engage in a PIA when they develop or procure information technology that collects, maintains or disseminates information that is in an identifiable form [15]. This provision triggers a review of privacy concerns where the agencies' data collection and the underlying purpose of the system remains static, but the technology used to execute it changes. It represents a recognition —the first to the best of the authors' knowledge—by the federal government that technology change alone can warrant a reexamination of policy choices with respect to privacy. The implementation guidance issued by the Office of Management and Budget (OMB) explicitly ties the new PIA process to the Government's National Strategy to Secure Cyberspace, explicitly recognizing the connection between the privacy of personal information and records, and security.

The OMB's guidance memo directs agencies during the development stage of a project to address privacy through "a statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment." In particular it directs agencies to "specifically identify[ing] and evaluat(e)[ing] potential threats (to privacy) [15]." "Major information systems" require "more extensive analyses of: the consequences of collection and flow of information; the alternatives to collection and handling as designed; the appropriate measures to mitigate risks identified for each alternative; and, the rationale for the final design choice or business process [15]."

From a technical perspective the detailed plan of analysis proposed by OMB is heartening. In addition to a needs assessment and functional analysis of the system, it requires threat modeling ("specifically identifying and evaluating potential threats"), the development and consideration of mitigation measures, and even consideration of alternative technologies ("alternatives to collection and handling as designed"). However, the Privacy Impact Assessment for the e-Passport project authored by the DOS falls far below the expectations set in the OMB guidance documents. It neither identifies nor addresses potential privacy risks created by RFID technology. It is a two page document that lacks any specific discussion of RFID. In comparison, the two PIAs conducted by the Department of Homeland Security for the US-VISIT project, which also implements RFID in travel documents, are fourteen and thirty-four pages respectively [16], [17]. The DHS PIAs contain relatively detailed information about the system architecture, data flows, and access controls, and also laid out the privacy threats and mitigators in clear charts. A comparison of the PIAs, without background knowledge of the projects, would lead to the erroneous understanding that the two agencies were undertaking wildly different projects rather than closely related projects – introducing RFID into different forms of travel documents.

2) Rule-making and Public Comment: In considering the adoption of RFID in the passport, public comment, via a Proposed Rule, was solicited via a notice published in the Federal Register [5]. These informal rule-making procedures were set out under the Administrative Procedures Act, referred to as "notice and comment" rule-making.[2] Furthermore, the Proposed Rule for implementation of the e-Passport was, like the PIA, devoid of any serious consideration of the privacy and security issues presented by the introduction of RFID. While the Proposed Rule makes

[2]This rule-making was not required by legislation. One comment charged that the DOS lacked authority to make this change to the passport. However, on its face it is unclear whether this would normally be considered "policy-making," thereby tripping the Administrative Procedures Act process, or considered just a procurement.

numerous statements about the risks posed by eavesdropping and skimming, the statements are dismissive of the probability of such threats materializing, and none are supported by citations to research studies or data.

The notice and comment process aims to facilitate public oversight and engagement in agency decision-making. Given the potential impact of the technology shift, the DOS correctly viewed the technology as worthy of a rule-making. However, the information provided in the Proposed Rule was insufficient to facilitate meaningful public participation in the agency's decision making with respect to the range of detailed technical issues presented by the RF technology.

The Proposed Rule failed to both provide data to support its technology decisions and make the testing methods and data publicly available. Descriptions of the technical specifications of the technology were largely absent from the Proposed Rule. Instead, the Rule referred readers to a list of documents generated by the ICAO. In order to obtain key information about the government's proposal one had to wade through documents at ICAO that have required and optional components. Absent more specific information from the DOS it placed the onus on the public to find and process an enormous amount of technical data in order to determine what the government was using from the ICAO standard and what it was discarding.

The Proposed Rule provided no information about the threats (threat model) and risks considered relevant by the DOS in their decision process. Similarly, it provided no information about the range of testing, let alone the data, which informed the DOS's decisions on technical matters. Given that the Proposed Rule made statements about some potential risks and stated it would not take certain technical precautions to mitigate them—for example, using encryption—it confounded public comment for the DOS to omit the basis for these early conclusions. Researchers and the public were left to wonder for themselves what information and testing the DOS was relying upon in making its technical assessments about risks and threats. Efforts by the public (including researchers and field experts) to evaluate the proposal were hindered by the lack of detailed information about the technical specifications, the threat models considered relevant by the DOS in evaluating the technology, the testing methods used to assess the potential risks, and the results of such testing.

The Proposed Rule, like the PIA, failed to meet the expectations established by the OMB in their guidance to agencies on the conduct of PIAs. It failed to meet the data quality standards and general standards under administrative law for the creation of a record to support agency decision-making. Considering the original target issuance date of the e-Passport was October 2005, soliciting public feedback in February raises questions as to how seriously the role of public feedback was considered by the DOS. Despite the timing and lack of detailed technical information, over two thousand comments were received. These comments, along with an ongoing assessment the DOS had at this point commissioned from the National Institute of Standards (NIST) and media coverage about the concerns raised with the original design led the DOS to announce changes in April 2005 to the e-Passport's specifications to specifically address the privacy and security concerns [18].

3) Security and Privacy Needs of Passport Holders: When reviewing the released documents, one notable omission is the lack of analysis of the security and privacy aspects of e-Passport project from the perspective of its intended users. Ironically, the functional testing of the e-Passport with its companion reader units inadvertently revealed usability issues with the readers. According to a Department of Homeland Security (DHS) document obtained through a FOIA request, mock point-of-entry tests highlighted severe usability flaws. The report concluded that "if [the] technology does not enhance or improve the existing process flow, new reader technology solutions will not be well-received by the POE (Point Of Entry) officer/inspector community [19]."

In contrast, no similar testing or analysis was indicated in the released documents for future e-Passport users. Because the development process did not seek to incorporate user testing or user-centered design principles, it is unsurprising that the original e-Passport design failed to yield appropriate checks for passport-holder security and privacy. As Bellotti notes, privacy concerns "do not necessarily have to do with technical aspects of computer and communications systems; rather, they arise from the relationship between user-interface design and socially significant actions."

4) Lack of Expert Analysis and Scientific Methods: While the DOS is to be commended for engaging the public through the rule-making process, their lack of diligence in proactively identifying the privacy and security risks and incorporating available relevant scientific research undermined the public's ability to meaningfully comment on the proposal as well as the agency's ability to claim that it was responsibly addressing privacy and security concerns.

According to released documents, no independent analysis of the proposed technology was ever requested or conducted. From a scientific perspective, while independent testing is not required, it is useful for mitigating bias. Functional testing for interoperability and durability of the e-Passport was originally included in the project plan, but security testing was only requisitioned late into the project in response to public criticism. The DOS did not commission testing of possible passport security and vulnerabilities by NIST until February 2005, one and one-half years after the original Request for Proposal for the e-Passport and concurrently with the issuance of the Proposed Rule. In contrast, several other nations adopting RF-enabled passports conducted a variety of security tests; we know through released documents that the DOS was aware of these tests as some are mentioned in discussions between department staff in email correspondence.

Due to the absence of information about the DOS's independent evaluation of the technology, it is unclear whether the agency performed any independent evaluation of the security and privacy risks or merely relied upon vendor information and assessments. The documents released in

response to our FOIA request show reliance by the DOS on the input of the Smart Card Alliance, an industry trade group, to formulate its e-Passport plan. The documents illustrate a close relationship between members of the Smart Card Alliance and State Department staff. In several emails, staff members from both groups discuss strategies for building up support for the e-Passport, with Smart Card Alliance members authoring talking points for the Department of State. For example, in one email from the director of the Smart Card Alliance, Randy Vanderhoof, to industry contacts, Vanderhoof asks:

> "Frank Moss [Deputy Assistant Secretary of State for Passport Services] is requesting some help to counter some new attacks against the choices of smart card technology in passports. If you have some input you can provide, please send it to Frank directly [20]."

And in turn, State Department staff demonstrated their unyielding support of the technology in the face of public criticism:

> "This is of course why the NIST/Boulder [testing] is so critical: to get the facts, and not the hyperbole. Indeed, it is the entire chip industry at question here. And in due course, the biometrics industry as well when its turn comes. I think we can do more to mobilize the chip people to articulate more and more broadly . . . I will try to gin up more movement. We are all in this together and the resources need to be better focused and targeted [21]."[3]

As shown by these examples, the DOS was concerned with demonstrating to the public that they were using the "right" technology and had utilized proper judgment regarding security and privacy issues. Frank Moss himself stated in April, 2005 in an exchange with members of the Smart Card Alliance that "maybe I am grasping at straws, but it would be great if we could say that the smart card really doesn't involve any additional risk [20]." Another State Department staffer said in response to the public criticism, "If we don't address skimming successfully this entire initiative will come unglued [22]." The Final Rule, composed months after these statements were made, demonstrates that the DOS did realize that the original implementation raised risks to privacy and security that had to be addressed in design.

IV. RECOMMENDATIONS

While our case study examines the e-Passport specifically, this analysis is applicable for any organization, public or private, considering integrating RF transponders into everyday things used by individuals. In this section, we offer recommendations to address the security and privacy risks inherent in embedded RF applications in this context.

[3]The NIST testing referred to in this excerpt still has not been released to the public at the time of writing.

A. Is RFID The Appropriate Technological Choice?

Embedding RF transponders in common, everyday objects greatly extends the reach of RFID, introducing new and emergent uses, benefits, and risks. As our case study demonstrates, embedding RF transponders in the e-Passport introduced new privacy and security risks for passport users. However, it is still questionable whether the benefits desired from this change of technology in the passport could have been obtained by a technology other than RFID with fewer risks to the intended users. As a draft report from the Department of Homeland Security Emerging Applications and Technology Subcommittee states,

> "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 [23]."

One of the first factors any organization considering embedding RFID into everyday objects should assess is to consider alternatives that offer similar functionality. Depending on the benefits the organization is seeking, 2-D or 3-D barcodes, or other forms of contact-based or optical scan technologies, may provide comparable features while presenting fewer security and privacy risks to users. Because contact-based technologies require a direct physical connection between the data source and the reader to facilitate data transmission, the risk of unauthorized remote accessibility is reduced, and the user is aware that the read is taking place. Thus, some of the privacy and security risks stemming from the remote capabilities of RFID are mitigated when using contact-based technologies.

With regards to the e-Passport, while initial claims by the DOS discussed efficiency as a primary reason for the project, that view was based upon a model with negligible privacy and security measures in place [14]. As the DOS responded to public concern and integrated security features into the e-Passport, claims of increasing efficiency at Points of Entry disappeared as security improvements necessitated visual scans of the passport's data page in order to implement Basic Access Control [7]. Since remote readability becomes unnecessary with this procedural requirement, it is unclear what gains RF transponders offer that contact-based technology could not have provided.

B. Integrating Users Into Design

If RFID is chosen as the best-suited technology, then appropriate design and testing of the overall system is crucial. When integrating RF transponders into everyday objects, not only must the technical design and configuration of the system be tested, but also the ways in which the intended users interact with and conceptualize the system. Thus, it is not enough to embed a transponder in an object and merely test the operation of the transponder. User-centered design principles must be incorporated into the design process from a project's earliest stages in order to ensure a design

consistent with the needs and values of its intended user population.

In private industry, a primary motivation in integrating user-centered design is to create successful products. Beyond that, the goal should be to adopt technology that is not only appropriate and useful to the intended user population, but also considers the users' context and needs, privacy and security concerns foremost among them. As the development of the e-Passport demonstrates, by failing to consider the security and privacy needs and risks of the passport holders, the DOS was forced to redesign the e-Passport midstream to respond to the risks inherent in the original design. One explanation as to why the State Department didn't consider the needs of its users is that the users in this scenario—U.S. citizens—do not have a choice of passport vendors; if a U.S. citizen wishes to travel abroad, he/she must have a passport, and the State Department is the only authority that can issue one. In the consumer world, "designs that don't meet users' needs often fail in the workplace or in the market, resulting in high costs in productivity, frustration, and errors that impact users and their organizations [24]." While users ultimately cannot opt-out of using an e-Passport if they wish to travel, it is likely some will take control of the privacy and security of their personal information by rendering the transponder inoperable, thus undermining the embedded design.

1) Integrate Data Protection Measures: There are many protection measures for data that can be incorporated to increase the security and privacy of the information stored on RF transponders. Encryption, access control, and authentication mechanisms are all means to help protect and secure data. While the DOS did take authentication mechanisms into account initially by digitally signing the data stored on the transponder, it avoided other forms of protections. The Proposed Rule stated that encryption was unnecessary as the data stored on the transponder was identical to the information printed on the passport and as such did not require extra protection nor the additional decreases in efficiency encryption would introduce [5].

While there are some additional costs with implementing these protection measures, in most cases these costs do not outweigh the cost of privacy and security to individuals. These protection measures need to be adequately considered with the users' needs in mind in order to determine whether they should be implemented or not. Recently, researchers at the University of Washington successfully built a working surveillance system using a Nike+iPod Sport Kit, a consumer product consisting of a RF transponder (meant to be placed in a user's shoe) and receiver unit intended for use with an iPod Nano. The kit provides the user workout data via his or her iPod such as running or walking speed and distance. The researchers discovered that not only can the transponder be paired with any receiver, it also broadcasts a unique identifier that can be detected up to 60 feet away while the unit is in motion [25]. While the sensor has a power switch and can be removed from the user's shoe, the product documentation explicitly advises the user to keep the unit powered on and stored in the shoe, despite the product's lack of privacy or security controls.

C. User Control and Awareness

According to user experience authority Adam Greenfield, systems incorporating ubiquitous technologies such as RFID must "default to a mode that ensures users' physical, psychic, and financial safety," "contain provisions for immediate and transparent querying of their ownership, use, and capabilities," and offer the users the ability to opt out, always and at any point [26]." In keeping with these principles, the system designer must ensure that the user's data cannot be accessed without his or her consent or knowledge, as well as incorporate systemic measures to prohibit data leakage to prevent security and privacy threats such as tracking, hotlisting, and identity theft.

A framework for evaluating usability in ubiquitous computing proposed by Scholtz and Consolvo states that trust by an individual is directly related to awareness and control over privacy [27]. Trust, in their framework, is a vital element in the evaluation of an application. Awareness of the system is assessed through a user understanding about how recorded data is used, and the user's understanding of the inferences that can be drawn about him or her by the application. Control is measured by the ability for users to manage how and by whom their data is used, and the types of recourse available to users in the event that his or her data is misused.

For example, giving the passport holder control over how and when passport data is accessed provides him or her greater personal security. Document security is another benefit of the e-Passport stated by the DOS, but the risks of eavesdropping and skimming arguably open the e-Passport to greater risk to the individual than the original paper-based passport. In the original e-Passport design, a Faraday cage was not considered, thus a transponder on a passport could be accessed by an unauthorized user, with appropriate equipment, at any time. In the late stages of the e-Passport adoption process, the DOS decided to incorporate a Faraday cage to limit when the data on the transponder could be read to the times when an individual decides to physically open the passport. Thus, the individual has agency over when data is being read from the transponder and knows when it occurs.

While giving the individual control over the transponder through Faraday cages and the like provides some clarity, a notification signal is also key. This could be an audible beep, a flashing light, or other sensory signal. For example, the FastTrak road toll payment system used in California uses a combination of feedback from an electronic sign posted at the fare crossing notifying the user that the toll was collected, along with with a beeping sound emitted from the transponder signaling a successful data read [28]. Were the transponder read at any other time, the audible beep would alert the user to the unauthorized read.

D. Public Awareness and Policy Measures

With the e-Passport project, the U.S. Government both solicited input from the public as well as performed a Privacy Impact Assessment. While these types of policy options

are not available to every organization considering adopting RFID, for those that do, these measures should be performed early in the design process. In the context of privacy, the PIA process—when undertaken with rigor and access to an appropriate level of scientific and legal evidence—can play an important threshing function assisting agencies in identifying which technology migrations, modifications or deployments have the potential to alter privacy expectations reflected in older systems, establish new de facto privacy and security rules, or in other ways rise to the level of something that looks and feels like policy-making that warrants public engagement. The use of PIAs by other agencies, such as the Department of Homeland Security, has resulted in the identification of privacy and security risks in similar types of projects. While DOS did not engage with the public as early and thoroughly as they could have, it is commendable that they did, as the public feedback and resulting media coverage helped uncover the flaws with the project and apply pressure for resolution.

Furthermore, acknowledging the need for and benefit gained from broad expert consultation, as well as threat modeling and testing that incorporates users' concerns and perspectives is key. Had the DOS invited a broader range of expert and impartial review, it is possible they could have identified many of the issues addressed in the Final Rule far earlier in the process. The same can be said for incorporating security and privacy analysis that specifically addresses the concerns of the future passport holders. Ideally, the final result would have been an e-Passport that managed to balance both the needs of the DOS with the best interests of the public. Whether the result of that process would be a design incorporating embedded RF transponders is open to debate.

V. CONCLUSION

As we have demonstrated, new applications of RFID, where transponders are embedded in the "everyday things" individuals carry with them, create new privacy and security risks that need to be addressed in design. We have used the adoption of the e-Passport by the U.S. Department of State as a case study to illustrate how to address the privacy and security risks to users stemming from the inclusion of embedded RF transponders. Both private and public organizations can incorporate the lessons learned from this project when considering similar applications of RF technology, including ascertaining the true need and benefits for embedding RF in everyday things.

REFERENCES

[1] S. Garfinkel and B. Rosenberg, *RFID: Applications, Security, and Privacy*. Upper Saddle River, NJ: Addison-Wesley, 2006.

[2] RFID Journal, "The History of RFID Technology," 2005. http://www.rfidjournal.com/article/articleview/1338/1/129/.

[3] D. A. Norman, *The Design of Everyday Things*. New York: Currency/Doubleday, 1990.

[4] Federal Register, Vol. 70, No. 205.

[5] Federal Register, Vol. 70, No. 33.

[6] Enhanced Border Security and Visa Entry Reform Act of 2002 - ALDAC No. 1., http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html.

[7] "The U.S. Electronic Passport Frequently Asked Questions," October 2006. http://travel.state.gov/passport/eppt/eppt_2788.html.

[8] U.S. Department of State, FOIA Request, page 41, Novermber 10, 2004.

[9] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in e-Passports," *In IEEE SecureComm*, 2005.

[10] T. Halfill, "Is RFID Paranoia Rational?" 2005. http://www.maximumpc.com/reprints/reprint_2005-01-14a.html.

[11] Business Travel Coalition, "U.S. State Department proposed passport program is bad policy," 2005. http://btcweb.biz/rfidstatement.htm.

[12] V. Bellotti, "Design for privacy in multimedia computing and communications environments," in *Technology and Privacy: The New Landscape*, P. E. Agre and E. Marc Rotenberg, Eds. Cambridge, MA: The MIT Press, 1998.

[13] Association of Corporate Travel Executives, "ACTE says passport bugs could put U.S. travelers at risk," March 28, 2005. www.acte.org/resources/press_release/032905.shmtl.

[14] U.S. Department of State, "Abstract of concept of operations for the integration of contactless chip in the U.S. passport," U.S. Department of State, Tech. Rep., April 2004.

[15] "E-Government Act of 2002," Pub. L. No. 107-347, December 17, 2002, §B.1.a.i. SEC. 208. PRIVACY PROVISIONS. See also, M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

[16] Department of Homeland Security, "US-VISIT Program, Increment 1 Privacy Impact Assessment," December 18, 2003.

[17] ——, "US-VISIT Program, Increment 2 Privacy Impact Assessment In Conjunction with the Interim Final Rule of August 31, 2004," September 14, 2004.

[18] S. K. Goo, "Security concerns prompt passport redesign," *Washington Post*, April 30, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/04/29/AR2005042901501.html.

[19] Department of Homeland Security, "E-Passport Mock Port of Entry Test—'Operational Impact on the Inspection Process'," Nov. 29 - Dec. 2, 2004.

[20] U.S. Department of State, FOIA Request, pg. 218, April 3, 2005.

[21] U.S. Department of State, FOIA Request, pg. 232, April 3, 2005.

[22] U.S. Department of State, FOIA Request, pg. 496, April 15, 2005.

[23] DHS Emerging Applications and Technology Subcommittee, "The Use of RFID for Human Identification - Version 1.0," 2006.

[24] J. Hackos and J. Redish, *User and Task Analysis for Interface Design*. New York: Wiley, 1998.

[25] T. Saponas, J. Lester, C. Hartung, and T. Kohno, "Devices that tell on you: The nike+ipod sport kit," Dept. of Computer Science and Engineering, University of Washington, Tech. Rep., November 2006, http://www.cs.washington.edu/research/systems/privacy.html.

[26] A. Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*. New Riders: Berkeley, CA, 2006.

[27] J. Scholtz and S. Consolvo, "Towards a discipline for evaluating ubiquitous computing applications," Report from National Institute of Standards and Technology. http://www.itl.nist.gov/iad/vvrg/newweb/ubiq/docs/1_scholtz_modified.pdf.

[28] "FasTrak Frequently Asked Questions," 2006. http://www.bayareafastrak.org/static/about/faq_using.shtml#7.