

Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond

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 library books, payment cards, and personal identification cards and documents. 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 present recommendations to assist government as well as industry in early identification and resolution of relevant risks posed by RFID technology embedded in everyday things. We show how these risks exist with many new and upcoming applications of embedded RFID in everyday things and how these applications can benefit from the recommendations for a more secure and privacy preserving design.

Index Terms—RFID, e-Passport,

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 a variety of applications, such as inventory management,

anti-theft monitoring of consumer merchandise, and the tagging of livestock [2]. With previous applications, it is difficult to link information stored on an RFID transponder to a specific individual. In anti-theft monitoring and inventory management, for example, the transponder is meant for temporary use and is externally applied, and thus easily removed if one desires.

Today, new applications for RFID embed RF technology in common objects, or “everyday” things used by individuals, such as library books, payment tokens, and government-issued identification [3]. For example, contactless smart cards, used in some public transportation and other electronic purse applications, contain an embedded chip which uses RF technology to communicate identifying data to the card reader. While these new applications of RFID can offer benefits, such as general convenience and decreased transaction times, they also pose new privacy and security risks for individuals which are not present with more traditional RFID applications.

The new risks associated with these applications 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, these RF-embedded objects 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. 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 that these applications pose is dependent on those procuring and designing the system.

The e-Passport, shown in Figure 1, is an important example of these new RFID applications. The e-Passport project began in 2002, when the U.S. Department of State (DOS) proposed adopting an “electronic passport,” or “e-

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.

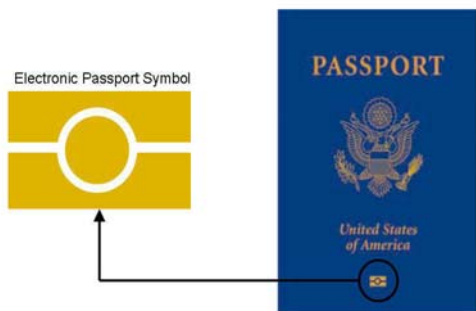


Figure 1. The E-Passport Cover

Passport,” with an RF transponder embedded in the cover. As the DOS moved forward with this project, it 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 DOS issued the first e-Passports, which were substantially changed from the original proposal, incorporating measures which 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. We expand upon the earlier work [5] by discussing the e-Passport process in more detail and addressing additional risks. We also provide a discussion of new and upcoming applications of embedded RFID technology for which these same risks arise and how these applications can benefit from the recommendation we present. 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 specifically, for the e-Passport. In Section IV, we identify reasons for the DOS’s failure to identify and address these risks even after the U.S. government’s process mandated a Privacy Impact Assessment. We present recommendations to improve the adoption process in Section V 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. New applications of RF technology are discussed in Section VI, and conclusions are presented in Section VII.

II. THE E-PASSPORT AND RFID

“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 [6]

A. Timeline of the e-Passport Project

The e-Passport project, from concept to issuance to the public of RF enabled passports, began in 2002 and wrapped up at the end of 2006, as shown on the timeline in Figure 2. The e-Passport project began with the passage of the Enhanced Border Security and Visa Entry Reform Act of 2002 [7]. 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) [7].” 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 originally moved to standardize the use of two-dimensional barcodes for optional capacity expansion, this decision was changed since “2-D barcodes have relatively low storage capacity and cannot be reprogrammed. Thus, 2-D barcodes would have difficulty storing biometric data and other types of information [8].”

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 [6]. The rule stated the agency’s 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 of the e-Passport 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 began at the end of 2006. This delay was partially due to revisions made to the project mid-stream after the

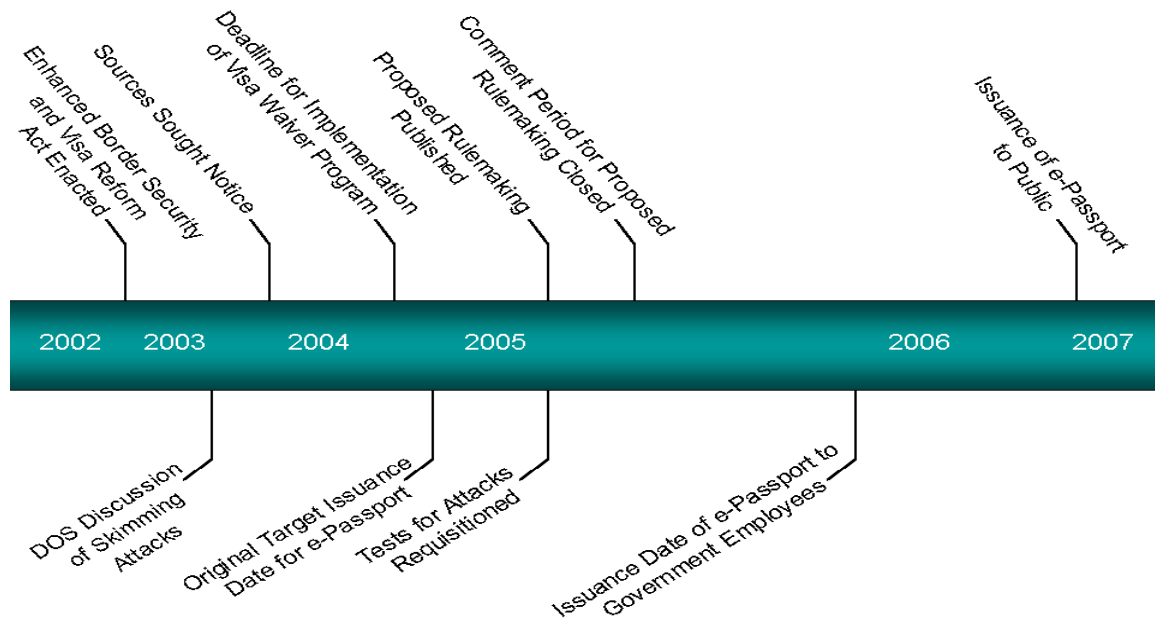


Figure 2. Timeline of e-Passport Process

negative reactions from the public regarding the lack of attention given to the privacy and security concerns of passport holders in the proposed design. The revisions included the incorporation of an anti-skimming material in the cover of the passport, as well as Basic Access Control (BAC), in which an unlock code is derived from a physical scan of the machine-readable portion of the data page of the passport [4]. BAC also encrypts the communication between the passport and reader. The Final Rule also mentioned that passport readers would incorporate shielding to minimize eavesdropping risks. 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 passport holder 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 [4]. The chip is passive and contains no power source, as it receives power from the RF fields produced

¹The 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.

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.

After the concern over privacy and security of the e-Passport, additional items were added to the design. Changes implemented with the Final Rule for the e-Passport include adding a metallic shield (a Faraday cage) to the cover of the passport to prevent skimming. Also, Basic Access Control is implemented in the e-Passport to prevent unauthorized readers from accessing the chip [9].

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. Unauthorized entities who have an RF reader may be able to obtain the information stored on the transponder using these methods [10]. Once data is obtained by these operations, this leads to further risks such as hotlisting, tracking, and cloning. Here we discuss the risks of RFID and how they apply to the e-Passport.

A. General RFID Risks

Skimming and eavesdropping are methods of surreptitiously obtaining information stored on a transponder.

- **Skimming:** Skimming occurs when the data on the RF transponder is read without the owner's knowledge or consent using an unauthorized reader. It is an active operation where an unauthorized reader interacts with the transponder to obtain data.
- **Eavesdropping:** 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 where transponders storing unencrypted identifying information are embedded in everyday things. Unlike temporary RFID tags that are externally applied to an item, transponders that are permanently embedded in an object 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. Because 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 them. These objects, from payment cards to passports, are such that they will often be carried or used in public places, creating 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 occurred.

While skimming and eavesdropping are problems in their own right, these vulnerabilities can lead to additional risks such as the tracking of individuals, hotlisting, identity theft, and cloning.

- **Tracking:** 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 theoretically 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, the aggregated data can yield insight into a person's actions and intentions as well.
- **Hotlisting:** With hotlisting, an adversary 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, the adversary can theoretically identify the individual. For example, the unique identifying number of a transponder in a passport may be 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 by Halfhill [11] is that of an "RFID-enabled bomb," an explosive device that is keyed to explode at the time

of a particular individual's RFID reading. In the case of e-Passports, this might be keyed on the collision avoidance unique identifier.

- **Identity Theft:** Identity theft is an additional risk. If unencrypted 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.
- **Cloning:** Cloning occurs when an adversary makes an identical clone of the data on the RFID transponder. This clone can then be used in place of the original transponder without the user's knowledge. This is of particular concern in implementations used for personal authentication, such as identity documents.

While many of these risks are common to all data storage technologies, the ease and ability of circumvention must be analyzed with respect to a specific technology. With regards to RFID, the ability to read a transponder remotely without the user's knowledge puts the stored information, and the user, at risk.

B. Risks Applied to the e-Passport

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 adequately 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 [6].

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 [12]. 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.

With regards to cloning the e-Passport, although a digital signature is stored on each passport chip to verify

its authenticity, these digital signatures do not bind the data on to a particular passport to a particular chip and offer little defense against passport cloning. Security researcher Lukas Grunwald demonstrated a successful clone of his German e-Passport in August 2006 at the Black Hat security convention [13], [14]. The German e-Passport uses the same standard as U.S. passports.

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 [15].” 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 [10]. 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 [16].”

IV. FAILURE TO ADDRESS RISKS FOR THE E-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 [9]. 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 [17].” 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.

A. *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 [18]. 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) [18].” “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 [18].”

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 I-94 project, which proposed embedding RF transponders in I-94 forms used by foreign visitors to the U.S., are fourteen and thirty-four pages respectively [19], [20]. 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. The documents also included a clear explanation why the specific technology was chosen. 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.

B. Rule-making and Public Comment

In considering the adoption of RFID in the passport, public comment, via a Proposed Rule, was solicited in a notice published in the Federal Register [6]. These informal rule-making procedures were set out under the Administrative Procedures Act, referred to as “notice and comment” rule-making.² 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 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 empirical 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 U.S. 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 [21].

C. 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. The consumer software and electronics industries over the past several decades have integrated design strategies from the discipline of human-computer interaction into their development processes to ensure they build successful products that capture the needs of their users. These strategies, generally referred to as user-centered or customer-centered design, include defining who the users of a technology are, understanding how they use the technology and why, and taking into account the broader context in which the technology is used, including ethical and cultural considerations. Designing implementations of ubiquitous technologies, such as RFID, also pose additional challenges due to their ability to be used in a multiplicity of situations and contexts beyond the traditional computing realm of the office or home desktop computer.

Value-centered design seeks to design technology that accounts for human values in a principled and comprehensive manner throughout the design process [22]. According to Friedman and Kahn, this is an iterative process that integrates conceptual, empirical, and technical investigations. With regards to the e-Passport, a value-centered approach raises conceptual questions, such as: who are the direct and indirect stakeholders affected by this design? How should trade-offs between values such as security and privacy be weighed against the need to move passport holders quickly through a port of entry? After the conceptual framework is defined, then an empirical investigation helps answer these questions by, for example, studying a variety of passport holders (for example, diplomats vs. pleasure travelers) and how they

²This 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.

use the passport. Finally, a technical examination can help answer whether a given technology is more suitable for certain activities and more readily supports certain values while rendering other activities and values more difficult to realize [23].

In the case of the e-Passport, integrating this approach could have demonstrated early on that incorporating RF technology was problematic. No testing or analysis was indicated in the released documents considering the needs of 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.”

Ironically, the functional testing of the e-Passport with its companion reader units was performed, inadvertently revealing 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 [24].”

D. 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.

Finally, while not subject to external assessment, the aforementioned US-VISIT I-94 project, which was piloted by DHS at the same time the passport was under

development, underwent extensive internal testing of the system [25]. Those test results were used to evaluate the feasibility of the project, and due to poor results it was cancelled in February, 2007 [26].

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 [27].”

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 [28].”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. Mr. 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 [27].” Documents obtained through our FOIA request 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. Mr. Moss 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,

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

substantially higher than the ten centimeter range originally stated [29]. Another State Department staffer said in response to the public criticism, “If we don’t address skimming successfully this entire initiative will come unglued [30].” As the Final Rule demonstrated, composed months after these statements were made, the DOS did eventually realize that the original implementation raised risks to privacy and security that had to be addressed in design.

V. 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.

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. The Department of Homeland Security’s own Data Privacy and Integrity Advisory Committee issued a report, adopted in December 2006, suggesting best practices for RFID used in human identification, but also cautioning:

“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 [31].”

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 eradicated, and the user is aware that the read is taking place, mitigating the privacy and security risks. 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 [17]. 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 [9]. 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 [32].” While users ultimately cannot opt-out of using an e-Passport if they wish to travel abroad, 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 [33].

1) *Integrate Data Protection Measures:* There are multiple data protection measures 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 [6].

While there could be additional costs with implementing these protection measures, in most cases these costs do not outweigh the cost of privacy and security to individuals. A loss of trust in the system by users that the system works in their best interests may mean that users will seek to opt-out or undermine the system. To prevent this, an evaluation of protection measures should consider the users' needs as its basis in order to determine whether they should be implemented or not. As an illustration, in 2007, researchers at the University of Washington 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 running shoe) and receiver unit intended for use with an iPod Nano MP3 player. The kit provides the user with personalized workout data, such as running or walking speed and distance, via his or her iPod. The researchers discovered that not only were there no authentication mechanisms between the transponder and the receiver, allowing the transponder to be paired with any receiver, it also broadcast a unique identifier that could be detected up to 60 feet away while the unit is in motion [34]. While the sensor does have a power switch and can also 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 [35]." In keeping with these principles, a system's designers must ensure that a 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, cloning, and identity theft. Additionally, because ubiquitous technologies like the e-Passport can be used virtually anywhere, understanding the contexts in which they are used becomes vital to ensuring a successful design. According to Moran and Dourish, context refers to the physical and social situation in which computational devices are embedded. [36] In regards to the e-Passport, the primary context of use might be at an official port of entry where the potential risks are well-known and security is tightly controlled. However, passports are often used for identification of citizens in many diverse circumstances where security is less controlled, and thus a comprehensive evaluation should also anticipate those uses as well.

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 [37]. 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, cloning, and skimming arguably open the e-Passport holder to greater risks than the original paper-based design. In the original e-Passport design, a Faraday cage was not considered, and a passport's transponder could be potentially 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 data reads on the transponder to the instances when an individual chooses to physically open the passport. This change provided the passport holder with personal agency over when data is read from the transponder.

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 FasTrak road toll payment system deployed in the states of 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 [38]. While this is a model example of user feedback, at the same time the Metropolitan Transportation Commission also silently reads FasTrak transponders for traffic analysis at various points along California highways with no notification to the user. To provide a level of privacy protection, FasTrak anonymizes the toll tag ID numbers and advises users who do not wish to have their transponders read without their knowledge to place the transponder into a Mylar bag when not in active use [38].

D. Public Awareness and Policy Measures

With the e-Passport project, the DOS both solicited input from the public as well as performed a Privacy Impact Assessment. Ideally, any organization, public or private, that is considering adopting RFID in a product or service that will be used in a public place should conduct some form of a PIA, as well as solicit user feedback, whether through public comment or end-user testing. 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 government 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 the U.S. Government in 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 in this case DOS did not engage with the public as early and thoroughly as they could have, it is commendable that they did at all, 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 ultimately be a design incorporating embedded RF transponders is open to debate.

VI. EMERGING APPLICATIONS FOR RFID IN EVERYDAY ITEMS

The e-Passport is just one example, which we use as a case study, of how RFID is being incorporated into everyday items. In this section, we discuss some emerging applications along with their concomitant risks. We also discuss how some of these RFID implementations are subject to "function creep," introducing new risks through the data they create.

A. Emerging Implementations of RF Functionality into Everyday Items

New RF-enabled devices are being used in many applications. The following are just some of the examples of existing and planned RFID implementations that introduce RF functionality into everyday objects.

Enhanced Driver's Licenses: In order to offer a cheaper alternative to the e-Passport for land and sea travel between Canada, Mexico, Bermuda, and the Caribbean countries under the Western Hemisphere Travel Initiative, the State of Washington is the first U.S. state to partner with the Department of Homeland Security to offer an "Enhanced Driver's License" (EDL) to state residents beginning in January of 2008 [39]. The EDL will be used to denote identity and citizenship at land and sea border crossings between the U.S. and Canada, and will incorporate passive ultra high frequency (UHF) RFID technology for remote readability at ports of entry. These UHF cards can be typically read at ranges up to thirty feet. When read, the EDL will transmit an identification number to the reader in order to authenticate the license holder in DHS databases. While this eliminates the risk of reading personally identifiable information without

detection, the static unique identifier, coupled with the high read range of this card, still presents cloning and tracking risks to the card holder.

Washington, along with other U.S. border states, currently participates in the NEXUS system with Canada, a program for frequent border crossers that also uses a contactless ultra-high frequency proximity card for identification. While both systems subject the card holder to cloning and tracking risks, NEXUS cards are purpose specific and conceivably could be carried only when the card holder anticipates crossing the border, while driver's licenses are used as a primary form of identification. Thus, the EDL has a higher likelihood of being carried by users at all times, providing increased opportunities for the EDL to be surreptitiously read.

As of yet, it is unclear if any security measures are being put in place in the EDL to protect against this threat. Unlike the e-Passport, which already had an outside cover prior to the introduction of the RF transponder that could be upgraded to prevent unauthorized reads, the form factor of a driver's license or other wallet-size identification card does not offer a simple solution for shielding the card. While small, card-sized shielding sleeves could be slipped over the card when not in use, this places all of the burden of protecting the card on the license holder. Furthermore, externally removable sleeves are likely to be lost or not even used at all. Presenting one's license for identification is such a common task, particularly when shopping, that many wallets have clear plastic windows to obviate the need to remove the card from one's wallet. A system that requires users to keep their license in an opaque sleeve is likely to fail, particularly if license holders do not understand the technology, its risks, and the risk mitigation shielding offers.

PASS Card: The Department of Homeland Security's own version of the EDL is the People Access Security Service (PASS) Card, which like the EDL is a card format limited use passport incorporating a passive UHF RF transponder [40]. Like the EDL, the intent of the card is to offer a lower cost alternative to the passport for US citizens. The data printed on the card will be identical to that displayed on the data page of the traditional passport, including a facial image, and like the EDL the only data stored on the RF chip will be a unique identifier that links to the card holder's record in DHS's database. DHS has proposed including a protective sleeve with the card to prevent unauthorized reads; this may be more effective for this type of card than for the EDL, since the PASS card will likely not be used for daily identification like the EDL, but it still puts the burden on the card holder to use the sleeve properly.

Payment Tokens: Contactless smart card chips like those used in the e-Passport are working their way into credit cards in the U.S., allowing card holders to make payments typically under twenty-five dollars without a signature by tapping the card on a reader. The first generation of these cards employed no encryption, typically storing the card holder's name, account number, and

expiration date in the clear and thus were vulnerable to eavesdropping, skimming, and replay attacks [41]. It is unclear at the time of writing whether or not the card issuers have begun encrypting card data to prevent financial exploitation or other threats through these types of attacks.

Additionally, U.S. transit authorities, such as Bay Area Rapid Transit (BART) in California, the Metropolitan Atlanta Rapid Transit Authority (MARTA) in Georgia, and the Metropolitan Transit Authority (MTA) in New York, are testing and incorporating contactless smart cards into their fare payment systems. The BART EZ Rider pilot card is loaded with a prefixed amount of money for transit, charged to the user's credit card account, and is automatically reloaded when the stored value on the card falls below a certain amount [42]. The MTA and Port Authority finished pilot testing their SmartLink card in May, 2007 [43]. This card operates similarly to the EZ Rider card and is intended to ease congestion at fare control areas. Due to the typically narrow scope of use of the transit cards and the very limited amount of data stored on and associated with them, these cards are not subject to as severe of security and privacy risks as identification cards are, particularly if they employ encryption, as the BART EZ Rider card does [44].

In general, if payment tokens are implemented with proper reader/card authentication, risks to the card holders are significantly reduced. Instead, the locus of risk shifts to the privacy and security protections implemented by the agency or business for the data collected from each card transaction, since cards linked to individual user accounts can reveal the user's travel or purchase history for as long as the system retains such data.

Human Implants: In what might be the most personal application of RFID of all, human-implantable RF chips are being used for a variety of authentication uses, such as authorizing use of computers, car door and building locks, and even recreational uses such as preferred entrance into nightclubs [45]. While the individuals in these cases have opted to have the chips implanted, there are reports of some employers requiring implants for high-security positions [45]. Additionally, the VeriChip corporation manufactures both implantable chips and wrist bracelets for storing health information and tracking patients in hospitals [46]. In 2007, the company partnered with a nursing home to implant chips in patients with Alzheimer's disease, raising some controversy over the issue of forced implantation [47]. Critics suggested RF bracelets would fulfill the same need, while others opined that the patients may remove them, defeating the purpose of the proposal.

Like identity cards, implants pose many risks, such as hotlisting and tracking, especially if the information on the chip is unencrypted. The cloning of these chips poses a threat as these chips are used for multiple authentication purposes and can provide access to high-security areas or sensitive information. As these implants are not easily removable, once an implant has been cloned and the security

compromised, it may be hard to overcome the effects [48]. Finally, they raise serious ethical considerations when considering who could be required—or forced—to receive an implant. It is questionable at what point requiring RF implants in persons with reduced capabilities or rights, such as mentally incapacitated adults, prisoners, non-citizens, or infants and children leads to a scenario where all members of a society are required to be identified through implanted RF chips.

B. Function Creep

While newly RF-enabled everyday items themselves create concerns, function creep in existing implementations is also an issue. Function creep, the expansion of functions of an item beyond its originally stated purpose, is occurring in some RFID applications. A key example of this is demonstrated with Hong Kong's Octopus transit card. Originally limited to transit payment, use of the card has expanded to include payment at "convenience stores, fast food shops, supermarkets, cake shops, vending machines, schools, and parking," as well as access control for homes and workplaces [49]. Furthermore, the Octopus form factor has even moved beyond cards to include watches and Nokia Xpress mobile phone covers [50]. Another example is California's FasTrak transponder, originally limited to paying bridge tolls, but which will be accepted in the future for parking payments at some local airports [51]. Additionally, the BART EZ Rider card has been proposed to be used for parking payment at BART stations.

In these examples, it is the indispensability of the everyday object—something that users already carry with them everywhere, everyday—that makes function creep irresistible. Unsurprisingly, the next generation of mobile phones, an object that many consider a required part of their everyday lives, will function both as an RF tag and reader⁴ to enable the purchase of goods and services without cash or credit cards, transforming the mobile phone into a hybrid phone-camera-electronic wallet [52].

Systems like these will weave RF transponders into the fabric of people's everyday lives, making the technology truly ubiquitous. While many of the threats discussed in this paper are generally small-scale, low probability threats in 2007, in the near future when most mobile phone users have a portable RF reader and numerous tags they carry with them at all times, the opportunities for data generation and capture through RF will vastly increase, as will the value of that data to marketers, governments, and thieves alike. While security that today relies upon a lack of readers in the hands of the public may work for some applications, like credit cards [41], it will not when both readers and tags are ubiquitous.

Function creep can introduce new risks, where the risk is not derived from the RF implementation itself as much as from the data produced by its use. A significant risk of

⁴The use of RF in mobile phones adheres to the Near Field Communication standard, which operates at 13.56MHz and includes ISO 14443 A and B and FeliCa tags.

function creep is the aggregation of all the data gleaned from the many times per day individuals use RF-enabled things to make purchases, identify themselves, ride public transit, or consume information. While the security of the RF applications themselves will remain paramount, laws and policies governing the capture, sharing, retention, and reuse of the data they generate will also be crucial. If the use of RF-enabled items subjects individuals to unwanted or aggressive marketing tactics, identity or financial theft, or intrusive government monitoring, the promises of convenience and efficiency that manufacturers make about RFID will be undermined.

VII. 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. [Online]. Available: <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] M. Meingast, J. King, and D. Mulligan, “RFID and everyday things: A case study of the security and privacy risks of the u.s. e-passport,” *IEEE International Conference on RFID*, Marci 2007.
- [6] Federal Register, Vol. 70, No. 33.
- [7] Enhanced Border Security and Visa Entry Reform Act of 2002 - ALDAC No. 1. [Online]. Available: http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html
- [8] International Civil Aviation Organization, “ANNEX I: Use of contactless integrated circuits in machine readable travel documents,” International Civil Aviation Organization, Tech. Rep., May 5 2004.
- [9] “The U.S. Electronic Passport Frequently Asked Questions,” October 2006. [Online]. Available: http://travel.state.gov/passport/eppt/eppt_2788.html
- [10] A. Juels, D. Molnar, and D. Wagner, “Security and Privacy Issues in e-Passports,” *In IEEE SecureComm*, 2005.
- [11] T. Halfill, “Is RFID paranoia rational?” 2005. [Online]. Available: http://www.maximumpc.com/reprints/reprint_2005-01-14a.html
- [12] Business Travel Coalition, “U.S. State Department proposed passport program is bad policy,” 2005. [Online]. Available: <http://btweb.biz/rfidstatement.htm>
- [13] Z. Kim, “Hackers clone e-passports,” August 3, 2006. [Online]. Available: <http://www.wired.com/news/technology/0,71521-0.html?tw=rss.index>
- [14] W. Sturgeon. Biometric passport cracked and cloned. [Online]. Available: http://news.com.com/2061-10789_3-6102333.html
- [15] V. Bellotti, “Design for privacy in multimedia computing and communications environments,” in *Technology and Privacy: The New Landscape*, Phillip E. Agre and Marc Rotenberg, Eds., Ed. Cambridge, MA: The MIT Press, 1998.
- [16] Association of Corporate Travel Executives, March 28, 2005. [Online]. Available: www.acte.org/resources/press_release/032905.shtml
- [17] 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.
- [18] “E-government act of 2002,” Pub. L. No. 107-347, December 17 2002.
- [19] Department of Homeland Security, “US-VISIT Program, Increment 1 Privacy Impact Assessment,” December 18, 2003.
- [20] —, “US-VISIT Program, Increment 2 Privacy Impact Assessment In Conjunction with the Interim Final Rule of August 31, 2004,” September 14, 2004.
- [21] S. K. Goo, “Security concerns prompt passport redesign,” *Washington Post*, April 30, 2005. [Online]. Available: <http://www.washingtonpost.com/wp-dyn/content/article/2005/04/29/AR2005042901501.html>
- [22] B. Friedman and P. Kahn Jr., *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*. Mahwah, N.J.: Lawrence Erlbaum Associates, 2003, ch. Human Values, Ethics, and Design.
- [23] K. J. P. Friedman, B. and A. Borning, *Human-Computer Interaction in Management Information Systems: Foundations*. New York: M.E. Sharpe, Inc., 2006, ch. Value Sensitive Design and Information Systems.
- [24] Department of Homeland Security, “E-Passport Mock Port of Entry Test—Operational Impact on the Inspection Process,” Nov. 29 - Dec. 2, 2004.
- [25] U. S. G. A. Office, “Homeland security: Prospects for biometric us-visit exit capability remain unclear,” June 28 2007.
- [26]
- [27] U.S. Department of State, FOIA Request, pg. 218, April 3, 2005.
- [28] U.S. Department of State, FOIA Request, pg. 232, April 3, 2005.
- [29] U.S. Department of State, FOIA Request, page 41, November 10, 2004.
- [30] U.S. Department of State, FOIA Request, pg. 496, April 15, 2005.
- [31] DHS and Emerging Applications and Technology Subcommittee, “The use of RFID for human identification - version 1.0,” 2006.
- [32] J. Hackos and J. Redish, *User and Task Analysis for Interface Design*. New York: Wiley, 1998.
- [33] J. Wortham, “How to: Disable your passport’s rfid chip.” [Online]. Available: <http://www.wired.com/wired/archive/15.01/start.html?pg=9>
- [34] 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. [Online]. Available: <http://www.cs.washington.edu/research/systems/privacy.html>
- [35] A. Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*. New Riders: Berkeley, CA, 2006.
- [36] T. Moran and P. Dourish, “Introduction to this special issue on context-aware computing,” *Human-Computer Interaction*, vol. 16, no. 2-4, pp. 87–97, 2001.

- [37] J. Scholtz and S. Consolvo, "Towards a discipline for evaluating ubiquitous computing applications," Report from National Institute of Standards and Technology. [Online]. Available: http://www.itl.nist.gov/iad/vvrg/newweb/ubiq/docs/l_scholtz_modified.pdf
- [38] "FasTrak Frequently Asked Questions," 2006. [Online]. Available: http://www.bayareafastrak.org/static/about/faq_using.shtml#7
- [39] "Enhanced Driver's License and ID Card." [Online]. Available: <http://www.dol.wa.gov/about/news/priorities/edl.html>
- [40] Department of State, "Card format passport; changes to passport fee schedule," Federal Register 22 CFR Parts 22 and 51, Volume 71, Number 200, October 17 2006.
- [41] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'Hare, "Vulnerabilities in First-Generation RFID-enabled Credit Cards," in *Proceedings of Eleventh International Conference on Financial Cryptography and Data Security*, Lowlands, Scarborough, Trinidad/Tobago, February 2007. [Online]. Available: <http://prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf>
- [42] "EZ rider information." [Online]. Available: <http://www.bart.gov/tickets/types/ezrider.asp>
- [43] "Smartlink-the smart way to go." [Online]. Available: <http://www.panynj.gov/CommutingTravel/path/html/smartlink/>
- [44] "Personal conversation with BART Project Manager Tom Parker, August 11, 2007."
- [45] K. R. Foster and J. Jaeger, "Rfid inside: The murky ethics of implanted chips," *IEEE Spectrum*, pp. 24–29, March 2007.
- [46] Verichip. [Online]. Available: <http://www.verichipcorp.com>
- [47] C. Biever, "Uproar flares over alzheimer's tags," *New Scientist*, p. 14, May 19 2007.
- [48] A. Graafstra, "Hands on: How radio-frequency identification and i got personal," *IEEE Spectrum*, pp. 18–23, March 2007.
- [49] O. Ltd., "Octopus products." [Online]. Available: <http://www.octopuscards.com/consumer/products/en/index.jsp>
- [50] —, "Other octopus products." [Online]. Available: <http://www.octopuscards.com/consumer/products/other/en/index.jsp>
- [51] "Update: SFO's community newsletter," fall 2006. [Online]. Available: <http://www.flysfo.com/web/export/sites/default/download/about/news/update/pdf/SFOUpdateFall2006.pdf>
- [52] B. Charny, "Will your phone become your credit card?" October 2004. [Online]. Available: http://news.com.com/Will+your+phone+become+your+credit+card/2100-1039_3-5406539.html

Deirdre K. Mulligan is the director of the Samuelson Law, Technology & Public Policy Clinic and a clinical professor of law at the UC Berkeley School of Law (Boalt Hall). Before coming to Boalt, she was staff counsel at the Center for Democracy & Technology in Washington. Mulligan writes about the risks and opportunities technology presents to privacy, free expression, and the access and use of information goods. She was a member of the National Academy of Sciences Committee on Authentication Technology and Its Privacy Implications; the Federal Trade Commission's Federal Advisory Committee on Online Access and Security, and the National Task Force on Privacy, Technology, and Criminal Justice Information. She was a vice-chair of the California Bipartisan Commission on Internet Political Practices and chaired the Computers, Freedom, and Privacy (CFP) Conference in 2004. She is currently a member of the California Office of Privacy Protections's Advisory Council and co-chari of Microsoft's Trustworthy Computing Academic Advisory Board. She serves on the board of the California Voter Foundation and on the advisory board of the Electronic Frontier Foundation.

Marci Meingast is currently a Ph.D. candidate in the Electrical Engineering and Computer Science Department at University of California, Berkeley. Her research interests include computer vision, sensor networks, and security and privacy preservation with technology. As part of the Samuelson Law, Technology, & Public Policy Clinic at UC Berkeley's School of Law, she draws upon her technical training to investigate societal issues concerning technology.

Jennifer King is a social technologist who draws upon her training in the social sciences and human-computer interaction to investigate the issues that arise when technology and society collide. As a researcher at the Samuelson Law, Technology, & Public Policy Clinic at UC Berkeley's School of Law, Ms. King focuses on privacy and security in sensor networks and ubiquitous computing (including RFID and video surveillance technologies), usable security, and deviant user behavior in online environments.