The James A. Baker III Institute for Public Policy
Rice University

# Innovation by Policy: A Study of the Electronic Passport

By

R. Christopher Bronk, Ph.D.

Fellow in Technology, Society and Public policy
James A. Baker III Institute for Public Policy
Computer and Information Technology Institute
Rice University

May 2007

This paper was written by a researcher (or researchers) who participated in a Baker Institute research project. Wherever feasible, these papers are reviewed by outside experts before they are released. However, the research and views expressed in these papers are those of the individual researcher(s), and do not necessarily represent the views of the James A. Baker III Institute for Public Policy.

## *Note from the Author*

Representing the Baker Institute’s Technology, Society and Public Policy (TSPP) program, the author views this issue through the cognitive lenses of a software developer, political scientist and, perhaps most importantly, a former consular officer with experience in applying the law to determine citizenship and issue passports to his fellow citizens. This experience was prior to the current position of the author at Rice University, an institution with tremendous intellectual holdings in faculty and students within the areas of computer science, electrical engineering, and applied mathematics. Building interdisciplinary bridges to better understand the space where technology and policy intersect requires an atmosphere in which novices may be suffered gladly so as to improve understanding of topics of nuance and complexity, from federal budgeting to digital file compression algorithms. The ability to ask the experts, “Does this really work this way?” or “How does it work?” in the most blunt language was of huge value to this research. Without this honest exchange, any understanding of how the computerized passport—a product of technology created through public policy—will impact society would be fundamentally unsound.

The author wishes to acknowledge the many individuals who have helped in preparing this paper. Special thanks go to the TSPP Rice University interdisciplinary support network: Moshe Vardi, Jan Odegard and Amy Kavalewitz at the Rice Computer and Information Technology Institute; Allen Matusow and Mark Scheid at the Baker Institute; and Charles Henry and Karen Hyde at the Fondren Library. Collaborators at Rice and beyond informed the author considerably of computing and imaging technology, immigration policy and methods of study including Jeffrey Seifert, Derek Ruths, Nick DeBaggis, Rey Koslowski, Mili Shah and Briann Vollmer. Finally, the author owes a great debt to the officers of the Foreign Service and Department of Homeland Security with whom he served on both sides of the U.S.–Mexico border.

## *Executive Summary*

In responding to public demand for remedy of policy problems of the national interest, there exists within the history of the United States a strong tendency to apply new technology. It should be unsurprising then that the national leadership chose to seek technological solutions involving computing and information technologies to mitigate the terrorist threat following the September 11, 2001, attacks upon the United States. This paper investigates one small piece of this mammoth effort—the process, from problem identification to technology implementation, of a new, computerized, electronic passport currently issued by the U.S. Department of State. It examines how a failed terrorist attack by a British national placed into doubt a convenience-oriented international regime in which the citizens of the world's most developed countries travel between one another without the hassle and cost of obtaining specific permission in the form of a non-immigrant visa.

Jeopardized by the bungling "shoe bomber," the international Visa Waiver Program remains in place largely due to U.S. legislation and international agreements, which promulgated the adoption of a computerized passport. Beliefs that this new technology renders the program less risky and elevates the level of security for U.S. travelers overseas are rendered baseless, as analysis of the passport technology reveals considerable flaws on two fronts. First, the passport was intended to serve as a biometric device, one in which the physical attributes of its bearer would be automatically matched to data on the document's microchip by computer. Second, it was intended to be more resistant to tampering and forgery by malicious parties. On both counts, according to information in the public domain, the electronic passport, or e-passport, has failed and, at worst, may jeopardize the safety of those to whom it is issued.

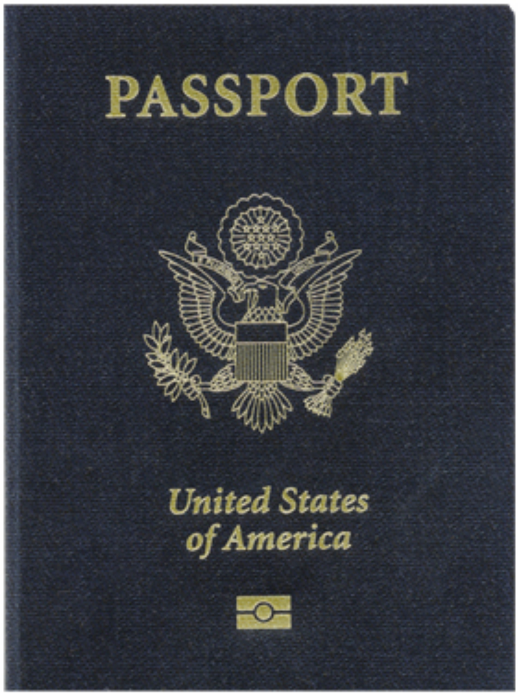
The author argues that the congressional mandate to create a biometrically enabled, electronic passport put political goals ahead of the technically feasible. Congress wrote into law a directive to create an advanced computer imaging technology—that did not,

and likely still does not, exist—by producing legislation demanding an electronic passport as the "silver bullet" rhetorical solution to an immensely complex problem.

In addition, the technology's specifications and functionality were created by an international body in an opaque manner without a monopoly of expertise regarding the creation of such a device under the stewardship of a former U.S. government official. This only served to fuel those fearing government infringement of personal liberties or equating the lack of transparency to purposefully engineered acts of conspiracy.

Labeled a "loser system"[1] by the journal of the largest professional organization of electrical engineering professionals and academics, the electronic passport should be viewed as an exemplar of failure to grasp both technical complexity and open governance in the creation of an electronic device and document that will be required for re-entry of all U.S. citizens, including crossings of the land borders with Mexico and Canada beginning January 1, 2008.

FIGURE 1: THE ELECTRONIC PASSPORT



*Source: U.S. Dept. of State*

[1] "Passport to Nowhere: the Radio-Tagged Biometric Passport Won't Faze Industrious Terrorists," *IEEE Spectrum*, January 2005, 55.

## *The Problem*

Several hours into a transatlantic flight on December 22, 2001, a conspicuously disheveled young man with a window seat in the 29th row of an American Airlines Boeing 767 waited for the woman seated beside him to visit the restroom and then ignited a series of matches. Smelling the sulfur-smoke, a flight attendant confronted the six-foot-four individual. Watching him ignite another match, she attempted to wrestle an athletic shoe with a protruding wire from his hands. Overpowered and thrown to the floor by the occupant of seat 29A, the attendant was joined in the altercation by a second crewmember, who noisily recoiled after being bitten on the hand. Spurred into action, passengers of Flight 63 subdued the man fanatically intent on igniting the shoes he'd worn onboard. In the days following the incident, news media speculated on the identity of this "shoe bomber." French authorities believed him to be identified as Tariq Raja, a Sri Lankan, or perhaps as Abdel Raheem. But as events unfolded in the investigation, it was discovered that Mr. Raja/Raheem had boarded the aircraft with a British passport, which one Reuters journalist speculated had been acquired through use of fraudulent documents. Eventually under the scrutiny of criminal investigation, the man who attempted to take 196 lives over the North Atlantic was identified as Richard Colvin Reid of Bromley, South London, and he had received his "freshly minted British passport" from his country's embassy in Brussels a fortnight before on December 7.[2]

Only weeks after the September 11 attacks, Reid's act was yet another swipe at the American psyche.[3] By December, the world knew that the perpetrators of the attacks on New York and Washington were Arab Muslims, citizens of Middle Eastern countries and

[2] This account draws from multiple sources: Leslie Gervitz, "U.K., France Investigate Security Lapse: Police Trying to Determine if Failed Bomber Acted Alone," *Ottawa Citizen*, December 24, 2001; Philip Shennon, and Pam Belluck, "A Nation Challenged: The Suspect; F.B.I. Tests Find Explosives in Shoes of Jet Passenger," *New York Times*, December 24, 2001; "Securing the Skies," *New York Times*, December 25, 2001; Daniel Jeffreys, "War on Terror Flight 63," *The Advertiser* (London), December 25, 2001; Paul Harris, Nick Paton Walsh, and Burhan Wazir, "The Making of a Terrorist," *The Observer*, December 30, 2001; Allen Pusey and Jim Morris, "Little Help Given to Crew in Shoe-Bomb Plane," *Dallas Morning News*, June 9, 2002; Brad Smith, "Air of Terror," *Tampa Tribune*, October 27, 2002; Pam Belluck, "Man Accused of Shoe-Bomb Plot Says He Intends to Plead Guilty," *New York Times*, October 3, 2002.

[3] Donald F., Kettl, *System under Stress: Homeland Security and American Politics* (CQ Press: Washington, DC, 2004).

members of the notorious Al Qaeda terrorist network. The United States and its NATO allies had dispatched military force to Afghanistan, which was aimed at shattering the forces of the U.S. nemesis Osama Bin Laden. Weeks after the September attacks Reid turned the profile of the fanatical Islamic terrorist on its ear. A British man with English and Jamaican parents, he was radicalized as a disaffected youth in a Brixton mosque, used his citizenship to board an aircraft and came incredibly close to detonating a device capable of crippling or destroying the plane. Before Reid, the U.S. leadership knew a comprehensive overhaul of immigration policy would be needed, especially with regard to Saudi Arabia.[4] After Reid, a realization set in that if future attacks were to be thwarted, international movement of all travelers might have to be monitored very closely.[5]

By failing to ignite his shoes, Reid laid bare an immense issue for public policy by falsifying the perception that terrorist bombers only come from Gaza or Beirut. In so doing, this raised the question, in the minds of the Western world's leadership, whether the system of international travel—which still more than five years later permits significant mobility between the world's most wealthy nations with a minimum of effort—might need dramatic restructuring, unless technologies and processes could be crafted to mitigate the risk of a citizen of one of the world's wealthiest countries to utilize his or her citizenship as a shield from scrutiny in the conduct of a terrorist attack.

### *Policy and Technology in an Age of Information*

In answering demands for innovation and remedying the problems of public policy—in this case the problems of effective immigration management and counter-terror risk mitigation—the United States government, usually in concert with industry, has increasingly pursued strategies utilizing information and computing technology. A primary developer of the contemporary, near-ubiquitous computing environment, the United States has a long history of drawing upon technical expertise in international economic and military battlefields as well as in its domestic concerns. On U.S. soil the

[4] Joel Mowbray, "Catching the Visa Express," *National Review*, July 1, 2002.

[5] Rey Koslowski, "International Cooperation on Electronic Advanced Passenger Information Transfer and Passport Biometrics" (meeting of the International Studies Association, March 17-20, 2004).

greatest battle between an agrarian and industrial power was ultimately fought and won by the player holding vast material superiority begotten by industrial innovation, the product of a military-technical revolution.[6] Even before Gettysburg, the United States demonstrated a strong propensity toward developing new technologies to alter the calculus of its national problems so as to rebalance them and permit resolution and progress. It should be no surprise then that the problems of the third American century, characterized by complexity and fluidity, will be met with solutions enabled by the country's most recent pair of world-changing technologies: the microchip and the Internet.

This paper grapples with the process of how scientists and engineers collaborate with politicians and bureaucrats to mitigate a policy problem in large part with the application of information and computing technology (ICT). The political issues of interest to this paper are currently of great importance on the national agenda: national security and international immigration. In addition, the latter item is highly divisive and prone to inflammatory and often irrational debate. Seeking to meet a mandate for "secure borders and open doors,"[7] the United States' newest cabinet-level department, the Department of Homeland Security, has partnered with its oldest, the Department of State, to create new mechanisms for managing the flow of migrants, isolating and intercepting criminally- and politically-motivated malicious actors, while continuing to attract the world's greatest minds to academic, cultural and commercial activity so as to maintain a vibrant and competitive society. Crafting security policy, which harnesses technology to promote both security and openness, is intensely complicated[8] and also a necessity if the United States is to maintain or enhance its international influence and economic strength. Engaging in scholarship to study such policy is equally complicated and could easily be swamped by the enormity of the issues, both technical and political.[9]

[6] Andrew Krepinevich, "The Military-Technical Revolution: A Preliminary Assessment," (Washington, DC: Office of Net Assessment - Department of Defense, July 1992).

[7] Maura Harty, "U.S. Visa Policy: Securing Borders and Opening Doors," *The Washington Quarterly*, Spring 2005.

[8] Charles R. Wise and Rania Nader, "Organizing the Federal System for Homeland Security: Problems, Issues, and Dilemmas," *Public Administration Review*, September 2002.

[9] Deborah Stone, *Policy Paradox: The Art of Political Decision Making* (New York: W. W. Norton & Co., 1997).

Breaking such a big problem into component parts is thus requisite. Furthermore, exploring known terrain, the previously accepted fundamentals and conceptually identifiable constructs of the issue, would seem of benefit as well. Desired is an answer to the question: How has the need to mitigate terror threats, manage illegal entry and attract visitors affected the technological infrastructure of international travel? That is likely a question of book-length scale or more deserving of the attention of blue ribbon expert panels. Shrinking the issue set to an even smaller space is required, by further specifying the question posed above and asking: How has the need to mitigate terror threats, manage illegal entry and attract visitors affected the technological infrastructure of the government-issued passport? Temporally, it may be a good time to seek answers because, as of December 1, 2006, every passport issued by the United States as well as those issued by more than two dozen other countries will be not only an internationally recognized identification document but a computerized data transmission device as well. This event marks an opportunity for evaluation and stocktaking. What has the citizenry of the United States gotten with its computerized international travel document?

Explaining how this issue arose and ultimately how a technology was produced through policy, rather than falling into the already bulging file of failed government information technology (IT) projects from local to global scale, is necessary so that we may better understand how emerging policies and technologies are combined to achieve results, whether they be desirable, unanticipated or other. Over the past five years, computerizing the passport—the fundamental international citizenship and travel document for more than a century—has drawn the opinions, resources, expertise, and attention of foreign ministries, news outlets, border police, international organizations, academic institutions, global multinational corporations, computer hackers and civil libertarians, among others. Each constituency has produced research and analysis, serving to inform the greater discourse on the issue while also standing as official representation of desired capabilities and possible concerns, along with declaring the unacceptable or infeasible. Barring limited publicly available research from the largest of think tanks[10] and the products of

[10] John D. Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas, "Biometrics: A Look at Facial Recognition," RAND: Santa Monica, CA, 2003.

uniquely trained and singularly interested cross-disciplinary academics,[11] the quantity of scholarship relevant to the new e-passport is incredibly limited. This paper shows that adopting empiricist precepts regarding falsifiability[12] necessitates rigorous and diverse effort designed to probe accepted convention and theory regarding the performance of one particular technology. This paper also adopts constructivist theory to a contextually rich and complex subject involving a systemic and technical problem-solving approach involving political debate designed to achieve a policy goal.[13]

As the prior questions regarding the capacity to function connote, study of this technology, the e-passport, although multifaceted, attempts to address whether it will perform in actual use as envisioned by policymakers and engineers as specified in law and technical standards, respectively. Embedding a computing device within the passport did not emerge from a vacuum in the public policy arena. The most profound shock to the United States since Pearl Harbor led it to stimulate the deployment of this technology, so it is necessary to first revisit the turbulent environment immediately following the September 11, 2001, attacks to understand the initial political moves that initiate this narrative.

### *On Borders – Controlled Immigration and the Developed World*

For the nation state, perhaps no component of asserting sovereignty holds greater importance than the capacity to maintain its territorial integrity. Protecting the state from invasion by outside forces has represented a core role for government since Thucydides wrote on the subject. In the past century's Cold War, boundaries between rival blocs assumed a prominent position in international affairs. Defenses were probed and transgressors intercepted, while individuals, often at great peril, defected from one side to another. Countries on the frontier between East and West exerted their sovereign territorial rights to the extreme with barbed wire, landmines and massive standing armies.

[11] Rey Koslowski, "Information Technology and Integrated Border Management," *Managing International and Inter-Agency Cooperation at the Border*, Geneva Centre for the Democratic Control of the Armed Forces, March 13-15, 2003.
[12] Karl Popper, *The Logic of Scientific Discovery* (Basic Books, New York, 1959).
[13] Herbert C. Simon, *The Sciences of the Artificial* (MIT Press, Cambridge, MA, 1999).

Other than the 38th Parallel and a few other locales, borders have generally grown more open following the fall of the Iron Curtain.[14]

Readers in the world's most developed countries may largely take for granted the simplicity of international travel. From New York's John F. Kennedy Airport, U.S. citizen travelers may catch flights to Seoul, Santo Domingo or Stockholm (but not Pyongyang) with only a passport and plane ticket. No visa is required for an American to cross from El Paso to Ciudad Juarez, nor Detroit to Windsor. Because U.S. citizens are generally assumed to hold the intent to return home, barriers to international travel are few. Indeed, for citizens of the world's wealthier countries, crossing borders has largely become an exercise in formalities, with an entire block of countries, those of the Western European Schengen Zone,[15] abandoning border control altogether. Clearing immigration in one Schengen port of entry permits travel between Schengen Convention countries as free from restriction as movement from Illinois to Colorado. Predating implementation of Schengen by nearly a decade, the 1986 implementation of the United States Visa Waiver Program (VWP) terminated visa requirements for short-term tourist and business travel with a group currently numbering 27 countries, including all of the current full Schengen members with the exception of Greece. After more than a decade in pilot status, President Bill Clinton signed into law House Resolution 3767, the Visa Waiver Permanent Program Act, on October 30, 2000.[16] That year, "17 million individuals entered the United States" under the program.[17] As one immigration critic would state in hearings for the National Commission on Terrorist Attacks upon the United States three years later, it permitted citizens of the VWP countries to "board airplanes bound for the United States merely by

[14] Considerable ink has been dedicated to post-Cold War sovereignty issues by political science, economics and geography, with particular emphasis placed on globalization. New directions in border studies are perhaps best summarized in Vladimir Kosssolov, "Border Studies: Changing Perspectives and Theoretical Approaches," *Geopolitics*, Winter 2005.

[15] Austria, Belgium, Denmark, Finland, France, Germany, Greece, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain and Sweden with some territorial exceptions.

[16] *Visa Waiver Permanent Program Act*, H.R.3767, 106th Cong., 2nd Sess. (March 1, 2000), http://thomas.loc.gov/cgi-bin/bdquery/z?d106:HR03767:@@@L&summ2=m&.

[17] Thomas R. Eldridge, et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: National Commission on Terrorist Attacks Upon the United States, August 21, 2004) 77.

purchasing tickets and showing their passports."[18] The law cemented a policy, which made enormous sense on cost grounds. The U.S. State Department would see reductions "of up to 80 percent" in this non-immigrant visa caseload at its embassies and consulates in VWP countries.[19]

**Table – Number of Admissions to U.S. (Form I-94), Visa Waiver Program FY 1996-2004[20]**

| Year | Travelers for Business (in millions) | Pct. of Total | Travelers for Pleasure (in millions) | Pct. of Total |
|---|---|---|---|---|
| 1996 | 1.369 | 36.3 | 11.033 | 57.8 |
| 1998 | 2.142 | 46.7 | 9.732 | 40.4 |
| 2000 | N/A | | N/A | |
| 2002 | 2.330 | 53.2 | 8.773 | 44.0 |
| 2004 | 2.240 | 48.7 | 9.185 | 40.3 |

While September 11 exposed the need to implement effective immigration controls designed to deter and interdict international terrorists,[21] the arrest of "shoe bomber" and British citizen Richard Colvin Reed, aka Tariq Raja and Abdel Rahim, for his attempt to destroy American Airlines Flight 63 bound for Miami from Paris' Charles De Gaulle International Airport hit the VWP countries' weaknesses squarely. Committed to the destruction of the aircraft, Reed presented a disturbing new wrinkle for U.S. counter-terrorism policy. Traveling with a British passport, Reid's first encounter with a U.S. official would occur at the U.S. port of entry, as was also the case of French citizen Zacarias Moussaoui.[22] Policymakers in the United States recognized that additional

[18] Jan Ting, statement to the National Commission on Terrorist Attacks Upon the United States, sixth public hearing of the National Commission on Terrorist Attacks Upon the United States, December 8, 2003, http://www.9-11commission.gov/hearings/hearing6/witness_ting.htm

[19] Department of State Memo, "Continuation of a Nonimmigrant Visa Waiver Program," January 11, 1990, quoted in Eldridge, et al., *9/11 and Terrorist Travel*, 77.

[20] Figures do not include visa waiver travel to the U.S. Territory of Guam nor visa travel in all other classes beyond the B1/B2 non-immigrant travel visa category. Fiscal Year 2000 data were incomplete due to lapse in the Visa Waiver Pilot Program and transition to permanent status. Office of Immigration Statistics, *2005 Yearbook of Immigration Statistics*, (Department of Homeland Security: Washington, D.C., November 2006).

[21] Rey Koslowski, "Towards an International Regime for Mobility and Security?" in *Globalizing Migration Regimes*, ed. Kristof Tamas and Joakim Palme (Ashgate Publishing: Burlington, VT, 2006).

[22] Jan Ting, *The Open Door How Militant Islamic Terrorists Entered and Remained in the United States, 1993-2001* (Washington, D.C.: Center for Immigration Studies, National Press Club, May 22, 2002), http://www.cis.org/articles/2002/terrorpanel.html#ting.

safeguards would be required, crafted and implemented by governments of VWP countries, the airlines, U.S. agencies and others, contingent upon the program's survival.

Through late 2001 and early 2002, members of the United States Congress proposed sweeping new legislation with regard to immigration policy. In late October Florida Congressman Michael Bilirakis submitted House Resolution 3181, requesting a nine-month moratorium on the issuance of student visas.[23] Another Floridian, Representative Dave Weldon, proposed a moratorium on the issuance of visas to citizens of "(1) Afghanistan; (2) Algeria; (3) Egypt; (4) Lebanon; (5) Saudi Arabia; (6) Somalia; (7) United Arab Emirates; (8) Yemen; or (9) any country designated as a state sponsor of terrorism," with the exception of diplomats.[24] Republicans Bilirakis and Weldon did not represent a partisan anti-immigration block, with Senator Diane Feinstein, a Democrat, considering a student visa moratorium[25] and eventually proposing legislation to overhaul the visa adjudication process.[26] For U.S. college administrators and Middle Eastern businessmen alike, these were alarming proposals, however, what is of importance to this paper is the suggested remedy contained within these resolutions as well as several others.

While the legislation proposed by all three legislators ultimately stalled in committee, a new policy designed to reduce or eliminate vulnerabilities exploited by foreign terrorist networks would ultimately be enacted into law. Perhaps the most controversial and rhetorically charged piece of legislation written by the Congress in recent memory, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 cleared the House with a 357-66 vote and passed the Senate without amendment, 98-1. Debate over the USA PATRIOT Act's new investigative and surveillance powers has been considerable but is not the focus of this paper. A single reference is of importance, however. Under Section

[23] H.R. 3181, 107th Cong., 1st Sess., *Cong. Rec.*, October 30, 2001, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3181:.

[24] *Terrorist Admission Prevention Act of 2002*, H.R. 4010, 107th Cong., 2nd Sess., *Cong. Rec.*, March 20, 2002, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.4010:.

[25] "Chiller on Campus," *The Economist*, November 22, 2001.

[26] *Visa Entry Reform Act of 2001*, S.1627, 107th Cong. 1st Sess., *Cong. Rec.*, November 1, 2001, http://thomas.loc.gov/cgi-bin/bdquery/z?d107:SN01627:.

417, the resolution placed emphasis on auditing the implementation of machine readability features for the passports issued by VWP countries. The law stipulates, "[T]he government of the [visa waiver] country certifies that it issues to its citizens machine-readable passports that satisfy the internationally accepted standard for machine readability."[27] Visa waiver partner nations would be held accountable in meeting the machine-readable technical standard for passports, a process overseen by the International Civil Aviation Organization (ICAO) in Montreal, Canada. Ostensibly, those countries not meeting the ICAO standard could be bumped from VWP status. The United States would demonstrate clearly in early 2002 that VWP countries could be dropped, with Argentina's removal from the program in the wake of its December 2001 economic crisis.[28]

Referencing a technically oriented international standards organization on the vague issue of machine readability, USA PATRIOT avoided mentioning by name the technology suggested in many remedies intended to repair the immigration apparatus that had rendered the nation vulnerable. During the time of USA PATRIOT's drafting and revision through committees on Capitol Hill, the future of the Visa Waiver Program was not entirely assured. Congress needed to know how the United States could bolster its capabilities in effectively screening visa waiver travelers as well as the implications involved in abandoning the program. Visas might be needed for all international travelers to the United States to adequately protect the American people, but reinstituting such a program would be costly. According to estimates contained within a report of the Government Accountability Office (GAO), abandoning the program would produce the need for some 14 million new visa applications, with up-front program costs of as much as $1.28 billion and recurring costs ranging, "between $522 [million] and $810 million."[29] Creating overseas positions to adjudicate visas in some of the world's most expensive cities would carry a hefty price tag.

[27] *Visa Waiver Program for Certain Visitors*, *U.S. Code* 8, Chapter 12, Subchapter II, Part II, § 1187.

[28] "Termination of the Designation of Argentina as a Participant under the Visa Waiver Program," *Federal Register* 67, no. 35 (February 21, 2002): 7943-44.

[29] General Accounting Office, *Border Security: Implications of Eliminating the Visa Waiver Program*, GAO-03-38, Washington, D.C., November 22, 2002.

Furthermore, there existed the concerns for the larger and less measurable cost of lost international tourist traffic. Presented with the hurdle of a visa interview and the lengthy wait required to get one as the State Department hired and trained new staff as well as modified and reopened consular facilities, it was logical to assume that foreign tourists would stay home or travel elsewhere. A Department of Commerce study cited by the GAO estimated that abandonment of the program could result in a loss of 3 million visitors, $28 billion in tourism exports, and 475,000 jobs."[30] According to the Travel Industry Association of America (TIA), September 11, ostensibly in combination with other factors, would produce an 11 percent decline in international visitor spending in 2002, an estimated "loss of $9.2 billion."[31] Abandoning VWP could only worsen matters for the travel industry.

In a February 28, 2002 hearing, House Immigration Subcommittee Chair George Gekas asked the TIA's representative to consider where "persons seeking good travel" might choose to visit "if we obliterated our visa waiver," an issue he stated he was not contemplating.[32] Exactly how close the U.S. Congress came to abolishing the Visa Waiver Program is unknown; however, repair was clearly needed. If the VWP could not be abolished, then policy would be required to fix it. The preferred remedy was one proposed by Bilrakis, Feinstein, Weldon and others—a technology called biometrics. In no less than 53 bills proposed before the House and Senate during the 107th Congress, the term "biometric" was included. Some time later, the Congressional Research Service would create a strong working definition of the term:

> Biometrics are physical or behavioral characteristics of a person that can be measured and used for identification. Fingerprint patterns are a familiar example. Of the biometric technologies so far deployed or tested by border security agencies, fingerprints and face recognition are the most commonly used, and iris scans are widely viewed as promising for future applications. Images and measurements of biometrics are typically digitized and reduced to a numerical identifier that is unique to a particular person. Biometric identifiers can then be used for two distinct purposes, identity verification and identity discovery. In other words, they can answer two questions: Is this person really

[30] General Accounting Office, *Border Security.*

[31] House Committee on International Relations, *Implications of Transnational Terrorism on the Visa Waiver Program,* 107th Cong., 2nd sess., February 28, 2002, 58.

[32] House Committee on International Relations, *Implications of Transnational Terrorism*, 64.

who he says he is? and Who is this person?[33]

Already the United States was collecting fingerprint data in issuing a special immigration document, the Border Crossing Card (BCC), to Mexican citizens.[34] Only a week before the September 11 attacks, Senator John Kyl entered a bill in the Senate to extend the program an additional year. After the attacks and allegations linking Moussaoui to Al Qaeda and the Reed shoe-bombing attempt, biometric technology seemed to capture the imagination of policymakers. Shutting down VWP was hugely unappealing on cost grounds, loss of economic activity and the possible negative impact on the United States' bilateral relations with member countries. Technology might be used to address the problem by applying biometric data to the standard international travel document, the machine-readable passport.

Revising the Immigration and Nationality Act (INA), the drafters of the sweeping USA PATRIOT legislation chose a peculiar maneuver to move forward on the technological overhaul of the passport. While a biometric passport was not explicitly mandated, room was given in the law to provide a broader space for innovation. As amended, the INA language regarding passport technical specifications now dictated that the document "[satisfy] the internationally accepted standard for machine readability."[35] Rather than legislate the standard, specifics regarding the biometric component could be couched within the more general heading of machine readability, a standard set by the ICAO. Aiding the ICAO would be one of the United States' great resources on biometrics, information technology, and travel documents. Former Deputy Assistant Secretary of State for Passport Services Barry Kefauver, who worked in the machine-readable and secure document business[36] after his retirement from the State Department in 1995, would have a considerable role in managing the ICAO's New Technology Working Group and coordinating with the International Organization for Standards (ISO) on the

[33] Daniel Morgan and William Krouse, *Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues* (Washington, DC: Congressional Research Service, Library of Congress, 2005) 2

[34] Andrew Schulman, "The US/Mexico Border Crossing Card (BCC):
A Case Study in Biometric, Machine-Readable ID," April 29, 1992, http://www.undoc.com.

[35] *Visa Waiver Program*, *U.S. Code* 8.

[36] "Statistica Modernizes Border Control Abroad," *Washington Technology*, July 27, 1995, http://www.washingtontechnology.com/news/10_8/news/9468-1.html.

technical specifics. As the State Department's Bureau of Consular Affairs moved toward the deployment of a biometric-bearing electronic passport under congressional mandate, it would partner with an individual rich in job knowledge to upgrade the standard for machine readability to include a much larger biometrically enabled data component.

### *Security Through Passports*

By 2002 preserving the Visa Waiver Program would primarily be dependent on the activity of scientists and engineers. Congress had opened the door for passport machine readability to include a biometric component. The law stipulated that the U.S. government succeed in a technical achievement that would produce a passport document containing some piece of data that would allow a machine to draw a comparison with a physical attribute of its holder. Sought was a high-accuracy system with which to verify identity and prevent forgery:

> The new passport design is intended to serve two purposes: (a) the biometric information can be used for identity verification at border control, and (b) cryptographic technologies can be used to ascertain the integrity and originality of passports, thus preventing high quality passport forgeries that might otherwise pass a visual inspection.[37]

But biometric devices were not an entirely mature technology in 2002, and some areas of biometric development outpace others. Furthermore, adding a computational component to the passport might draw out the Pandora's Box of integrity, security and privacy issues regarding digital technology. The end goal was a more secure set of immigration controls, but the new data element would have to be secure from tampering as well. With an immense record of computer security breaches and data leaks continuing to flood the popular media, questioning whether the e-passport's data component could be secured as well as the printed document would seem valid.

Securing computer technology is immensely expensive, time-consuming work, with high-profile targets, such as the software of leading developers or the computer networks

[37] Guarav S. Kc and Paul A. Karger, *IBM Research Report: Preventing Attacks on Machine Readable Travel Documents (MRTDs)* (Yorktown Heights, NY: IBM Research Division, March 10, 2006) 3.

of major corporations or high-visibility government agencies enduring a high volume of attacks.[38] In granting authentication to computer systems, security is divided between three general categories: information that the user knows, such as a login and password; a token the user holds, such as an identification card; and a unique physical attribute, such as a fingerprint or iris scan. For most interactions with computer systems, users have been required only to have a one factor level of security, traditionally their unique user identification and password. Increasingly, however, two- and even three-factor schemes for authentication are gaining favor in enhancing the level of trust in online transactions. Three-factor authentication, which adds a biometric component that is unique to the user, represents the highest degree of certainty currently available in verification. By combining the passport, a token, with a biometric, the immigration authority would have two-factor authentication of identity before the traveler could answer a question beyond, "Passport please?"

### *Crafting the Electronic Passport*

A key challenge for management of legal immigration within the Visa Waiver Program was and remains to elevate the level of confidence in establishing the identity of travelers and validity of their travel documents through the employment of technical measures. Increasingly, government looks to information technology and computational resources to enhance the immigration inspector's capacity to detect fraud and deception. Offering the possibility of producing a machine-determinable match between person and document, biometric data offer the enticing possibility to retool the immigration process, thereby cutting costs and freeing assets for use in other areas, including the interdiction of illegal immigration conducted outside government-controlled ports of entry. This thinking is emblematically displayed in Malaysia's implementation of a biometrically driven, automated entry system for its citizens. "When flying through Kuala Lumpur International Airport, a Malaysian citizen passes through an automated gate that reads the

[38] John D. Howard, "An Analysis of Security Incidents on the Internet 1989 –1995," (Ph.D. diss., Carnegie-Mellon University, 1997).

thumbprint from the chip and compares it to the thumb pressed on a [fingerprint] scanner."[39]

Before 9/11, absent an international standard for a biometric passport, Malaysia deployed a system embracing efficiency that is able to clear a passenger in 15 seconds without direct permission from an immigration agent.[40] Malaysians who submitted fingerprint records to receive their passports are also issued a national identity card, known as "MyKad," which also serves as a driver's license, medical data card, public transportation ticket, and automated teller machine card; for a single token, it contains an enormous quantity of personal information.[41] Convenience and efficiency are of highest priority in the Malaysian example; however, the security of both Malaysia's ID card and passport is largely unknown.

Mitigating the risk of terrorist action through issuance of a passport with an electronic component requires the securing of that component. It is necessary then to establish if the e-passport, as conceived, designed and implemented, could be secure from electronic eavesdropping and tampering. Troubling to civil libertarians and the computer security community in the United States was the e-passport's mechanism for delivering its electronic data, the contactless smart chip technology.[42] Categorized with the Radio Frequency Identification (RFID) technology used for inventory control and a variety of other commercial applications, the contactless smart chip is a more sophisticated instrument with internal computational capabilities.[43] The smart chip, designed to be

[39] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports," in *Security and Privacy for Emerging Areas in Communications Networks, 2005*, SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communication Networks, 74- 88 (September 5-9, 2005).

[40] Dato Mohd Jamal Kandi, *The Malaysian Electronic Passport*, Twelfth Meeting of the Facilitation Division, International Civil Aviation Organization (Cairo, Egypt, March 22 – April 2, 2004).

[41] MyKad, Multipurpose Card, "Single Card Multiples Solutions," (Malaysia: Government of Malaysia), http://www.jpn.gov.my/kppk1/Index2.htm.

[42] The ICAO created "technical specifications for passports to contain a paper-thin integrated circuit—basically, a tiny computer. This computer has no internal power supply, but when a specially designed reader sends out a radio signal, a tiny antenna draws power from the wave and uses it to wake the computer up. The computer then broadcasts back the data that are stored in it." "New Look Passports," *The Economist*. February 12, 2005, http://www.economist.com/science/displaystory.cfm?story_id=E1_PGGGTST

[43] Kc and Karger, *IBM Research Report*.

electronically read by a specialized piece of equipment when the document is in close proximity, was thought to add an additional layer of defense, making the forger's work harder.

Adding a computerized element to improve the passport's resistance to tampering invites some mention regarding the forgery and fraud problem for the passport's text and image. Both previously issued passports and blank passports may be stolen. United States passports are issued with a 10-year period of validity, and those issued in 1997 did not include the same physical security features as those turned out in 2001 or 2005. Forgers have employed a variety of tactics in substituting passport photographs, revising text, and in ideal conditions, creating passports for a false identity utilizing a blank document. [44] Forging the passport has traditionally been an exercise in typography, chemistry and attention to detail; however, application of computing technology has further enhanced the forger's capabilities. One must assume that the electronic passport was largely conceived as a response to the expanding, digitally enabled capabilities of the forger.

Troubling is the enormous stock of passport documents with which false or altered identities may be assumed. The number of lost and stolen passports from visa waiver countries is staggering. In 1999, the U.S. Department of Justice's (DOJ) Inspector General's office cited that the agency was aware of 61,836 stolen blank passports from visa waiver countries.[45] Between April 2002 and June 2004, more than 300,000 U.S. passports were reported lost or stolen to the Department of State.[46] These daunting figures, as well as the anecdotal record of failed and successful use of visa waiver

[44] One of the co-conspirators in the 1993 World Trade Center bombing, Palestinian Ahmed Ajaj, attempted to re-enter the United States with a photo-substituted Swedish passport. Ajaj had previously resided in Houston, while pursuing a claim of political asylum with the Immigration and Naturalization Service. J. Gilmore Childers and Henry J. DePippo, "Foreign Terrorists in America: Five Years after the World Trade Center," (Washington, DC: Senate Judiciary Committee Subcommittee on Technology, Terrorism, and Government Information, February 24, 1998).

[45] Department of Justice, Office of the Inspector General, *The Potential for Fraud and INS's Efforts to Reduce the Risks of the Visa Waiver Pilot Program*, Report Number I-99-10, March 1999, http://www.usdoj.gov/oig/reports/INS/e9910/i9910results.htm.

[46] The author contacted the Bureau of Consular Affairs, Office of Public Affairs, to inquire on the official policy of disclosure regarding stolen, blank U.S. passports on January 12, 2007. No formal response has been received regarding the query.

passports, valid or altered, led Representative Henry Hyde of Illinois to opine, "A stolen passport may be worth more than its weight in gold."[47]

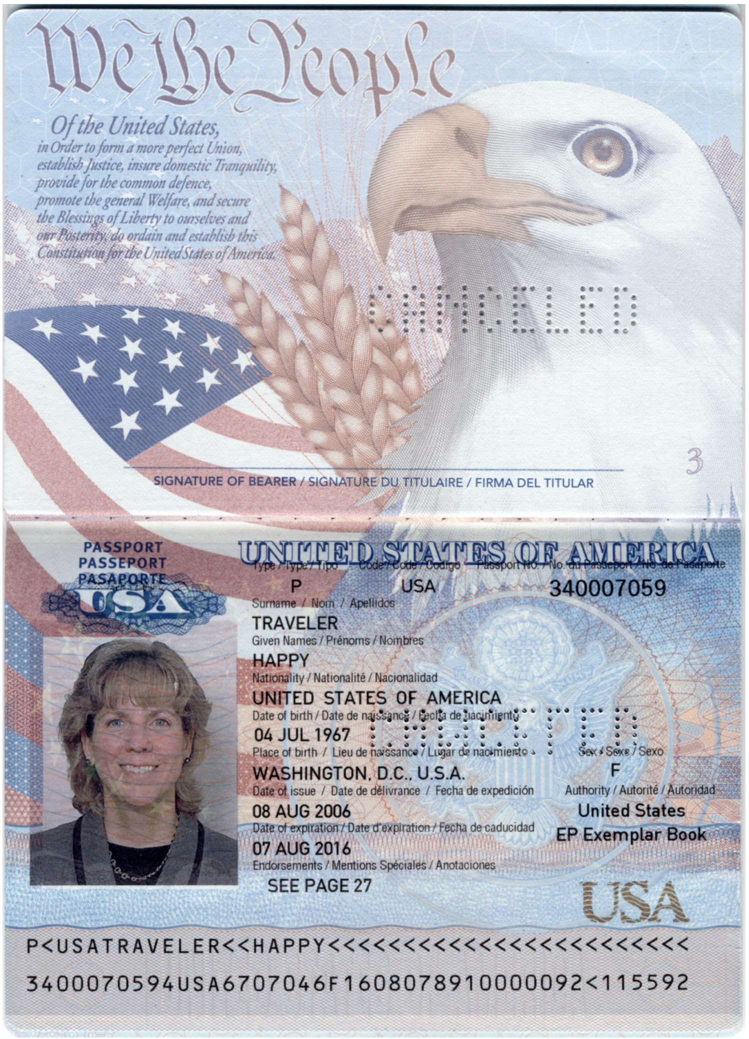
There is considerable credence to the claim, "doing a passable job of doctoring a typical passport is not very hard."[48] Accepting this, the need for additional security features falling under the heading of machine-readable becomes apparent. Photo substitution is rendered far more difficult by the printing of digitally scanned passport photographs directly onto the document's biographical page rather than using a laminate over the applicant-submitted photograph. "Photodigitization has been an unqualified success.… We have now produced over 25 million passports using photodigitization and the number of credible alterations we have encountered still number in the single digits."[49] Despite this significant improvement, policy demanded a more comprehensive system of features to beat passport fraud.

[47] House Committee on International Relations, *Stolen Passports, a Terrorist's First Class Ticket,* 108th Cong., 2nd sess., 2004, 6.

[48] Jeff Goodell, "How to Fake a Passport: The Global Capital of Identity Fraud is Belgium, Where All it Takes is an Easily Stolen Blank, a Laser Printer and Some Candle Wax," *New York Times Magazine*, February 10, 2002, 44.

[49] Assistant Secretary for Consular Affairs Maura Harty, statement on the *Enhanced Border Security and Visa Reform Entry Act* to the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security, January 28, 2004, http://www.state.gov/r/pa/ei/othertstmy/32986.htm.

FIGURE 2: THE PASSPORT BIOGRAPHICAL PAGE WITH DIGITAL PHOTOGRAPH



We the People

Of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

CANCELED

3

SIGNATURE OF BEARER / SIGNATURE DU TITULAIRE / FIRMA DEL TITULAR

PASSPORT
PASSEPORT
PASAPORTE
USA

UNITED STATES OF AMERICA

Type / Type / Tipo: P
Code / Code / Código: USA
Passport No. / No du Passeport / No. de Pasaporte: 340007059
Surname / Nom / Apellidos: TRAVELER
Given Names / Prénoms / Nombres: HAPPY
Nationality / Nationalité / Nacionalidad: UNITED STATES OF AMERICA
Date of birth / Date de naissance / Fecha de nacimiento: 04 JUL 1967
Place of birth / Lieu de naissance / Lugar de nacimiento: WASHINGTON, D.C., U.S.A.
Sex / Sexe / Sexo: F
Date of issue / Date de délivrance / Fecha de expedición: 08 AUG 2006
Authority / Autorité / Autoridad: United States EP Exemplar Book
Date of expiration / Date d'expiration / Fecha de caducidad: 07 AUG 2016
Endorsements / Mentions Spéciales / Anotaciones: SEE PAGE 27

CANCELED

USA

```
P<USATRAVELER<<HAPPY<<<<<<<<<<<<<<<<<<<<<<<<
3400070594USA6707046F1608078910000092<115592
```

*Source: U.S. Department of State*

New digital features ostensibly could enhance security of the immigration system as well as the susceptibility of the document to fraud and forgery. Although not directly stipulated in the USA PATRIOT Act, there existed the mandate to work with the ICAO on meeting "the internationally accepted standard for machine readability."[50] Reporting from the former Immigration and Naturalization Service showed that the numbers for surreptitious entry employing stolen blank passports were considerably lower for machine-readable documents than ones not carrying the electro-optically-scanned

[50] General Accounting Office, *Border Security*, 13.

alphanumeric data.[51] After passing USA PATRIOT with only a machine-readable clause, the U.S. Congress legislated the biometric passport into effect with the Enhanced Border Security and Visa Entry Reform Act, which was signed into law on May 14, 2002. The "Technology Standard for Visa Waiver Participants" deserves citation at length.

> Not later than October 26, 2004, the government of each country that is designated to participate in the visa waiver program established under section 217 of the Immigration and Nationality Act shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization.[52]

Enacted was the requirement to create a technical standard incorporating a mechanism for passing biometric information from the passport of a foreign country to some type of computerized machine able to make a real-time comparison between the electronically stored physical attribute and an electronic capture of the same attribute at the immigration station. Fixing the visa waiver through the implementation of new technologies for the verification of identity would require new technical standards agreed upon by the ICAO and by extension the ISO. Through the same legislation, new requirements for machine readability and biometrics were also mandated for nonimmigrant visas. The State Department had been collecting biometric data, a fingerprint, from Mexican visa holders since 1996; presumably the same could be done for other foreign nationals. But for the electronic passport, the data would be collected not by American consular officers, but the foreign governments of the VWP. To make a fingerprint biometric work, VWP countries, including the United States, would need to collect fingerprints (likely the right and left index fingers) of all passport applicants.

Operating under deadline from the United States Congress to deploy the biometric-enabled e-passport, the U.S. State Department began its work with the ICAO on the new

[51] Department of Justice, Office of the Inspector General, *The Potential for Fraud and INS's Efforts to Reduce the Risks of the Visa Waiver Pilot Program*, Report Number I-99-10, March 1999, http://www.usdoj.gov/oig/reports/INS/e9910/i9910results.htm.

[52] *Enhanced Border Security and Visa Entry Reform Act of 2002*, Public Law 107-173, 107th Cong., 2nd Sess., (May 14, 2002) http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=107_cong_public_laws &docid=f:publ173.107.

technological features. Former Passport Services Deputy Assistant Secretary Kefauver assumed his role on the New Technology Working Group, and the ICAO moved forward on setting a standard for a biometric component for the electronic passport. ICAO would determine which type of biometric best suited the passport, then the VWP countries would need to determine how to field the contactless chips, chip readers, biometric recognition equipment, and the other assorted pieces needed to make the system work by October 26, 2004. For the United States, Public Law 107-173 stipulated that the equipment necessary to perform this function be installed "at all ports of entry of the United States equipment and software to allow biometric comparison and authentication of all United States visas and other travel and entry documents issued to aliens," including visa waiver passports.[53] It was a hugely ambitious directive.

As the latest step in creating globally accepted standards for passports, the ICAO could draw on its previous experience in the creation of the standard for the Machine Readable Travel Document (MRTD).[54] In accordance with a standard adopted by the ICAO in 1980, passports of many countries became machine-readable through the employment of optical character recognition technology similar to that used in banking to scan personal checks.[55] The ICAO MRTD standard specified in Document 9303 established a system to eliminate the manual data entry of information from the passport into computer databases, speeding the entry process and improving the quality of information while mitigating data entry error issues.[56]

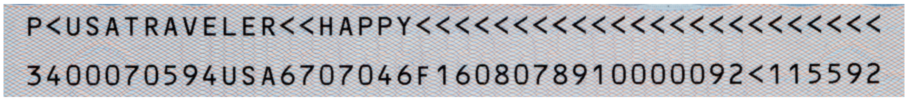
[53] *Enhanced Border Security and Visa Entry Reform Act of 2002*.

[54] The machine-readable component represented "two lines of 44 characters on the passport's data page that encapsulate the essential information – name, country, and passport number." "Passport to Nowhere: the Radio-Tagged Biometric Passport Won't Faze Industrious Terrorists," *IEEE Spectrum*, January 2005, 54.

[55] ICAO, "Document 9303, Machine Readable Travel Documents," October 2004.

[56] The seriousness of operator error is underlined by a recent example in which an instruction by a Mizuho Financial Group trader to sell 610,000 shares of a stock on the Tokyo Exchange at ¥1 rather than a single share for ¥610,000. Amplifying the mistake was the fact that the security traded was an initial public offering (IPO). The incident would cost Mizuho in excess of $224 million. "Mizuho Says Trader Error to Cost it at Least $224 Mln," *Bloomberg.com*, December 9, 2005, http://www.bloomberg.com/apps/news?pid=10000080&sid=a0rSxr9MJe_E&refer=asia.

FIGURE 3: MACHINE READABLE TEXT



P<USATRAVELER<<HAPPY<<<<<<<<<<<<<<<<<<<<<<<<

3400070594USA6707046F1608078910000092<115592

*Source: U.S. Dept. of State*

Building on the optical character recognition standard for machine readability, the ICAO would need to craft a standard for embedding data on a microchip within the passport as well as specifying the details on the biometric component. A decision was needed on what biometric or biometrics to utilize in meeting the congressional mandate. It would come, in principal, with the 2002 Berlin Resolution of the ICAO's Technical Advisory Group/Machine Readable Travel Document (TAG/MRTD) New Technologies Working Group (NTWG). The body endorsed, "the use of face recognition as the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents."[57] Although it called for digital representations of the document holder's other unique physical attributes, such as fingerprint or iris scan to be embedded within the passport, the focus of the effort would be facial recognition. The United States had been using the fingerprint biometric since 1996, yet the ICAO selected a different one. Why?

After the Berlin Resolution, the NTWG released a formal declaration supplemented with additional guidance prepared from its March 2003 meeting in New Orleans. The body stipulated that the same photograph represented on the biographical page of the document would be stored digitally on the contactless chip. In function, the passport reader machine could now pull the biographical information from two sources, the strip of machine-readable letters and the chip, as well as lifting the image data from the chip. The inspector could ostensibly compare the printed image in the passport and the electronic one appearing on his or her computer terminal's screen displaying the traveler's likeness and immigration records. In passing the image, two fundamental requirements existed: the image had to be small in size; and it had to be of a format generally recognizable by computers. The Working Group selected the International Standards Organization 10918

[57] ICAO TAG/MRTD NTWG, "Biometrics Deployment of Machine Readable Technical Documents, Version 2.0," May 21, 2004.

format, the JFIF, or Joint Photographic Experts Group File Exchange Format, commonly known as the JPEG, preferred for utilization on the Web due to its small size. A file size of 2 Kilobytes (KB) was selected for inclusion on the data microchip although the ICAO recommended use of an image not less than 11 KB in size.[58]

Desired was the capacity to collect enough data from the e-passport image to compare against images collected during the entry interview and determine a match between them in near-instantaneous fashion, a true biometric test. This would require application of research in the creation of computer systems able to match two-dimensional photographic images taken at different times, in different locations, under different conditions. Crafting of logarithms capable of culling sufficient data points to positively match the document and its holder covers a variety of approaches. One promising area of inquiry studies symmetry in biological constructs, from proteins to the geometry of the human face. By embracing mirror-image symmetry, the problem is simplified by essentially removing half of the picture and inserting instructions to rebuild the whole image from what is available, a process known as symmetry preserving single value decompression or SPSVD.[59] SPSVD represents only one possible avenue for continuing research[60] and is not a mature technology ready for fielding in the near term. With a hypothesized accuracy rate of approximately 80 percent under controlled conditions, current technology in this area falls short of expectations for application in immigration control.[61] Another set of researchers has pursued work in exploring how highly compressed JPEG graphics may be used for biometric applications without degradation in biometric applications. They assert that small graphic files may work as well as larger ones, but the

[58] FCD 19794-5, "Biometric Data Interchange Formats – Part 5, Face Image Data," (New York: Technical Committee ISO/IEC JTC 1, Biometrics, American National Standards Institute, 2004).

[59] Mili Shah and Danny Sorenstam, "A Symmetry Preserving Singular Value Decomposition," *Society for Industrial and Applied Mathematics*, 2006, http://www.siam.org/journals/simax/28-3/64667.html.

[60] Face recognition research is conducted by a number of groups utilizing a variety of approaches. Particularly prolific are those engaging in independent component analysis (ICA): M.S. Bartlett, H. M. Lades, and T. J. Sejnowski, "Independent Component Representations for Face Recognition," in Proc. SPIE Symposium. *Electronic Imaging: Science Technology—Human Vision and Electronic Imaging III*, ed. T. Rogowitz and B. Pappas (San Jose, CA, 1998).

[61] Mili Shah, Personal communication with the author, December 5, 2006.

success rate for face recognition trials rarely exceeded 80 percent, hardly a workable figure for use in immigration control.[62]

Moving from the laboratory to deployment for face recognition does not appear to have been a smooth process for the United States. Documentation released in response to Freedom of Information Act (FOIA) requests for material related to e-passport tests by the U.S. Department of Homeland Security (DHS) under simulated operating conditions revealed that the compression and decompression "of images stored on some e-passports caused the image extracted to be of too poor a quality for automated facial comparison."[63] Nonetheless, DHS continued to pursue automated facial recognition biometric despite the formidable set of issues present in making such a system work.

Although its strong potential capacity to correctly identify highly individualized, distinct features in a relatively unobtrusive manner makes facial recognition a highly desirable form of biometric authentication, there exists considerable evidence that in application, the technology remains highly prone to failure. The National Institute for Standards and Technology (NIST), a component agency of the U.S. Commerce Department increasingly involved in assessing and creating policy regarding information technology and computer security, continues to engage in extensive testing of biometrics including facial recognition. Inherited by NIST, the U.S. Department of Defense Counterdrug Technology Development Program Office's Face Recognition Technology (FERET) program[64] continued with ongoing Face Recognition Vendor Tests (FRVT) building on FERET work to foster the development of facial recognition equipment by private industry for government application. The goal for a fielded system is highly ambitious, as

[62] Kresimir Delac, Mislav Grgic, and Sonja Grgic, "Effects of JPEG and JPEG2000 Compression on Face Recognition," *ICAPR 2005*, LNCS 3687 (2005): 136 – 145.

[63] Department of Homeland Security, International Civil Aviation Organization, and International Organization for Standardization, *E-Passport Mock Port of Entry Test November 29 thru December 2, 2004: Operational Impact on the Inspection Process*, obtained by Electronic Privacy Information Center (EPIC) through FOIA requests, 19.

[64] P.J. Phillips, Hyeonjoon Moon, S.A. Rizvi, and P.J. Rauss, "The FERET Evaluation Methodology for Face-Recognition Algorithms," *Pattern Analysis and Machine Intelligence*, IEEE Transactions on Pattern Analysis and Machine Recognition, October 2000.

NIST "wants companies to demonstrate … 98 percent reliability for facial recognition systems,"[65] a figure far higher than research programs in the field have produced.

Outside controlled conditions, biometric facial recognition—producing matches between a representation of the document holder's face electronically stored within the travel document with one capturing the traveler's appearance at the immigration desk—has not met initial or revised deadlines for the implementation of the program in the United States and elsewhere. Although the technology strives to employ a logarithmic approach emphasizing facial geometry, for example the distance between the eyes, lighting and other factors often produce false rejections within the automated system. FERET tests in the late 1990s revealed that comparison of a database image with one captured under different lighting conditions on the same day would produce a false rejection rate of nearly 10 percent. When the stored image was compared against one taken 18 months later, the false reject rate rose to 43 percent. In addition, other real-world conditions reduce the efficacy of automated face recognition, with differences in camera angle to subject between the stored and live images as low as 15 degrees, significantly raising the false reject figure.[66] For a travel document holding a 10-year period of validity, these observations are deeply troubling.

Skepticism regarding the viability of the facial recognition component of the e-passport has emerged from the electrical and electronic engineering community. Employing a scanned passport photograph to create a biometric identification feature appears a flawed exercise. The chair of the International Biometrics Foundation is one critic, stating in 2005, "'You could say an image of anyone is a biometric of some sort but I think it is a shame it has been extended that far.'"[67] Purdue University's Stephen Elliott casts doubt on the utility of the scanned photograph suggesting, "In an ideal situation, passport authorities would call applicants in to have their photograph taken or to undergo a 3D

[65] "Passport to Nowhere," 55.

[66] D. Jonathon Philips, et al., "An Introduction to Evaluating Biometric Systems," *IEEE Computer*, February 2000.

[67] Chris Edwards, "Borderlands of Confusion," *IEEE Review*, November 2005, 36.

face scan."[68] The United Kingdom Passport Office has reported that photographs submitted with passport applications also are problematic, with one in every seven images rejected as unusable.[69] Even Barry Kefauver, the former State Department official tasked with leading the ISO and ICAO effort to develop a standard e-passport admitted that tests of the technology "raised a host of concerns" when quoted in an article that deemed the technology a "loser system."[70]

Despite its flaws, the United States and the visa waiver countries have moved forward in implementing the facial recognition standard. Considerable technical obstacles in producing a workable biometric standard have not, however, served as the primary area of contention regarding the adoption of the biometric-enabled e-passport. Although it remains to be seen whether or not the face recognition biometric actually works under real-world conditions at all of the United States' ports of entry, far more criticism has been heaped upon the contactless chip technology and its capacity to adequately safeguard the individual data it stores and transmits in this particular application.

With the deployment of supporting infrastructure for utilizing the biometric component of the e-passport very much a work in progress several months after the United States' switch to the document, the other overarching policy question for this new technology remains: Is the e-passport secure from monitoring, replication, and manipulation? According to Bruce Schneier, computer security authority for the American Civil Liberties Union (ACLU) and IBM, among others, the answer is an emphatic "no." In an op-ed for the *The Washington Post*, Schneier asserted, "Your passport information might be read without your knowledge or consent by a government trying to track your movements, a criminal trying to steal your identity or someone just curious about your citizenship."[71] The ACLU argued the international standard for electronic passports "will

[68] Edwards, "Borderlands of Confusion," 36.

[69] Bryan Betts. "UK Passport Service struggles with facial recognition," *TechWorld*, January 12, 2006.

[70] "Passport to Nowhere," 55.

[71] Bruce Schneier, "The ID Chip You Don't Want in Your Passport," *The Washington Post*, September 16, 2006, A21.

leave citizens vulnerable to identity theft, invasions of privacy, or worse."[72] After tipping off State Department officials regarding their concerns, IBM researchers stated that the new passport made it "possible to stalk selected passport holders … facilitate identity theft crimes," and "a previous version of the ICAO specification could have *facilitated* passport forgery."[73] Since the beginning of the e-passport project, security issues have emerged, while concerns for privacy and abuse of personal data have dominated debate.[74]

Internal discussion at the State Department regarding security features has consistently advocated little effort in the area. In an August 2003 memorandum to Assistant Secretary for Consular Affairs Maura Harty, the State Department's lead on passport affairs, Frank Moss, downplayed issues of security for data stored on the device. Moss stated, "Data written to [a] chip and data exchanged between a reader and a passport will be free and clear without the need for encryption."[75] Addressing the possible vulnerability of the e-passport to clandestine electronic monitoring or "skimming," Moss added the following:

> There is little risk here since we plan to store only the currently collected data and a facial image which are already stored visibly on the passport. In order to facilitate travel through automated border crossing gates, the U.S. will recommend against the use of pins [personal identification numbers] or other methods that might be required to unlock a chip for reading. DHS concurs with this position.[76]

A State Department internal report filed regarding the May 2003 NTWG subcommittee meeting mentioned the skimming problem and detailed U.S. views on the topic at length. While some European Union members fretted about the failure to adequately safeguard data on the contactless chip, the document raised concerns about the cost of more sophisticated passport screening machinery and the potential for added security measures to derail automated border gate systems such as Homeland Security's Secure Electronic

[72] American Civil Liberties Union, "Naked Data: How the U.S. Ignored International Concerns and Pushed for Radio Chips in Passports Without Security, An ACLU White Paper," November 24, 2004, 1.

[73] Kc and Karger, *IBM Research Report*, 2.

[74] This paper acknowledges the importance of concerns regarding the potential for abuse by government of civil liberties enabled by digital technologies, but the author chooses not to direct significant attention to the topic with this work.

[75] Frank Moss, *State Department Internal Memorandum, Special Meeting of the PKI Sub-Group of ICAO New Technologies Working Group*, document released in response to ACLU FOIA request, August 23, 2004, 2.

[76] Moss, *State Department Internal Memorandum,* 2.

Network for Travelers Rapid Inspection (SENTRI) program. German officials in particular raised concerns that the storage mechanism would not comply with European legislation on individual privacy. For the United States, the only desired encryption would be an electronic signature[77] used to verify the validity of the data on the chip.[78] The Americans at the table did not view skimming as a problem, but under pressure from privacy advocates, the State Department would eventually incorporate some basic security features, including Basic Access Control (BAC) encryption and metallic shielding, embedded in the passport cover designed to defeat electronic eavesdropping known as a Faraday Cage.

Deep flaws were identified within the new passport design with regard to the chip's computer security features, both as originally proposed and following the adoption of BAC, an encryption scheme designed to permit the passage data only to an authorized reader machine, such as those used by immigration authorities. The IBM researchers determined the initial electronic signature regime would make "counterfeiting biometric passports … easy." A forger could splice together valid electronic signatures with false identity information and biometric data.[79] After the incorporation of BAC, a Dutch computer security expert discovered that the encryption of his country's new passports could be defeated by a personal computer generating all possible key sequences in less than two hours and that the chip itself could be cloned by defeating the encryption scheme as well.[80]

Rising to the cloning challenge, German security consultant Lukas Grunwald was able to copy the chip but could not alter the data stored on it in a manner undetectable upon inspection due to the digital signature utilized. Moss' response, as summarized by the IEEE, accepted the cloning flaw, but he assured that "the passport's designers have long

[77] Definitions of electronic or digital signatures are varied as are implementations of the technology, however for the purposes of this report, an electronic signature may be considered a large, unique identifying number used to electronically identify the document.

[78] Trip Report, *ICAO NTWG PKI Subcommittee Meeting*, London, England, document released in response to FOIA request from the ACLU, September 4-5, 2003.

[79] Kc and Karger, *IBM Research Report,* 6.

[80] Marc Witteman, "Attacks on Digital Passports," in the *What the Hack* conference (Liempde, the Netherlands, July 27, 2005) http://wiki.whatthehack.org/index.php/Track:Attacks_on_Digital_Passports.

known about the chip's ability to be cloned and have added security safeguards into the passport's design, such as embedding the passport holder's digital photo into the data page."[81] This claim echoes Harty's congressional testimony regarding the robustness of photodigitization in thwarting forgers mentioned earlier.[82] Although the digital signature exposes tampering in 2006, that may not be the case in 2016, when the first e-passports expire. A general problem for the 10-year validity passport remains. "Today's digital signatures … do not guarantee the desired long-term security." The passport chip does not have the capacity to evolve retroactively to meet new threats. Furthermore, using the radio-based contactless chip limits the capacity of digital signature and encryption schemes, "since they require too much computing power and storage."[83]

An additional set of technical concerns revolved around radio issues, as contactless chips are activated when they come into contact with radio energy at the proper frequency. As the U.S. "transparency lobby"[84] has expended significant effort in exposing the potential for government to abuse data—either surreptitiously or legitimately—collected via radio-enabled electronic passports, this study defers to the considerable literature created in shaping the debate in Washington. Accepting privacy concerns as valid, the standard for the contactless chip selected, ISO 14443, does possess other attributes that may be exploited by parties not holding legitimate need to access the data contained on the electronic passport. While cryptographic weakness and susceptibility to cloning have been discussed already, there remain problems of clandestine tracking and scanning, eavesdropping, and data leakage.[85] The contactless chip enters the passport document into the radio area of the electromagnetic spectrum. The passport is transmitting through the air its electronic contents when activated by the proper radio signal. Although the close-proximity contactless chip is designed only to work when it is within four inches of a chip reader, technology exists that may permit reading the chip from many feet away.

[81] Brandy Ortega, "NewsBriefs," *IEEE Privacy & Security*, September-October 2006, 10.

[82] Assistant Secretary for Consular Affairs Maura Harty, statement to the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security.

[83] J. Buchmann, A. May, and U. Vollmer, "Perspectives for Cryptographic Long-Term Security," *Communications of the ACM 49*, 9 (2006): 54.

[84] Alasdair Roberts, *Blacked Out: Government Secrecy in the Information Age*, (New York: Cambridge University Press, 2006).

[85] Juels, Molnar, and Wagner, "Security and Privacy Issues in E-passports," 74- 88.

In 2004 tests at the Morgantown, West Virginia, facility of the National Biometric Security Project, "NIST testers were able to lift 'an exact copy of digitally signed private data' from a contactless e-passport chip [lacking the later Faraday Cage] 30 feet away."[86]

Understanding why the NIST team succeeded in scanning the chip requires some background on the evolution of wireless communication. The e-passport's contactless chip and all of the technologies falling under the Radio Frequency Identification (RFID) label evolved from technology developed during the Second World War to identify aircraft. Although radar could detect aircraft, its significant shortcoming was in its inability to tell friend from foe. To prevent fratricide the Allies developed a technology to pass identity back to the radar operator in addition to location. This technology, the Identification Friend or Foe (IFF) transponder, is a device that passes identity information when properly queried by a radio signal. The type of RFID chosen for the contactless chip works in very much the same manner. A transmitter sends a signal to the chip and the chip replies. Unsurprisingly, the electronics industry developed many variations of IFF countermeasures and counter-countermeasures in the struggle to retain the advantage of knowing who is who.[87] Protecting the contactless chip is a similar effort in countermeasures, provided through shielding the chip from detection and unauthorized transmission. The potential downside of failure in this area could be very serious indeed.

As a transponder, a device for receiving a radio signal and automatically transmitting a responding signal, the contactless chip attracted the imagination of technical experts. With the remotely detonated improvised explosive device (IED) being the leading killer of American soldiers in Iraq, the question was posed and answered regarding the e-passport's potential use as a trigger for an explosive device.[88] At the 2005 Computers, Freedom & Privacy Conference, Frank Moss dismissed the possibility of detecting e-passports at a distance, stating, "The idea that you can walk down a hotel hallway and

[86] Junko Yoshida, "Tests Reveal E-passport Security Flaw," *EE Times Online,* http://www.eetimes.com/showArticle.jhtml?articleID=45400010.

[87] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "The Evolution of RFID Security," *Pervasive Computing*, IEEE, 5, no.1 (January – March 2006): 62- 69.

[88] Gregory M. Lamb, "New 'E-passports' Raise Security Issues," *The Christian Science Monitor*, October 19, 2006.

identify the Americans is, quite frankly, poppycock."[89] Fifteen months later, Flexilis, a U.S. firm specializing in security for mobile computing applications, conducted a test of a contactless chip passport mock-up employing the same standards as the U.S.-issued e-passport, in which the company's representatives touted that the electronic shielding added to thwart skimming would fail if the passport booklet was open a fraction of an inch. To dramatize the vulnerability, the company presented a video at the 2006 Black Hat computer hacking convention of a test it conducted in which it is claimed that a small charge would be detonated if a sensor detected the contactless chip's radio signature.[90] After airing the video at the conference, Flexilis posted it on YouTube and issued a press release.[91]

Although the Flexilis demonstration probably represents the unlikeliest of scenarios[92] for the real world and serves as an emblematic example of the type of publicity stunt that gains notice in the ever-growing computer security field, a former U.S. Army researcher suggested an RFID-based terrorist scenario months before the Flexilis team made their short film.[93] Another hypothetical concern could be the delivery of malicious computer code via the e-passport itself. Although the amount of data passed from the contactless chip to the immigration screening computer system is quite small, this may not be entirely discounted as a vector for attacking the networked computer system of an immigration service. Posed with this scenario, Nick DeBaggis, the individual credited by Microsoft for first discovering a computer virus embedded within the JPEG-type graphics file (the same format used in the e-passport), illustrated several examples of computer attacks triggered by programs of incredibly small size.[94] Computer security researchers Rieback, Crispo and Tannenbaum drew considerable attention in March 2006 when they

[89] Robert Lemos, "Privacy Groups Slam U.S. Passport Technology," *The Register* (UK), http://www.theregister.co.uk/2005/04/20/privacy_groups_attack_passport_tech/print.html.

[90] Felxilis, "RFID Passport Shield Failure Demonstration," http://www.flexilis.com/research.

[91] YouTube, http://www.youtube.com/watch?v=-XXaqraF7pI.

[92] James A. Lewis, "Much Smoke, No Fire: The RFID Debate," (Washington, DC: Center for Strategic and International Studies, November 2006).

[93] D.R. Thompson, "RFID Technical Tutorial," *The Journal of Computing Sciences in Colleges*, 21, no. 5 (May 2006): 8-9, presented at Mid-South Consortium for Computing Sciences in Colleges (CCSC_MS), Memphis, Tennessee, March 31 – April 1, 2006.

[94] Nick DeBaggis, email message to author, December 2, 2006.

raised the issue of computer viruses passed through RFID systems.[95] In response to the provocative paper, the authors downplayed its reception among the media as "irrational exuberance."[96] Dismissing the hysterical, they nonetheless speculated that "A disgruntled employee at an airport who has access to an authorized RFID [contactless chip] passport … could potentially re-initialize a passport with valid-looking malicious data without a problem."[97] This potential vulnerability exposes the systemic security issues requiring attention regarding the passport as well as the system of computer networks and databases with which it interacts.

Such examples and hypothetical scenarios underscore the difficulties inherent in making new computing technologies work and making them work securely. Changes were made to the e-passport largely because of political pressure from civil libertarians and privacy advocates. The delivery of the first e-passports to U.S. citizens or those of other visa waiver countries slid past a 2005 congressionally-mandated deadline, as U.S. public advocacy groups including the Electronic Frontier Foundation, the Center for Democracy and Technology, and the Electronic Privacy Information Center teamed with the American Civil Liberties Union to protest the absence of security controls. This pressure was a contributing factor to the inclusion of enhanced security features including Basic Access Control encryption and metallic shielding designed to defeat electronic eavesdropping (a Faraday Cage) by the State Department to combat issues discovered with the initial passport design. While these alterations placated some, the concept of an electronic passport remained controversial. Bill Scannel, a Washington-based independent publicist and opponent to the e-passport responsible for directing attention to the issue through a web-based advocacy campaign, expressed satisfaction that these security measures were included under pressure from privacy advocates, but said of the chip, "no matter how much stuff you layer on the technology, it is still inappropriate."[98]

[95] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?" *Pervasive Computing and Communications, 2006*, PerCom 2006, Fourth Annual IEEE International Conference on Pervasive Computing and Communications, March 13 – 17, 2006.

[96] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "RFID Malware: Truth vs. Myth," *Security & Privacy Magazine*, IEEE, 4, no.4 (July – August 2006): 70-72.

[97] Rieback, Crispo, and Tanenbaum, "RFID Malware," 70-72.

[98] Eric Lipton, "Bowing to Critics, U.S. Plans to Alter Electronic Passports," *New York Times*, April 27, 2005.

Perhaps inappropriate, but more disappointing, was the likelihood that the new technical features would not work and provide no significant additional capability in deterring or intercepting terrorists the likes of Reid.

### *Taking Stock: A Loser System?*

By the end of 2006 the State Department had begun the issuance of standard e-passports with these features included from its Denver regional passport office.[99] According to State Department figures, it is likely to issue more than 15 million e-passports in 2007.[100] In addition, passport demand in the United States should continue to rise due to the implementation of the Western Hemisphere Initiative, which will require all entrants to the United States, including U.S. citizens, to present a valid passport upon arrival at a U.S. Customs and Border Protection Port of Entry for air travelers by January 23, 2007, and at sea and land entry points in 2008. Traditionally, no passport has been required of Americans returning from Caribbean cruises, Mexican holidays or business trips to Canada, and it would seem reasonable that the new requirement will further elevate passport demand. With respect to the abolishment of visa waiver and the return to full visa adjudication, consular officers in Paris witnessed what a return to the old days would mean at their post when a labor dispute delayed the deployment of the French e-passport and took the country out of compliance with provisions of the VWP. An angry queue of French tourists and business travelers snaked around the U.S. embassy seeking visas from a beleaguered consular section, with one would be vacationer complaining, “We're not emigrating. We just want to travel to Dallas.”[101]

On a balance sheet, it is difficult to ascertain exactly what the United States has gained from the deployment of the e-passport. As Juels, Molnar and Wagner observe, there exists a risk that immigration inspectors may be lulled into a false sense of security by

[99] Lamb, “New ‘E-passports’ Raise Security Issues”.

[100] “Infineon Wins Order for U.S. Passport Chips; BRIEFING:(Finance),” *International Herald Tribune*, August 22, 2006.

[101] Doreen Carvajal, “Another Blow to U.S.-French Ties: A Visa Bottleneck,” *New York Times*, February 2, 2006.

automated screening technologies.[102] In addition, the envisaged automated facial biometric system still appears to be held up by a diverse set of obstacles as yet unaddressed by applied mathematics, computer engineering or other technical disciplines. Unfortunately, the e-passport does open up new possibilities for the unimagined in compromise of the system. For instance, compromise of the signing key encryption scheme, the mechanism used to build the digital signatures serving as a protective measure on the e-passport, is considered by DHS to be potentially disastrous, requiring the revocation of perhaps millions of travel documents.[103] This would tend to support a belief that when enhanced security is required for digital information, encryption alone should not be viewed as a panacea to the problem.[104]

### *Fielding the Technology*

In roughly five years, the United States and all but three other countries of the VWP (Andorra, Brunei and Liechtenstein are the exceptions) deployed e-passports meeting the extended deadline of October 26, 2006.[105] As this is no small feat, it remains to be asked, how much may this technology aid in protecting American citizens, at home and abroad, from terrorist activity? Or perhaps more importantly, if Richard Reid carried an electronic U.K. passport, would it provide information to airport security or the airline sufficient to deny him access to the aircraft? Unfortunately, answers to both questions would enter the area of speculation very quickly; for now they simply may be unanswerable. Casting some light on future prospects, DHS continues to discover instances in which entry is accomplished by fraudulent use of stolen blank visa waiver passports. Particularly vexing is the acknowledgement by the agency that "detecting these

[102] Juels, Molnar, and Wagner, "Security and Privacy Issues in E-passports," 74- 88.

[103] Department of Homeland Security, International Civil Aviation Organization, and International Organization for Standardization, *E-Passport Mock Port of Entry Test November 29 thru December 2, 2004: Operational Impact on the Inspection Process*, obtained by Electronic Privacy Information Center (EPIC) through FOIA requests.

[104] R.C. Bronk, "In Confidence: Information Technology, Secrecy and the State," (Ph.D. Diss., Syracuse University, December 2005).

[105] "VWP Countries Meet E-Passport Deadline," *Government Technology*, October 26, 2006, http://www.govtech.net/news/news.php?id=101923.

passports at U.S. ports of entry is extremely difficult."[106] Drawing on the computer hacking exploits detailed above, it seems unlikely that writing fraudulent data to a blank chip on a stolen blank e-passport will remain unassailable forever. Accepting this and moving on from the unanswerable, it is necessary to cull lessons from this process, through which a societal demand for enhanced protection from a set of threats produced a policy mandating the implementation of a new technology.

Foremost, it should be accepted that for a document as important as the passport, adoption of digital features should be an exercise in caution not to be rushed by legislative mandate or shielded from outside review. In this case, members of the U.S. Congress from both sides of the aisle embraced language underscoring the need to get results, but they failed to understand or receive adequate guidance regarding the cycle in which information technologies are developed, as evinced in the statement of Representative Brad Sherman, Democrat of California:

> I would point out that we as a Congress took some heat by telling our visa waiver partners they had to have biometric passports, and it is my understanding that Japan and Britain took us seriously and actually could have met the deadline. Our State Department apparently was less skilled, or took us less seriously, and could not. That is why Congress gave an extension for 1 year or 2 years, creating the kind of security at our border that is created at every McDonald's when you go to buy a hamburger with a credit card.[107]

This ambiguity is amplified, as it remains unclear as to the level of understanding of exactly what kind of biometric capability was delivered or mandated. Is a digital copy of the picture on the chip meant to serve as a representation on the immigration inspector's computer terminal that should match the photo on the biographical page, or is some manner of automatic recognition specified? State's Maura Harty chose her words carefully for hearings of the House Homeland Security committee in 2004:

> Embedding enhanced biometrics into passports so that a clear link can be established between the authorized bearer of that passport and the user is an important step forward in the international effort to strengthen border security…the Department of State has underway a program that should result in the production of our first enhanced biometric passports using the ICAO

[106] General Accountability Office, *Border Security,* 27.

[107] House Committee on International Relations, *Stolen Passports, a Terrorist's First Class Ticket,* 108th Cong., 2nd sess., 2004, 11.

> standard of facial recognition techniques in October of this year and we plan to complete the transition to this new biometric passport by the end of calendar year 2005.[108]

Congress stipulated that a biometric passport would be created, indeed innovated, upon its direction. In so doing it presumed the act of creating an internationally accepted standard for a computerized passport would make it function as envisioned. Indeed, there are certainly those holding a belief that it has. A representative of the International Air Transportation Association expressed faith in the program, stating, "The U.S. requirement for biometric passports is pushing a lot of governments in the right direction … the technology is there, these are not pie-in-the-sky discussions. There are international standards that exist."[109] Such bravado might easily lead to speculation that the influence of industry lobbies or commercial interests may prevail over rational discourse on technical feasibility. A response to a Department of State Federal Register Notice by the Smart Card Alliance (SCA) indicates just how emphatically the contactless chip lobby argues the value of its product.

Exemplifying the trade association's tenacity on the issue is debate regarding a digital document to meet the approaching the 2008 deadline when all U.S. citizens entering the United States will require some type of federally issued identity document. DHS and the State Department have begun work on the creation of a passport card, a wireless ID card which transmits information to an immigration inspector. Issued by the State Department, the new document is to be employed at the land borders, where Americans have up to now required little more than driver's license or birth certificate. Conceptually, it is an RFID-enabled Border Crossing Card. DHS already uses a "vicinity-read"[110] technology in its SENTRI and Free and Secure Trade (FAST) expedited crossing systems on the Mexican and Canadian borders, respectively, which allows communication at a distance (30 or more feet).

[108] Assistant Secretary for Consular Affairs Maura Harty, statement to the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security.
[109] Roger Blitz, "Taking Measures to Ensure a Protected Future," *Financial Times*, September 15, 2006.
[110] The RFID technology is specified under the standard ISO 18000-6, Type C.

Selection of vicinity-read RFID technology over a contactless chip system, the latter requiring automobile passengers to swipe ID cards within inches of card readers as opposed to data collection at longer ranges with the former, drew the ire of the Smart Card Alliance, which submitted a 10-page memorandum in response to the Department of State's request for public comment. It decried the new card's "lack of security safeguards" and the "inadequate discussion of implementation approach" in selecting the vicinity-read product while noting that the SCA's members provide both ISO 14443 "contactless smart card and RFID products."[111] This may be somewhat disingenuous, as the SCA's Web site includes no content advocating for the RFID (ISO 18000-6) standard (that of the new border crosser passport card) in any commercial or government application. Also interesting about the SCA Web presence is its roster of members, which includes both the Department of State and Infineon, a Munich-based firm that supplies chips for the U.S. and German e-passports. DHS is not a member. Finally, the following appears on SCA's comparison of contactless chip versus RFID for the passport card application: "Optional security features, such as additional biometrics, could also be stored in the PASS card chip and verified by the card reader. No assessment would be needed by the official."[112] This last clause is deeply disturbing, as it certainly sounds as if the SCA advocates a system in which the immigration inspector is usurped by a machine.

Understanding the mechanisms for adoption of international standards utilized in technology applications as important as the passport raises many questions. In this case did the United States foist the e-passport standard on the VWP countries in a unilateral drive at the ICAO's meetings? Were German objections on security grounds a bargaining tactic to steer a contract to a German firm? Once again, only speculation is possible, as efforts by the ACLU to gain access to ICAO meetings failed.[113] Returning to Assistant Secretary Harty, one must wonder what exactly the architect of "Secure Borders, Open Doors" meant when she asserted, "We recognize that convincing other nations to change

[111] Smart Card Alliance Comments of the Smart Card Alliance to the Department of State Federal Register Notice, "Card Format Passport; Changes to Passport Fee Schedule," 22 CFR Parts 22 and 51, RIN 1400-AC22, Public Notice 5558, 1-2, 5.

[112] Smart Card Alliance, "Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID," http://www.smartcardalliance.org/pages/publications-whti

[113] American Civil Liberties Union, "Naked Data."

and improve their passport requires U.S. leadership both at the International Civil Aviation Organization (ICAO) and practically by introducing these changes into the U.S. passport."[114]

The promulgation of the ICAO standard for the e-passport, while possibly mitigating vulnerability to terrorists attack, also produced considerable, and perhaps unnecessary, fear regarding the new document. Moving forward in the face of criticism, technical or libertarian, created of an atmosphere of distrust regarding the technology. After years of investigation and advocacy regarding the e-passport, the ACLU's Barry Steinhardt made the following admission:

> It remains a mystery to me as to what is going on here…It's either that they do want a system that will allow for Americans to be tracked when we move around with a passport, or they are just simply stubborn, and, having once set out on a course, they refuse to divert from it, and they refuse to concede they made a mistake.[115]

Through the entire process from specification to production, many critics of the new technology were unable to reach accommodation. The computer security community and its quasi-legal hacker alter-ego have more than adequately demonstrated the passport's security schemes as at least somewhat flawed and likely to be compromised within the decade-long period of validity for the document. At the same time, the biometric scheme has not been sufficiently proven to work, and any notions considering substitution of the facial recognition technology in its current form for human inspectors should be tabled as foolhardy and irresponsible. The issues in tandem, aggregating to a concern for biometrically enabled, computer-driven monitoring of movement may require remedy through additional U.S. legislation enhancing privacy and data protections similar to those in place in the European Union, a political body having the good fortune to draft its Bill of Rights during the explosive growth of cyberspace.[116]

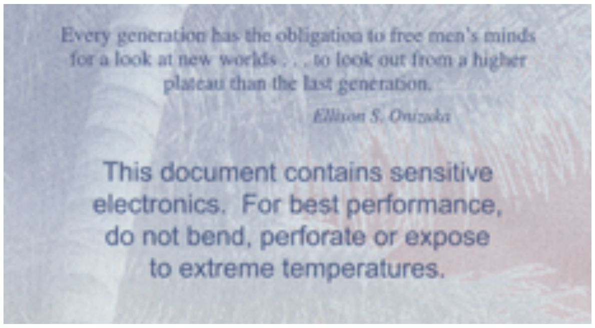
[114] Assistant Secretary for Consular Affairs Maura Harty, statement to the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security.

[115] Susan Carroll and James Pinkerton, "Change Could Cause Travel Woes," *The Houston Chronicle,* January 8, 2007.

[116] Council of Europe, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Communities*, no. L.281 (November 23, 1995).

An imperfect solution to a daunting problem, the e-passport represents the path from problem to policy and policy to technology. It is a computer system codified by law, of unknown but likely limited utility, able to be rendered inoperative with a single swift blow from any heavy blunt instrument. To change the program in any significant capacity requires accepting the advice of the Department of State's Moss, who in a detour for his prepared remarks during a Seattle speech opined, "If you really think this is a horrible idea, you better start writing to your members of Congress."[117]

FIGURE 4: INSTRUCTIONS FOR USE



Every generation has the obligation to free men's minds
for a look at new worlds . . . to look out from a higher
plateau than the last generation.

*Ellison S. Onizuka*

This document contains sensitive
electronics. For best performance,
do not bend, perforate or expose
to extreme temperatures.

*Source: U.S. Dept. of State*

[117] Robert Lemos, "Privacy Groups Slam U.S. Passport Technology," *The Register* (UK), http://www.theregister.co.uk/2005/04/20/privacy_groups_attack_passport_tech.