U.S. E-Passports: ETA August 2006: Recent Changes Provide Additional Protection for Biometric Information Contained in U.S. Electronic Passports

FRANCIS FUNGSANG*

ABSTRACT

In response to the call for increased U.S. border security, the Department of State has designed a new electronic passport – the "e-passport." The government began issuing e-passports to the general public on August 14, 2006. The new passport stores a digital photograph and personal information in an electronic chip contained within the passport. At the inspection site, a machine reader verifies the information's authenticity by capturing a radio frequency emitted by the electronic chip. However, privacy advocates have raised concerns regarding the need for more protection of such biometric information due to the dangers of: (1) the unauthorized capture of information; (2) clandestine tracking; (3) "function creep;" (4) information concentration; (5) the association of biometrics with criminality; and (6) automation. Therefore, the Department of State has revised its e-passport design to include protective features in addition to digital signatures and active authentication, most notably a cover made of anti-skimming material, and Basic Access Control.

I. INTRODUCTION

After a long, international flight ending with your arrival into the United States, you get off the plane and follow your fellow passengers to the passport inspection area. When your turn arrives, you approach the counter and hand your newly issued passport to the passport control officer. This passport is similar to your old one, but slightly thicker. The officer opens the passport to the data page, which includes a digital photograph, personal information, and two lines of printed characters on the bottom of the page, and swipes the page through a reader next to him. He then activates a camera, which takes a digital photo of your face. A few seconds after waving the passport inches away from another reader, the officer glances at you to compare your face with the images on his screen and in your passport. A short

* Francis Fungsang is a juris doctor candidate at The Ohio State University Moritz College of Law, class of 2007. The author has a B.A. in psychology and biology from Brown University.

time later, he hands the passport back to you, and you head to customs. This experience may seem vaguely similar to every other airport passport inspection you have experienced, but this time a very different sequence of events has occurred. In those brief minutes, the officer has: (1) accessed an electronic chip located within your passport; (2) retrieved a digital photograph of you and your personal information; and (3) verified that your passport was legitimately issued, the information contained within the chip has not been altered, your face and information match the information located on the passport data page and in the chip, and that your name has not been flagged as a wanted criminal or terrorist. Your newly issued passport is an "electronic passport" or simply "e-passport."[1]

This paper chronicles the growing use of biometrics in ensuring U.S. security and the evolution of the United States e-passport over the course of 2005, including its proposed approach, the privacy concerns raised in response to that proposal, and the Department of State's revised approach. However, the Department of State's revision remains susceptible to several privacy concerns and global interoperability problems must be resolved to ensure effective international implementation of e-passports.

II. ORIGINS OF THE U.S. E-PASSPORT

The U.S. government defines a "passport" as "any travel document issued by a competent authority showing the bearer's origin, identity, and nationality if any, which is valid for the admission of the bearer into a foreign country."[2] Subject to certain exceptions,[3] a U.S. citizen may not depart from or enter the United States unless he or she has a valid U.S. passport.[4] The Secretary of State has the authority to grant and issue passports and to allocate the authority to grant, issue, and verify passports.[5] In an effort to upgrade border security, the

---

[1] Roger Yu, *Electronic Passports Set to Thwart Forgers*, USATODAY.COM, Aug. 9, 2005, http://www.usatoday.com/travel/news/2005-08-08-electronic-passports_x.htm.

[2] 8 U.S.C. § 1101(a)(30) (2005).

[3] *See* 22 C.F.R. § 53.2 (2005).

[4] 8 U.S.C. § 1185(b) (2005).

[5] 22 U.S.C. § 211a (2005).

Department of State has begun incorporating facial recognition technology in the next generation of passports.[6] This is done using a biometric identifier contained within electronic chips implanted in the passports.[7] These "e-passports" include enhanced security features, that improve the ability of officials to verify identities and prevent misuse of passports by others.[8]

A. THE US-VISIT PROGRAM

Plans for these enhanced passports have coincided with the development and implementation of the United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"), which also seeks to improve border security by incorporating biometric technology.[9] The US-VISIT program authorized the Department of Homeland Security to require non-immigrants, who are seeking to enter or leave the United States, to provide biometric identifiers at all land, sea, and air ports of entry.[10] Required biometric identifiers include fingerprints and digital photographs.[11] Statutory authority for this program is found in the Immigration and Naturalization Service Data Management Improvement Act of 2000, the Visa Waiver Permanent Program Act of 2000, the USA PATRIOT Act of 2001, and the Border Security Act of 2002.[12] These statutes mandate the implementation of an automated entry-exit system that keeps a record of the arrival and departure of non-immigrants, verifies their identities,

---

[6] Electronic Passport, 70 Fed. Reg. 8,305, 8,305-06 (proposed Feb. 18, 2005) (to be codified at 22 C.F.R. pt. 51), *available at* http://edocket.access.gpo.gov/2005/05-3080.htm [hereinafter Proposed Rule].

[7] *Id.*

[8] *Id.* at 8,305-06.

[9] United States Visitor and Immigrant Status Indicator Technology Program, 69 Fed. Reg. 53,318 (Aug. 31, 2004) (to be codified at 8 C.F.R. pts. 215, 235, 252), GPO Access, *available at* http://a257.g.akamaitech.net/7/257/2422/06jun20041800/edocket.access.gpo.gov/2004/pdf/04-19906.pdf [hereinafter US-VISIT].

[10] *Id.* at 53,318.

[11] *Id.*

[12] *Id.* at 53,318-19.

and authenticates their travel documents using the biometric identifiers.[13] The arrival and departure data is entered into databases integrated with relevant law enforcement and intelligence systems, which are used to determine whether particular non-immigrants should be admitted.[14] Since its inception, Jim Williams, Director of the US-VISIT Program, has reported that the 104 northern and southern U.S. border land ports of entry with biometric capabilities have processed more than 47 million visitors, allowing the Department of Homeland Security to intercept more than 1,000 flagged travelers.[15]

B. THE U.S. VISA WAIVER PROGRAM

Travelers from countries participating in the U.S. Visa Waiver Program are required to enroll in US-VISIT identity verification and admissibility procedures.[16] The Visa Waiver Program allows travelers from twenty-seven countries to visit the United States for up to ninety days without a visa.[17] However, applicable countries must comply with certain requirements, including the issuance of machine-readable, tamper-resistant passports that comport with International Civil Aviation Organization ("ICAO") standards. Congress has extended the deadline for all visa waiver countries to issue e-passports that incorporate biometric identifiers to October 26, 2006, as many applicable countries have been unable to meet the previous October

---

[13] *Id.* at 53,319.

[14] *Id.*

[15] Interview by Lou Dobbs with Jim Williams, Dir. of the US-VISIT Program, Dep't of Homeland Sec., and Randy Hyatt, Dir. of Technology, Information and Architecture Systems at the Gov't Accountability Office (Jan. 27, 2006), *available at* 2006 WLNR 1693246 [hereinafter Interview with Williams & Hyatt].

[16] US-VISIT, *supra* note 9, at 53,322.

[17] U.S. Dep't of State, *Visa Waiver Program (VWP)*, http://travel.state.gov/visa/temp/without/without_1990.html#2 (twenty-seven countries participating in the Visa Waiver Program are: Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom).

2005 deadline.[18] Passports issued before October 26, 2005, must be machine-readable; those issued between October 26, 2005, and October 25, 2006, must either include a digitized photograph on the data page or feature an integrated chip containing information from the data page.[19] The digital photograph must be printed onto the passport data page rather than attaching it with glue or lamination techniques.[20] However, those who hold passports issued before October 26, 2005, will not have to apply for a new, enhanced passport as long as the passport has a machine-readable zone.[21]

Any visa waiver nation that does not incorporate biometric identifiers according to ICAO standards by October 26, 2006, risks denial of its citizens' entry into the United States. In addition, transportation carriers will be fined (up to $3,300) for each visa waiver traveler without an appropriate passport.[22] Additionally, the Department of Homeland Security has reported that twenty-five of the twenty-seven visa waiver countries have fully complied with the October 26, 2005, deadline requirements, with the majority incorporating digital photographs into their passports.[23] Thus far, only Italy and France[24] have been unable to meet the requirements, and

---

[18] *U.S. Extends Visa Scheme Deadline*, BBC NEWS, June 15, 2005, http://news.bbc.co.uk/1/hi/world/europe/4095244.stm.

[19] *Id.*

[20] U.S. Dep't of Homeland Security, *Visa Waiver Program: Passport Requirements Timeline*, http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0021.xml (last visited Mar. 3, 2006).

[21] *Id.*

[22] Press Release, U.S Custody and Border Patrol, Majority of VWP Countries to Meet Digital Photo Deadline (Oct. 26, 2005), http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2005_press_releases/102005/10262005.xml.

[23] *Id.*

[24] Doreen Carvajal, *Another Blow to U.S.-French Ties: A Visa Bottleneck*, N.Y. TIMES, Feb. 2, 2006, at A13, *available at* http://travel2.nytimes.com/2006/02/02/international/europe/02visa.html (dispute between the Ministry of the Interior and public labor unions over who will manufacture the new passports has forced French tourists wishing to visit the U.S. to obtain visas; however, fees and processing delays have created a huge disincentive for U.S. travel).

therefore, visitors from those countries have been advised to apply for a visa before attempting travel to the United States[25]

III. THE PROPOSED U.S. APPROACH

On February 18, 2005, the U.S. Department of State published a proposed rule for the design and implementation of the U.S. e-passport.[26] The Department of State has chosen to enhance the traditional U.S. passport by placing an electronic chip within the passport that contains information included on the passport's data page. In addition, the chip will include a digital version of the bearer's photograph, a unique chip number, and security measures to prevent unauthorized alteration or removal of data contained in the chip.[27] In order to ensure the global interoperability of its e-passports, the Department of State has elected to follow guidelines established by the ICAO regarding "machine-readable travel documents."[28]

A. ICAO STANDARDS FOR MRTD'S

The ICAO, composed of 189 member states and affiliated with the United Nations, creates standards and recommended practices ("SARPs") for the aviation industry.[29] These standards are internationally accepted among the member states and are under constant review to ensure global interoperability in aviation and safety.[30]

---

[25] Majority of VWP Countries to Meet Digital Photo Deadline, *supra* note 22.

[26] Proposed Rule, *supra* note 6.

[27] *Id.* at 8,306.

[28] *Id.* at 8,305.

[29] Int'l Civil Aviation Org. (ICAO), *Making an ICAO Standard*, http://www.icao.int/cgi/goto_m.pl?/icao/en/anb/mais/index.html (last visited Sept. 9, 2006).

[30] *Id.*

The ICAO mandates that "machine-readable travel documents" conform to the standards described in ICAO Document 9303.[31] These standards tackle issues such as the size of the passport and photograph, what biographical information must appear on the passport's data page, and how that data is organized.[32] The specifications for the passport data page require visual (eye-readable) data, as well as a separate data summary that is machine-readable.[33] The required data includes: the document type, issuing state or organization, name of holder, document number, nationality, date of birth, sex, and date of expiration or valid-until date.[34] The machine-readable information is located in the Machine-Readable Zone ("MRZ"), represented by two lines of printed text at the bottom of the data page, each with forty-four characters.[35] An appropriate reader optically scans the two lines containing the information that is located in the Machine-Readable Zone.[36] Additional use of capacity expansion technology (such as contact or contactless electronic chips, or optical cards) to increase information storage space is optional, but if used, the information requires a standardized Logical Data Structure ("LDS") to program it.[37] The standard structure ensures global interoperability for machine-reading of that data.[38] If such optional capacity expansion is utilized, then the only data that ICAO requires the chip to hold is that which is contained in the Machine-Readable Zone of the data page.[39]

---

[31] Int'l Civil Aviation Org. (ICAO), *Machine Readable Travel Documents – Biometrics: Introduction*, http://www.icao.int/mrtd/biometrics/intro.cfm (last visited Sept. 9, 2006).

[32] INT'L CIVIL AVIATION ORG. (ICAO), TECHNICAL REPORT: DEVELOPMENT OF A LOGICAL DATA STRUCTURE- (LDS) FOR OPTIONAL CAPACITY EXPANSION TECHNOLOGIES, REVISION 1.7, 10-16 (May 18, 2004), *available at* http://www.icao.int/mrtd/download/documents/LDS-technical%20report%202004.pdf [hereinafter LDS TECHNICAL REPORT].

[33] *Id.* at 10.

[34] *Id.* at 11, 16.

[35] *Id.* at 10-11.

[36] *Id.* at 11.

[37] *Id.* at 12.

[38] *Id.* at 13.

[39] *Id.* at 15.

The U.S. Department of State's proposal calls for the use of such capacity expansion technology. E-passports use contactless, integrated electronic chips embedded within the documents.[40] Aside from the information contained on the data page, the electronic chip will include a digitized version of the bearer's photo.[41] This digital photo will serve as a biometric identifier, which allows for the incorporation of facial recognition technology at passport inspection sites to verify personal identity.[42]

B. INCORPORATION OF BIOMETRICS

"Biometrics" refer to the automated methods of recognizing a living person through the use of physiological or behavioral traits.[43] In this context, a biometric sample is compared to a biometric "template," which refers to a version of a trait encoded by a computer algorithm such that comparisons of separately recorded traits of an individual sufficiently identify that individual.[44] Common physiological traits used for identification and verification include facial recognition, fingerprints, and iris recognition.[45] "Identification" refers to a one-to-many search in which biometric data is compared against a compilation of biometric templates made up of all subjects enrolled in the system; "verification" refers to a one-to-one match between biometric data taken from a passport bearer and the biometric template created when that bearer enrolled in the system.[46] According to ICAO standards, the use of biometrics is optional – at the

---

[40] U.S. Dep't of State, *The U.S. Electronic Passport*, http://travel.state.gov/passport/eppt/eppt_2498.html (last visited Sept. 9, 2006).

[41] *Id.*

[42] *Id.*

[43] INT'L CIVIL AVIATION ORG. (ICAO), BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS: TECHNICAL REPORT, VERSION 2.0, 8 (May 21, 2004), *available at* http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf.

[44] *Id.*

[45] *Id.*

[46] *Id.*

preference of the issuing State or organization.[47] However, if the issuing authority chooses to incorporate biometrics into its e-passports, ICAO standards mandate the use of a contactless integrated circuit to hold the biometric information.[48] The ICAO has adopted facial recognition as the primary, globally interoperable biometric identifier for machine-assisted identity confirmation, and therefore, an encoded digital photograph must be included in the enclosed contactless electronic chip if biometrics are incorporated into the passport.[49] Furthermore, fingerprint and iris information are optional if the issuing authority desires to incorporate additional identity confirmation techniques.[50]

C. CONTACTLESS INTEGRATED CIRCUITS USING RADIO FREQUENCY IDENTIFICATION

According to ICAO guidelines, the electronic chips used in machine-readable travel documents must follow the ISO/IEC 14443 standards.[51] Reasons for following this particular standard are multifold, including: (1) global interoperability;[52] (2) application of contactless integrated circuits ("ICs") to both staffed and automated border inspection methods;[53] (3) the increasing availability of radio frequency ("RF") reader machines that can read contactless ICs; (4) the durability of contactless ICs; (5) the inclusion of anti-collision procedures, which prevent multiple readings if multiple passports are

---

[47] LDS TECHNICAL REPORT, *supra* note 32, at 22.

[48] *Id.* at 13.

[49] *Id.* at 22.

[50] *Id.*

[51] INT'L CIVIL AVIATION ORG. (ICAO), USE OF CONTACTLESS INTEGRATED CIRCUITS IN MACHINE READABLE TRAVEL DOCUMENTS: VERSION 4.0, 6 (May 5, 2004), *available at* http://www.icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf [hereinafter USE OF CONTACTLESS ICS].

[52] *Id.* at 7 (the radio frequency band required by ISO/IEC 14443 is available worldwide).

[53] *Id.* (staffed border inspections required the passport bearer to surrender his or her passport to a border official, whereas in automated inspections the bearer approaches an automated gate with the passport and is either permitted or denied entry or exit).

in the active range of the RF reader; (6) the availability of data storage to encode the data structure and biometric data; and (7) ease of incorporation into machine-readable travel documents.[54]

Silicon chips represent the optimal solution for machine-readable travel document data storage, as opposed to alternatives such as bar codes and optical cards that respectively suffer from low storage capacity and impracticality.[55] Silicon chips are widely used today in bank cards and other "smart cards," which are contact integrated circuit cards (requiring physical contact to transmit data).[56] However, these are impractical for e-passport purposes due to the need for physical swiping, and potential interference from dirt or moisture.[57] Contactless cards that use silicon chips, on the other hand, utilize radio frequencies ("RF") that can transmit data from a distance between the card and an RF machine reader, permitting Radio Frequency Identification ("RFID").[58] Such cards are already used in tollbooths, of which E-ZPass is the most notable example. In addition, contactless integrated circuits, consisting of an electronic chip and antenna, can take the form of plastic sheets that are easily incorporated into laminated passport covers or pages.[59]

The contactless integrated circuit in e-passports would rely on the radio frequency machine reader for power, due to the impracticality of incorporating battery power into the passports itself.[60] Once a suitable machine reader is in range, the reader would generate a strong radio frequency electromagnetic field from its antenna, thus activating the circuit.[61] Using a "load modulation" process that varies the amount of energy it draws from the electromagnetic field, the contactless integrated circuit would then be able to transmit information to the

---

[54] *Id.* at 7-8.

[55] *Id.* at 9.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.* at 10.

[61] *Id.* at 11.

reader.[62] The machine reader itself would consist of an antenna, a control module, and a high frequency module for transmitting and receiving.[63] The ISO/IEC 14443 standard sets the RFID frequency at 13.56 MHz with a wavelength of 22.1m.[64] This standard limits the maximum strength of the electromagnetic field and asserts a reliable range of up to 10 cm between the circuit and reader.[65] In addition, radio frequency readers can read multiple contactless circuits simultaneously, thereby increasing the speed and convenience of the process.[66] The suggested lifespan of an e-passport incorporating a contactless integrated circuit is ten years, which represents the amount of time the circuit can store its electrical charge.[67]

D. DIGITAL SIGNATURES: USING PKI AND ACTIVE AUTHENTICATION

The U.S. Department of State has also followed ICAO standards for information security by requiring digital signatures with a Public Key Infrastructure ("PKI") scheme to be stored on the electronic chip.[68] PKI is used to protect the information contained in the contactless circuit from tampering by confirming the authenticity and integrity of the data and components.[69] Authenticity refers to confirmation that the data structure and components were created by the issuing authority; integrity refers to confirmation that the data

---

[62] *Id.* at 10-13.

[63] *Id.* at 11.

[64] *Id.* at 12.

[65] *Id.* at 16.

[66] *Id.* at 10.

[67] *Id.* at 17.

[68] Proposed Rule, *supra* note 6, at 8,306.

[69] INT'L CIVIL AVIATION ORG. (ICAO), TECHNICAL REPORT: PKI FOR MACHINE READABLE TRAVEL DOCUMENTS OFFERING ICC READ-ONLY ACCESS: VERSION 1.1, 4, (Oct. 1, 2004), *available at* http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf [hereinafter PKI TECHNICAL REPORT].

structure and components have not been altered from that created by the issuing authority.[70]

The e-passport must prove possession of a private "key" in the form of a series of numbers, before the radio frequency machine reader recognizes the information contained within the chip as authentic.[71] The reader first sends an 8-byte "challenge" to the contactless circuit contained in the e-passport, which digitally "signs" the value and returns it to the reader.[72] The reader then verifies the response by comparing it against the public "key" for that passport.[73] This high strength digital signature prevents any copying of the digital data and proves that the read data came from an authentic chip that has not been substituted or amended.[74] Each country using such active authentication procedures generates its own public and private "keys," which will be distributed to other participating countries if those countries sign certain certificates entrusting those countries with the "keys."[75] Therefore, if personal or other information must be updated, the e-passport would have to be replaced rather than amending the existing information in the chip.[76] If a bearer requests an updated e-passport within one year of its original issuance, the replacement would be provided free of charge.[77]

IV. OPPOSITION TO THE U.S. DEPARTMENT OF STATE E-PASSPORT PROPOSAL

After publishing its U.S. e-passport proposal in the Federal Register on February 18, 2005, the Department of State designated a

---

[70] LDS TECHNICAL REPORT, *supra* note 32, at 12.

[71] Ari Jules, David Molnar & David Wagner, *Security and Privacy Issues in E-passports* 9, *available at* http://eprint.iacr.org/2005/095.pdf.

[72] *Id.*

[73] *Id.*

[74] PKI TECHNICAL REPORT, *supra* note 69, at 18.

[75] *Id.* at 12-13.

[76] Proposed Rule, *supra* note 6, at 8,306.

[77] *Id.*

forty-five day period for public comment until April 4, 2005.[78] Within that time period, the Department received a total of 2,335 comments: 98.5% were categorized as negative, 1% as positive, and 0.5% as neutral, with the vast majority of negative comments citing security and/or privacy concerns.[79] Outspoken privacy advocates have voiced several concerns regarding the incorporation of biometric information in e-passports, especially with the controversial use of RFID to transmit data from a contactless integrated circuit to a machine reader.

A. UNAUTHORIZED CAPTURE OF INFORMATION

Concerns primarily deal with potential capture of the RFID frequency and leakage of personal and biometric information. Clandestine capture of the RFID frequency may occur in two ways: "skimming" and "eavesdropping." "Skimming" refers to the formation of an unauthorized connection with the contactless integrated circuit to gain access to the information within.[80] "Eavesdropping" refers to the unauthorized interception of data transmitted between a contactless integrated circuit and a radio frequency machine reader.[81]

1. LACK OF ENCRYPTION

Privacy advocates have expressed concern over the lack of encryption for the information in the contactless chip, because of its vulnerability to "skimming."[82] Although digital signature and public

---

[78] *Id.* at 8,305.

[79] Electronic Passport: Final Rule, 70 Fed. Reg. 61,553, 61,553 (Oct. 25, 2005) (to be codified at 22 CFR pt. 51), *available at* http://edocket.access.gpo.gov/2005/05-21284.htm [hereinafter Final Rule].

[80] *Id.* at 61,554.

[81] *Id.*

[82] Electronic Frontier Foundation (EFF) et al., Commentary, *Comment in Response to U.S. Department of State's Request for Comment Regarding the Issuance of E-Passports Using RFID Technology* 7 (Apr. 4, 2005), *available at* http://www.eff.org/Privacy/Surveillance/RFID/RFID_passport.pdf [hereinafter *EFF Comment*].

key infrastructure measures are in place to prevent amendment of or tampering with data, the Department of State has chosen not to encrypt the data.[83] The Department has justified the lack of encryption for the following reasons: (1) the data stored in the contactless electronic chip is the same information displayed on the data page of the traditional passport; (2) encryption would increase processing time at ports of entry because encrypted data takes longer to read; and (3) encryption may hinder global interoperability because of elevated technical requirements.[84] However, privacy advocates have disputed the merits and truth of these arguments.[85]

2. THE BROADCAST OF INFORMATION

RFID signals continuously transmit the data contained in the contactless chip, and therefore without sufficient protection any unauthorized radio frequency reader, possibly available on the open market, may capture the signals.[86] Lee Tien, an attorney with the Electronic Frontier Foundation, identified three aspects of RFID tags that create privacy issues: (1) promiscuity, in that they will respond to any compatible reader; (2) remote readings, in that RFID chips can communicate at a distance and through certain materials; and (3) stealth, in that these tags can appear inconspicuous as well as transmit information without the bearer's knowledge.[87] The National Institute of Standards and Technology has demonstrated that RFID signals with digitally signed personal data can be captured by an antenna-equipped reader from up to thirty feet away, much farther than the ICAO specifications restricting the range to ten centimeters.[88] Thus, the holder of an e-passport with insufficient protection may be continually

---

[83] Proposed Rule, *supra* note 6, at 8,306.

[84] *Id.*

[85] *EEF Comment*, *supra* note 82, at 7.

[86] *Id.* at 10.

[87] Lee Tien, Electronic Frontier Foundation (EFF), *RFID Policy: What Does Congress Need to Know?, available at* http://www.eff.org/Privacy/Surveillance/RFID/RFID_one_pager.pdf.

[88] Junko Yoshida, *Tests Reveal E-Passport Security Flaw*, EE TIMES, Aug. 30, 2004, http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=45400010.

transmitting his personal information, national identity, and digitized picture to anyone from thieves to terrorists.[89]

The Association of Corporate Travel Executives[90] and the Business Travel Coalition[91] have both released press statements on March 28, 2005 condemning the Department of State's e-passport proposal. Both organizations were particularly concerned about the dangers of broadcasting personal information such as one's nationality while traveling on business outside the United States, especially to those interested in identifying and harming U.S. citizens.[92] Furthermore, inclusion of personal information such as the e-passport holder's name, date of birth, and a digitized photograph in the contactless integrated circuit would increase the risk of identity theft if unauthorized parties captured such information.[93]

3. POTENTIAL SOLUTIONS

Some experts recommend the enclosure of e-passports with "Faraday cages," named after the scientist Michael Faraday, who found that an electrical charge given within a hollow conductor will spread over the outside of the conductor, producing no electrical field inside the conductor.[94] The "Faraday cage" is made of material that will prevent dispersion of the RFID signal.[95] However, even if such "Faraday cages" are utilized, the RFID signals are still susceptible to unauthorized "eavesdropping" when the "Faraday cage" is removed or

---

[89] *Id.*

[90] Press Release, Jack Riepe, ACTE Global Communications Director, ACTE Says Passport "Bugs" Could Put U.S. Travelers At Risk (Mar. 28, 2005), *available at* http://www.acte.org/resources/press_release.php?id=56.

[91] Press Release, Kevin Mitchell, U.S. State Department Proposed Passport Program Is Bad Policy (Mar. 28, 2005), *available at* http://btcweb.biz/rfidstatement.htm.

[92] *Id.*; Riepe, *supra* note 90.

[93] Jules, Molnar & Wagner, *supra* note 71, at 5.

[94] RF Safe, *Faraday Cage*, http://www.rfsafe.com/research/rf_radiation/shielding_rf_hazards/faraday_cage.htm (last visited Aug. 6, 2006).

[95] Jules, Molnar & Wagner, *supra* note 71, at 2.

the e-passport is opened during inspection.[96] Privacy advocate Bill Scannell, the Electronic Frontier Foundation, and the Electronic Privacy Information Center, amongst others, have advocated that unauthorized capture of RFID information and the associated risks could be eliminated by simply switching to contact integrated circuits (requiring physical contact with the machine reader).[97] Not only does such a switch eliminate the "skimming" and "eavesdropping" issues, but consumers are already accustomed to and are aware of the risks of such technology, due to the widespread use of credit cards and other swipeable contact cards.[98] Other options that avoid implementing RFID include "2-D barcodes," readable at a distance, and optical memory stripe cards, which require presenting the card to the reader at a certain distance and orientation.[99] Furthermore, these alternatives avoid the need for encryption. Renowned security technologist Bruce Schneier speculates that the only reason for choosing the riskier contactless chip is that the U.S. government is actively seeking the ability to stealthily capture the information continually broadcasted for itself, to identify certain individuals or groups of people.[100]

B. CLANDESTINE TRACKING

As long as the information within a contactless integrated chip is freely broadcasted, anyone who can access the information with an unauthorized radio frequency reader could clandestinely track an individual.[101] Every RFID tag contains a unique identifying number that distinguishes one e-passport holder from another carrying a

---

[96] *Id.*

[97] *EFF Comment*, *supra* note 82, at 6.

[98] *Id.*

[99] *Id.*

[100] Bruce Schneier, *Does Big Brother Want to Watch?: Passport Radio Chips Send Too Many Signals*, INT'L HERALD TRIB., Oct. 4, 2004, *available at* http://www.iht.com/articles/2004/10/04/edschneier_ed3_.php.

[101] *EFF Comment*, *supra* note 82.

different RFID tag.[102] Tracking would therefore allow unauthorized users to monitor and record a specific individual's actions.[103]

RFID technology has garnered much press recently for its application in the retail industry by large companies such as Wal-Mart and Walgreens. Walgreens has begun incorporating RFID tags in promotional store displays to analyze the impact of the displays and their locations on sales.[104] Seventy protestors filled the sidewalks next to a Dallas Wal-Mart to protest the store's use of RFID to tag individual consumer items,[105] such as the Hewlett-Packard printer/scanners.[106] Privacy advocates such as Katherine Albrecht, founder of Consumers Against Supermarket Privacy Invasion and Numbering ("CASPIAN"), have raised concerns about the tracking of consumer products, from which tracking of purchasers' behavior results without their knowledge.[107] Albrecht advocates the use of RFID tags to track the transportation of merchandise, but only if the tags are destroyed once the products reach the ultimate consumers.[108]

C. FUNCTION CREEP

Clandestine tracking could lead to "function creep," in which the use of obtained information is expanded to include purposes beyond

---

[102] *Id.*

[103] *Id.*

[104] Press Release, GOLIATH Solutions, GOLIATH Solutions to Install Display Tracking System at Walgreens Stores Chainwide (Dec. 5, 2005), *available at* http://www.forbes.com/prnewswire/feeds/prnewswire/2005/12/05/prnewswire200512050901PR_NEWS_B_MWT_CG_CGM022.html.

[105] CASPIAN Anti-RFID Protest: Dallas, Texas, http://www.spychips.com/protest/walmart/protest-slideshow/index.html (last visited Aug. 6, 2006).

[106] Laurie Sullivan, *Consumer Group Calls for RFID Protest at Dallas Wal-Mart*, INFORMATIONWEEK Oct. 14, 2005, *available at* http://www.informationweek.com/showArticle.jhtml;jsessionid=0CHHDQNIXBLSWQSNDBECKHSCJUMEKJVN?articleID=172301047.

[107] *See id.*

[108] Todd R. Weiss, *Privacy Groups Question RFID Use in Medicine Tracking*, COMPUTERWORLD Oct. 14, 2005, *available at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,105432,00.html.

those initially stated.[109] Privacy concerns are raised when such "function creep" occurs without the knowledge or consent of the individual providing the information.[110] The classic example is the expanded use of Social Security numbers, which are now incorporated as a form of identification in secondary, non-governmental uses.[111] Of primary concern is how the personal and biometric information contained in the e-passports will be shared among other agencies and databases.[112]

A "function creep" of clandestine tracking could include "hotlisting" or "profiling," which refers to the assembly of a database matching unique identifiers to specific individuals.[113] Such a database containing personal information could affect individuals' anonymity, as use of standard biometrics could allow tracked information such as business transactions, habits, or ethnicity to be linked together.[114] The risk of abuse regarding such a database is high, as assemblers of such a database could compile a profile of an individual's actions and private life.[115] The risk of such abuse is compounded by the inclusion of biometric information in contactless integrated circuits, as biometric identification technology could lead to surveillance and acquisition of

---

[109] Paul Rosenzweig, Alane Kochems & Ari Schwartz, *Biometric Technologies: Security, Legal, and Policy Implications*, THE HERITAGE FOUND., June 21, 2004, http://www.heritage.org/Research/HomelandDefense/lm12.cfm.

[110] *Id.*

[111] Malcolm Crompton, Fed. Privacy Comm'r, *Biometrics and Privacy: The End of the World as We Know It or The White Knight of Privacy?* (Mar. 20, 2002), *available at* http://www.privacy.gov.au/news/speeches/sp80notes.htm.

[112] Jane Wakefield, *Doubts Over Biometric Passports*, BBC NEWS, Oct. 27, 2005, http://news.bbc.co.uk/1/hi/technology/4381160.stm.

[113] American Civil Liberties Union of Northern California, *RFID: Government Identification Documents and "Tracking" Issues* 6, 8 (Dec. 2, 2005), *available at* http://www.aclunc.org/privacy/technology/yes768/050808-rfid-packet.pdf.

[114] GOVERNMENT ACCOUNTABILITY OFFICE, RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT, REPORT 05-551 25-26 (May 27, 2005), *available at* http://www.gao.gov/new.items/d05551.pdf#search=%22Government%20Accountability%20Office%2C%20Radio%20Frequency%20Identification%20Technology%20in%20the%20Federal%20Government%22.

[115] *Id.*

personal data without the individual's awareness or consent.[116] Biometric information can act as a unique identifier to bring together unrelated pieces of information about an individual, thus eliminating that individual's control over the use of his or her information.[117]

In comments to the Department of Homeland Security, the Electronic Privacy Information Center expressed concern about biometric data collected for the US-VISIT program, citing the Computer Assisted Passenger Prescreening System ("CAPPS II") as an instance where "mission creep," (also known as "function creep") became problematic.[118] Intended originally as an aviation security tool, the use of CAPPS II has expanded into the law enforcement realm, particularly in analysis of those with outstanding arrest warrants.[119]

D. THE DANGERS OF INFORMATION CONCENTRATION

The decision to include a digitalized photograph on the e-passport's chip may lead to the incorporation of those photographs into a database. This could allow facial recognition systems to survey and compile a list of individuals' actions and travels. Moreover, this "function creep" may consequently lead to the integration and inter-agency sharing of such personal information. Barry Kefauver, who heads the ICAO's biometric working group in the creation of global standards, noted that although linkage of data between e-passports and law enforcement databases is controversial and would require safeguards, it is essential for realizing the e-passport's enhanced security.[120] Kefauver claims that preventing the proliferation of false passports by comparing passports to a list of lost or stolen documents

---

[116] *Id.*

[117] Crompton, *supra* note 111.

[118] Electronic Privacy Information Center (EPIC), Comments in Response to Department of Homeland Security Border and Transportation Security Doctorate, Docket No. BTS 03-01: Interim Final Rule and Notice, 5-6, http://www.epic.org/privacy/us-visit/us-visit_comments.pdf.

[119] *Id.* at 6.

[120] Wakefield, *supra* note 112.

is crucial because a "fake passport in the hands of a terrorist is as important a tool as a bomb."[121]

Frank E. Moss, Deputy Assistant Secretary for Passport Services of the Department of State, also recognizes the importance of ensuring that only entitled American citizens receive U.S. passports and therefore finds international data exchange essential.[122] The Department of State has worked on establishing data-sharing programs with other federal agencies such as the Social Security Administration ("SSA") (to verify identities by correlating applicant data with the information in the SSA systems) and the U.S. Marshals Service (to accumulate names of fugitives or other individuals of concern to law enforcement in a passport "lookout system").[123] The Department of State has also worked to implement international programs, such as INTERPOL, with which the Department shares its lost and stolen passport database.[124] The Department of Homeland Security is currently working with the Federal Bureau of Investigation ("FBI") to make the FBI's Integrated Automated Fingerprint Identification System ("IAFIS")[125] more interoperable with the Department of Homeland Security's Automated Biometric Identification System ("IDENT") in an effort to identify those with outstanding criminal warrants.[126] The linkage of multiple databases containing personal information or its concentration in a central database increases the potential for tracking individuals and their activities for secondary uses of the information without consent.[127]

---

[121] *Id.*

[122] *Improvements Needed to Strengthen U.S. Passport Fraud Detention Efforts: Hearing on GAO Report 05-477 Before the S. Comm. On Homeland Sec. & Gov't Affairs*, 109th Cong. (June 29, 2005) (statement of Frank E. Moss, Deputy Assistant Sec'y for Passport Services, U.S. Dep't of State), *available at* http://travel.state.gov/law/legal/testimony/testimony_2552.html.

[123] *Id.*

[124] *Id.*

[125] Federal Bureau of Investigation, Criminal Justice Information Services Division, *Integrated Automated Fingerprint Identification System or IAFIS*, http://www.fbi.gov/hq/cjisd/iafis.htm (last visited Sept. 9, 2006).

[126] Interview with Williams & Hyatt, *supra* note 15.

[127] Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J.L. & TECH. 319, 328 (2002).

E. ASSOCIATION OF BIOMETRICS WITH CRIMINALITY

Privacy advocates are also concerned about the association of biometric identification information with criminality,[128] particularly, the inclusion of fingerprint information in e-passport contactless integrated circuits.[129] The ICAO has made optional the inclusion of digitized fingerprint information as an encoded identification feature,[130] though the European Union ("EU") has mandated that both facial and fingerprint information be included in the e-passports for the fifteen member states which have adopted the Schengen Treaty (which removed EU internal border controls).[131] Germany has mandated incorporation of fingerprints be incorporated into its e-passports by March 2007.[132] Fingerprints have been traditionally used to identify criminals, using a one-to-many search in which an individual's fingerprint is compared to all those listed in a database; such an association with the criminal justice system is thought to render people reluctant to get fingerprinted.[133]

F. THE DANGERS OF AUTOMATION

Automation of e-passport deployment and authentication could lead to less human oversight, thereby increasing the risk of biometric authentication system deception.[134] Radio frequency machine readers

---

[128] *Id.* at 364-65.

[129] *Id.* at 364.

[130] LDS TECHNICAL REPORT, *supra* note 32, at 22.

[131] Mark Oliver & Agencies, *Cost of Standard UK Passport to Rise*, GUARDIAN UNLIMITED, Nov. 17, 2005, http://www.guardian.co.uk/uk_news/story/0,,1644867,00.html.

[132] Victor Homola, *World Briefing Europe: Germany: Debut for Electronic Passports*, N.Y. TIMES, Nov. 2, 2005, at A8, *available at* http://query.nytimes.com/gst/fullpage.html?res=9E0CE5DA163EF931A35752C1A9639C8B63&fta=y.

[133] Rich Lowry, *The Power of the Fingerprint*, JEWISH WORLD REV., June 27, 2005, http://www.jewishworldreview.com/0605/lowry062405.php3; *see also* findBiometrics.com, *Privacy – Friend or Foe?*, http://www.findbiometrics.com/Pages/privacy.html.

[134] *EFF Comment*, *supra* note 82, at 13.

can read multiple e-passport contactless integrated circuits at a time because of their anti-collision technology, and therefore prevent potential interference from two different e-passports in the same range.[135]

Tsutomu Matsumoto, a cryptographer, has demonstrated that plastic mold made out of gelatin can be used to imitate a fingerprint; the fake finger fooled fingerprint detectors eighty percent of the time.[136] Matsumoto enhanced fingerprints taken from a glass with super-glue fumes, photographed them with a digital camera, and after some work with PhotoShop, he printed the fingerprint onto a transparency sheet.[137] Then, he etched the fingerprint onto a copper printed-circuit board using the transparency and made a gelatinous finger from the etchings.[138] Thus, the risk of deceiving the system appears real in light of the relative technical ease involved in the process. Increased automation of e-passport authentication and inspection could also increase the risk of such biometric imitations to bypass biometric authentication systems.

V. THE DEPARTMENT OF STATE'S REVISED APPROACH

On October 25, 2005, the Department of State released its final rule regarding the design and implementation of U.S. e-passports. In response to the many negative comments received during the rulemaking process regarding security and privacy issues, the Department of State has worked with the Government Printing Office and National Institute of Standards and Technology to add security enhancements designed to address the major privacy concerns regarding its previous proposal, in accordance with ICAO recommendations.[139]

---

[135] USE OF CONTACTLESS ICS, *supra* note 51, at 10.

[136] John Leyden, *Gummi Bears Defeat Fingerprint Sensors*, THE REGISTER, May 16, 2002, http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/.

[137] *Id.*

[138] *Id.*

[139] Final Rule, *supra* note 79, at 61,553-61,554; *see supra* Part III (A)-(D) of this article.

A. RETAINING RADIO FREQUENCY IDENTIFICATION

Despite the numerous privacy concerns with Radio Frequency Identification ("RFID)" the Department of State has elected to preserve its use of contactless integrated circuits embedded in the cover of the e-passport.[140] In order to protect against hacking and counterfeiting of the RFID signal, the Department of State is utilizing third party certification, and conducting regular audits of chip manufacturers and processes to ensure security.[141] In addition, the contactless chip will be placed in a newly designed, tamper-proof document in the e-passport.[142] The Department of State rejected the concept of replacing the contactless chip with a contact chip because contact chip technology does not transfer well from card formats to book-type formats.[143] Because contact chips require physical contact with the reader, instituting contact chips in a book-format passport would lead to unreliable readings; this unreliability is expanded by the increased wear from repeated insertion of the e-passport into machine readers.[144]

B. ANTI-SKIMMING COVER

Working in combination with the Government Printing Office to test devices that reduce the passport's vulnerability to "skimming," the Department of State has revised the U.S. e-passport cover and spine to include anti-skimming materials preventing RFID signals from escaping.[145] Although this cover will not prevent "eavesdropping" on authorized readings, it is an effective way to prevent unauthorized readings when the e-passport holder does not expect it.[146] The results

---

[140] *Id.* at 61,553.

[141] *Id.* at 61,554.

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] Jules, Molnar & Wagner, *supra* note 71, at 11.

of tests conducted by the Department of State, in conjunction with the Government Printing Office and National Institute of Standards and Technology, indicate that the addition of the anti-skimming material will alleviate the threat of "skimming" beyond the ICAO standard of ten centimeters while the e-passport is closed or partially closed.[147]

C. BASIC ACCESS CONTROL

In response to calls for the encryption of e-passport data, the Department of State will also incorporate Basic Access Control ("BAC"), which requires authentication of radio frequency readers before data transmission, and the encryption of the data transfer between the contactless integrated circuit and the machine reader.[148] BAC requires a machine reader to physically identify the Personal Identification Number ("PIN") in order to unlock the data on the contactless integrated circuit.[149] Without accessing a PIN, no reader could retrieve the e-passport data via RFID signal access. The PIN for U.S. e-passports is accessible by physically scanning the second line of printed characters on the Machine-Readable Zone on the e-passport data page.[150] The data page is the page of the passport with a facial portrait and personal information, and two printed lines at the bottom representing the Machine-Readable Zone.[151] The passport officer would optically scan the readable portion using the reader, which would generate the PIN from the scanned data, thus allowing the reader to capture the RFID signal.[152] Officials from the Department of State admitted that it previously underestimated the potential range of RFID signal transmissions.[153]

---

[147] Final Rule, *supra* note 79, at 61,554.

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] LDS TECHNICAL REPORT, *supra* note 32, at 10-11.

[152] Kim Zetter, *Feds Rethinking RFID Passport*, WIRED NEWS, April 26, 2005, http://www.wired.com/news/privacy/0,1848,67333,00.html.

[153] *Id.*

The incorporation of the BAC process complies with ICAO Document 9303 security recommendations,[154] and will prevent "skimming" and "eavesdropping" even if the e-passport is open. One cannot "skim" because BAC requires physically opening and scanning the e-passport through the reader before accessing the contactless chip data; one cannot eavesdrop because the communication channel between the integrated circuit and the machine reader remains encrypted, as BAC requires the correct PIN number.[155] Some vendors testing e-passports that incorporate BAC have found that read times are twice as slow as those without it; however, these differences in read times represented a matter of seconds.[156]

In addition, the Department of State believes that physically shielding the radio frequency machine readers will also minimize the possibility of "eavesdropping" while the e-passport is open at the inspection site.[157]

VI. CONCLUSION

Since the September 11, 2001, tragedy, the United States government has focused on increasing the nation's border security, particularly through the incorporation of biometric technology into security procedures. In addition to its use in the US-VISIT program, the use of biometric information has garnered much international attention due to the U.S. Visa Waiver requirements calling for biometric information in e-passports. These requirements, based on ICAO standards, have sent other nations scrambling to manufacture and implement acceptable electronic passports that store biometric information such as digital photographs in electronic chips within the passports.

---

[154] PKI TECHNICAL REPORT, *supra* note 69, at 15-17 (recommending the inclusion of optional security features such as active authentication, basic access control, extended access control, and encryption).

[155] Zetter, *supra* note 152.

[156] LIN YIH & SUNNY HO, SUMMARY REPORT OF E-MRTD INTERFEST TESTING SESSION 4 3 (2005), *available at* http://www.itsc.org.sg/tc/6th_term_compo/SummaryofInterFest3Feb05_Final.pdf.

[157] Final Rule, *supra* note 79, at 61,554.

Contactless reading of such biometric information using a RFID signal capture process has raised a significant number of privacy concerns, most notably regarding the unauthorized capture of personal information, the potential for clandestine tracking, hotlisting, and function creep, and to a lesser extent, the association of such information with criminality and the danger of automation.

Taking these concerns into account, the Department of State has revised its e-passport approach to provide additional protection for personal information. Although the use of RFID to transfer the information has been retained and concerns regarding clandestine tracking and information concentration remain unanswered, the introduction of an anti-skimming front-cover and BAC will serve to prevent the unauthorized capture and use of biometric information.

The Department of Homeland Security successfully completed its testing of e-passports and readers that apply BAC at the San Francisco International Airport in April 2006.[158] The Department of Homeland Security had been testing e-passport machine readers, in conjunction with the nations of Australia, New Zealand, and Singapore to ensure global interoperability and international implementation of ICAO standards.[159] A spokesman for the Department of State has announced that it will begin issuing electronic passports on August 14, 2006, at the Denver Passport Agency, followed by the Special Issuance Agency in Washington D.C.[160]

---

[158] Roy Mark, *U.S. Completes E-Passport Testing*, INTERNETNEWS.COM, Apr. 20, 2006, http://www.internetnews.com/infra/article.php/3600526.

[159] Press Release, Dep't of Homeland Security, *E-Passport Testing to Begin at San Francisco International Airport* (Jan. 13, 2006), http://www.dhs.gov/dhspublic/display?content=5342.

[160] Security Document World, *U.S. Epassport Ready to Roll*, Aug. 4, 2006, http://www.securitydocumentworld.com/public/index.cfm?&m1=c_10&m2=c_4&m3=e_0&m4=e_0&subItemID=682.