UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC

DIRECTOR
Deirdre K. Mulligan
(510) 642-0499
dmulligan@law.berkeley.edu

CLINIC FELLOW
Jack Lerner
(510) 642-7515
Jlerner@law.berkeley.edu

BOALT HALL SCHOOL OF LAW
BERKELEY, CALIFORNIA 94720-7200
TELEPHONE (510) 643-4800 •
FAX (510) 643-4625
http://samuelsonclinic.org/

April 22, 2005

Chief, Legal Division,
Office of Passport Policy, Planning and Advisory Services,
2100 Pennsylvania Ave., NW., 3rd Floor,
Washington, D.C. 20037

Re: Comments on RIN 1400-AB93
Electronic Passport

We appreciate the opportunity to provide the Department of State with comments on the proposed rules with respect to "electronic passports." These comments respond to the Federal Register Notice of February 18, 2005 by the Department of State entitled "Electronic Passport." Through these comments we offer you the technical and policy expertise of leading computer scientists and engineers in the nation.

We file these comments to urge the Department of State to fully address the security and privacy implications posed by the inclusion of the 64 kilobyte contactless integrated circuit chip with antenna (hereinafter RFID) that will contain the information currently on the data page of the passport plus biometric data—at this point limited to a facial image but in the future likely to include fingerprint and iris biometrics as well. Public documents reveal that the United States resisted certain privacy and security protections against the advice of security experts and over the objections of other nations participating in the process of developing the international standards that form the basis for the Department of State's proposed rules.[1] We are

[1] ACLU, *Naked Data: How The U.S. Ignored International Concerns and Pushed for Radio Chips In Passports Without Security,* Nov. 26, 2004, *at* http://www.aclu.org/Privacy/Privacy.cfm?ID=17078&c=130.

deeply troubled by the decision to ignore the increased security risks posed by the changes in data format and retrieval methods. Ignoring both the increased and the new security risks introduced by the use of RFID in passports, the Department of State will foist needless privacy and physical security risks upon the public.

Many in our community believe that the case for using RFID in this context has not been made and are unclear as to why other technology such as 2-D barcodes and contact smartcards, which have the ability to store the necessary information while preventing unknown remote data capture, have not been selected. Given the current decision to use RFID, we believe that the introduction of any new technology must be accompanied by a serious evaluation and response to changes in risk. For that reason, we request that the Department of State address the specific risks of eavesdropping, skimming, cloning, and error rates presented by RFID and the chosen facial image biometric. These comments present an analysis of the newborn threats and the solutions to mitigate the ensuing risk. We provide our recommendations based upon current understanding in the scientific community of these risks and technical responses available to minimize their exploitation.

Our goal here is to ensure that sound science and the best available research inform the Department of State's technical security decisions in the area of electronic passports.

I. Background

With the introduction of the Enhanced Border Security and Visa Entry Reform Act (EBSA) of 2002, Congress required nations participating in the visa waiver program to issue machine-readable and tamper-resistant electronic passports based on the standard established by the International Civil Aviation Organization (ICAO).[2] The EBSA neither requires nor empowers the State Department to conform U.S. passports to the ICAO standards. This act was designed to enhance the 1986 Visa Waiver Program (VWP) which was created to decrease the long delays associated with document reviews at ports of entry, especially at airports.[3] The VWP was premised on the idea that citizens from countries with similar standards of living as the U.S. would not overstay their visas and become illegal immigrants.[4] After 9/11 it remained imperative, both politically and economically, to maintain the VWP,[5] but as the recent Madrid Bombings (perpetrated by Spanish citizens who would be eligible

[2] 8 U.S.C. §§ 1732

[3] Rep. Sensenbrenner. Judiciary Committee on Biometric Passport Deadline, April 21, 2004. 2004 WL 882916.

[4] Rep. Watt and Sec. of Homeland Security, Tom Ridge, 2004 WL 882916.

[5] *The Visa Waiver Program and the Screening of Potential Terrorists*, Before House Committee on International Relations, 108th Cong. (June 16, 2004) (Statement of Catherine Barry, Dir. Office of Visa Services) *at* wwwc.house.gov/international_relations/108/bar061604.htm; Sec. of State Powell, April 21, 2004. 2004 WL 882916. (Stating that 1 of 8 US jobs are related to the tourist industry and that travelers from VWP countries account for most of the revenue.)

to travel to the U.S. visa-free) and the failed British shoe-bomber demonstrate, eligible citizens from VWP countries are capable of committing terrorist acts.

Through the EBSA Congress seeks to keep terrorist and other security threats out of the country by establishing a rapid and reliable method, using RFID, to positively authenticate passport holders. The U.S. and 27 other countries, that are part of the VWP, are implementing these systems with the goal of improved authentication. Participants would be pre-screened through various methods (consular information, database sharing and comparing between Interpol, the FBI and other criminal databases, etc.)[6] and the identity information contained in the RFID chips embedded in their passports would be checked at ports of entry to verify the passport holder.

Under standards promulgated by the ICAO, electronic passports must embed RFID tags containing the personal data currently on the passport and a jpeg image of the passport owner to be used as a "biometric" identifier in the covers.[7]

The proposed rules for electronic passports issued by the Department of State require U.S. passports to comply with the ICAO standard. The proposed rule calls for the data on the RFID chip to be unencrypted and the chip itself to contain a unique identifying number. The proposed rules do not mandate any technical measures to prevent the unauthorized reading and cloning of the passport, although they suggest that measures to address cloning will be developed.

II. New Security Threat Analysis

The notion that the same security threat analysis applies to both data typewritten on a page, which can only be accessed by someone physically controlling the document, and to electronic data, designed to be accessed remotely, is naive. The change in data format alone creates additional security risks, in particular increased opportunities for data capture and reuse that must be addressed. An example of secondary use directly enabled by a change in data format is the shift to encoding personal information in a magnetic stripe on the back of driver licenses. Driver licenses are routinely requested to prove age in establishments that sell alcohol. However, due to the shift in data format, at least one establishment in Massachusetts took the opportunity to capture all the information contained in the magnetic stripe on the back when they examined licenses for proof of age. This data was then used for business and marketing purposes.[8] This practice is referred to as "feature creep" and amply illustrates the additional risks posed by the mere change in format of passport data.

---

[6] *The Visa Waiver Program and the Screening of Potential Terrorists*, Before House Committee on International Relations, 108th Cong. (June 16, 2004) (Statement of Robert Jackstra, Executive Director of Border Security) *at* http://wwwc.house.gov/international_relations/108/jac061604.htm.
[7] *See infra* Footnote 4, statement by Dir. Of Visa Services, Catherine Barry.
[8] "Swipe at Your Privacy," WHDH TV, June 4, 2002 *at* http://www.whdh.com/features/articles/specialreport/H37/.

A. Ease of Data Accessibility and Data Capture

The new threats that arise from the change in data storage format include skimming, eavesdropping and cloning. The proposed rules do not disclose the Department's future plans to incorporate true biometrics and it is not obvious if the Department has taken into consideration the error rates and false positives inherent in various biometrics. The Department of State's cursory review of a subset of the threats introduced by the ICAO standard fails to reckon with the significance of the changes in data format and data accessibility. While the proposed rules briefly discuss the risks, they downplay the possibility they will be exploited and offer no concrete proposal to minimize these risks.

In theory, the ICAO standard is designed to limit the read range of the RFID chip to approximately 10 cm.[9] Yet researchers have already shown that this read range can be extended to 30 feet.[10] Given the rates of identity theft, it is wise to assume that there exists a class of highly motivated individuals who will invest in technology to exploit this vulnerability. Given that U.S. citizens are a preferred target of terrorists in some parts of the world, the ability to remotely and surreptitiously identify U.S. citizens will surely aid those seeking to harm them. Incorporating RFID technology into a passport means that "anyone with a reader can learn that [identity] information, without the passport holder's knowledge or consent," observes security expert Bruce Schneier, such that "pickpockets, kidnappers, and terrorists can easily—and surreptitiously—pick Americans or nationals of other participating countries (visa waiver countries) out of a crowd."[11]

We urge the Department of State to give the required attention to these urgent security issues by fully exploring and incorporating the corresponding countermeasures into electronic passports prior to their development and issuance. It is unreasonable for the U.S. government to fail to address documented security risks with currently available countermeasures. As the driver of this new application, the U.S. government has an obligation to its citizens to conduct and fund security research to fully address risks that current technology is incapable of mitigating.

1. Skimming

Skimming occurs when the data on the passport is read without the owner's knowledge or consent. The proposed rules do not require personal data to be encrypted nor do they adopt other protective measures. As a result, the identity data contained on passports will be vulnerable to motivated individuals who purchase an off the shelf RFID reader. Armed with such a reader, a skimmer can surreptitiously learn the name, nationality, passport number and other data about the passport holder.

[9] ICAO Technical Report, *Biometric Deployment of Machine Readable Travel Documents,* May 21, 2004.
[10] Junko Yoshida, "Tests reveal e-passport security flaw," EE Times, August 30, 2004 *at* http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=45400010; Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard* Systems, Cryptology ePrint Archive, Report 2005/052, 2005.
[11] Bruce Shneier *at http://www.schneier.com/blog/archives/2004/10/rfid_passports.html.*

The proposed rules disregard the option of encrypting the data because the "personal data stored on the passports' electronic chip consists simply of the information traditionally and visibly displayed on the passport data page; encrypted data takes longer to read, increasing port of entry processing time; and in order to be globally interoperable encryption would require a higher level of technology and more complicated technical coordination with other nations."[12] However, the Department offers no supporting evidence for its rationale rejecting encryption. Although the Department of State believes that skimming is difficult it nonetheless states that it will have an anti-skimming feature in place at the time the first ICAO standard passport is issued. However, they do not specify what "anti-skimming feature" will be implemented. It is impossible for the public to provide meaningful feedback without additional information about the technology being pursued and unacceptable to postpone public feedback and the public resolution of this important issue until the time at which passports are already being issued.

2. Eavesdropping

Eavesdropping is the opportunistic interception of information on the chip while the chip is being accessed by a legitimate reader. While similar to skimming, eavesdropping may be feasible at longer distances, given that eavesdropping is a passive operation.[13] The Department of State says that "eavesdropping is difficult to achieve" and would be "obvious and detectable." This is not the whole picture. Eavesdropping may take place from a distance of 30 feet,[14] a distance that is sufficiently removed to go unnoticed by authorities. This is complicated by the fact that hand held readers available to ordinary consumers are sufficiently small to be hidden from sight in backpacks, luggage, laptop cases or purses in crowded public places, like airport terminals. It is unreasonable to assume that individuals engaged in eavesdropping will be noticed by airport officials.

The proposed rules state that the Department will work with other governments to eliminate the threat of eavesdropping by electronically shielding the reader. This is not an adequate response but rather demonstrates the limited effort on behalf of the U.S. government to understand the eavesdropping risk. It misstates the risk, which includes not only relays from authorized readers, but more importantly from the interception of data communicated between the passport and the authorized reader. The proposed rules ignore the need to shield the RFID chip itself to prevent eavesdropping.

3. Problems arising from Skimming and Eavesdropping

Skimming and eavesdropping are problematic in their own right, but could foreseeably lead to further problems such as identity theft, tracking of passport

[12] Federal register notice by Department of State, *Electronic Passport*, Feb. 18, 2005.
[13] Junko Yoshida. *Tests Reveal e-passport security flaw*, EE Times, August 2004.
[14] Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, 2005.

holders, and hotlisting. From skimming and eavesdropping, an unauthorized person may obtain the personal data of a passport holder and "steal" his/her identity. As the Association of Corporate Travel Executives President Greely Koch stated, "[t]he thought that your travel documents could be broadcasting your nationality to those with an interest in harming U.S. citizens is bad enough, but it could also be pinpointing likely targets for pickpockets, thieves, and even providing information to steal."[15] An adversary will not only have access to the passport holder's name, birth date, and social security number, but they will also have access to the digital image of the person. The adversary would then have all the information needed to commit identity theft, allowing it to open lines of credit and bank accounts, and commit other acts under the traveler's name.

The passport holder can now be tracked based on the information obtained from skimming. Using any type of personal data on the passport, from the owner's name to the unique identifying number of the passport, an adversary can track the movements of the passport holder based on the RFID device. As the Business Travel Coalition pointed out, a passport could be read by an adversary while "walking down a hotel corridor" and it would be simple to determine in which guestrooms Americans were staying. They continued on, stating that "[i]n some countries, an American passport is worth $3,000 in hard cash on the black market," so in a sense a "U.S. passport would be akin to placing a sign on one's lapel advertising a $3,000 give away." [16] Information from the passport obtained through tracking when combined with other information gathered from the passport holder's actions and aggregated over time, could open up further avenues for crimes against the passport holder, such as stalking, assault, and theft. Thus, the passport makes the owner a target for victimization.

Hotlisting is another dangerous side effect of skimming and eavesdropping. In hotlisting, an adversary builds a database and can create and match identifiers to people of interest so that later, when that identifier is seen again, the adversary knows who the person is without having to read the electronic passport again. Hotlisting permits the targeting of specific individuals potentially facilitating a range of harms.

The Department of State has mentioned they are taking "measures to prevent skimming" and "will work vigorously with other governments to encourage them to eliminate the threat of eavesdropping by requiring all chip readers to be electronically shielded." However, these counter measures to secure personal data need to be explored and explicitly stated in the proposed rules to allow for meaningful public comment. The technology to address these risks should not be an afterthought.

---

[15] ACTE, *ACTE Says Passport "Bugs" Could Put U.S. Travelers At Risk,* March 28, 2005 *at* http://www.acte.org/resources/press_release/032905.shtml.

[16] Business Travel Coalition, "*U.S. State Department Proposed Passport Program Is Bad Policy",* March 28, 2005 *at* http://btcweb.biz/rfidstatement.htm.

B. Cloning

Cloning involves creating a passport double that imitates the original, authentic, passport. While embedding a RFID chip in the passport cover will be another step that must be imitated by cloners, it provides minimal added protection against cloning given the proposed rules. The proposed rules only require a digital signature to be stored in each RFID chip to verify that the chip is authentic. However, these digital signatures do not bind the data to a particular passport or to a particular chip and offer little defense against passport cloning.

The proposed rules mandate that upon obvious tampering with the passport or the data recorded inside, the passport will not be accepted as identification. However, once an adversary has previously captured the signature and the data through skimming or eavesdropping, they can encode the data on a commercially available replacement chip. In three separate incidents during February 2004, France lost up to 20,000 un-issued passports, which remain unaccounted for.[17] Therefore, an official-looking document could easily be created by combining a stolen passport with a replacement chip. A cloned passport could be created by an adversary, undermining the limited security benefits the RFID system may offer.

Remote reading and retrieval of passport data will ease the ability of thieves, terrorists and others to acquire personal information. The security risks introduced by RFID technology must be analyzed and addressed. To do otherwise risks reducing the security of the passport system.

C. Biometric Instability

The facial recognition methodology currently proposed in the rules does not qualify as a biometric. Under the proposed rules, "border inspectors would compare the passport bearer with the digital facial image stored on the electronic chip." Yet, biometric is commonly defined as "the statistical analysis of biological observations and phenomena"[18] and more often refers to "authentication techniques that rely on measurable physical characteristics that can be automatically checked."[19] There is no statistical evaluation or quantitative analysis being done under the proposed rules; thus, it is unclear why the image of the passport holder needs to be in jpeg format and put on an RFID chip where it can be surreptitiously read. The proposed method could be performed with the image in a hard copy format on the passport as is currently the case.

[17] Fox News, *FBI warns of Stolen Passports*, *at* http://www.foxnews.com/story/0,2933,117200,00.html.
[18] Webster's Dictionary *at* http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=*biometric.*
[19] Webopedia *at* http://www.webopedia.com/TERM/B/biometrics.html.

The proposed rules hint at further plans for biometrics stating "the inclusion of facial image data in the U.S. passports is considered a first step in ensuring that an effective biometric system is incorporated into the U.S. passport system." The future use of biometrics is mentioned but again there is little evidence that the risks and benefits of biometrics overall or particular biometrics are being rigorously studied. The introduction of biometrics, while useful for security in some contexts, does not guarantee improved security. With respect to the facial biometric, its proven inaccuracies may make border crossings less efficient due to the high rate of false negatives, causing "false alarms [to] become the norm."[20] To achieve acceptable levels of accuracy, studies have shown that the images stored on the chip, including those taken abroad, must be captured under a rigid set of parameters.[21]

We urge the Department of State to thoroughly consider the privacy, security and efficiency risks and benefits presented by various biometrics *before* introducing them into the passport system.

II. Making Electronic Passports More Secure

Adopting RFID into passports presents new threats that must be addressed through technology and practice. There are some relatively simple and obvious measures that can be taken to mitigate these risks. We detail them below.

A. Encryption

The proposed rules make it clear that the Department of State will not implement Basic Access Control to protect the data on the electronic passport. Encryption is dismissed for three reasons:

- "the personal data stored on the passports electronic chip consists simply of the information traditionally and visibly displayed on the passport data page;
- encrypted data takes longer to read, increasing port of entry processing time; and,
- in order to be globally interoperable encryption would require a higher level of technology and more complicated technical coordination with other nations"[22]

We feel this reasoning is flawed and that encryption would be beneficial and could be implemented efficiently.

We have already addressed the Department's first concern and demonstrated that a change in data format incurs a different set of security threats. In response to the

[20] The Economist, *High-Tech Passports Are Not Working*, Feb. 17, 2005.
[21] Washington Post, *Passport ID Technology Has High Error Rate*, August 6, 2004. http://www.itl.nist.gov/iad/Articles/Facial-Passports.html.
[22] Federal register notice by Department of State, *Electronic Passport*, Feb. 18, 2005.

second concern, reading encrypted data will not take a significantly longer amount of time than reading the unencrypted data on the electronic passport. The passport processing rate depends on how much data is on the card and is transferred from it to the back-end system. Even with encryption, processing time at points of entry will be markedly reduced, as the processing time necessary to decrypt 64 kilobytes of data is almost immeasurably small. More importantly, the emphasis of the Department of State's effort on providing a better authentication mechanism between the passport and the holder will be furthered by encrypting passport data. Encrypting the data will make passports less susceptible to forgery, along with the digital signature currently proposed, by limiting the ability of those engaged in skimming and eavesdropping to access personal information

Finally, Active Authentication is currently mandated by the ICAO standards for electronic passports. The capabilities that make Active Authentication possible are enough to implement Basic Access Control. All the information necessary to create keys for Basic Access Controls will be present on the data page of the electronic passport under the current standards, thus no further coordination between nations is necessary. Currently, Germany and other European Union nations, are adopting the "Basic Access Control" (BAC) requirement that a plain-text key be displayed in the second line of the Machine Readable Zone (MRZ) of the passport. Only by optically scanning the opened passport can the key be read to unlock the facial image and the personal data on the RFID chip.[23] There are also other types of encryption methods, such at those proposed under ISO/IEC 18033 standard, which are internationally accepted and could be implemented by all participating nations. In the absence of encryption any ISO 14443-compliant reader can read the data on an electronic passport. Such readers are readily available to the public.

We respectfully urge the Department to State to revise its proposed rules to incorporate encryption of passport data.

B. Faraday Cage

In addition to encrypting passport data, the Department of State should require the passport cover to contain a radio frequency blocking material. This is a simple measure that will prevent unauthorized skimming of data on the passport. Aluminum fiber and other such materials are opaque to radio waves. Incorporating such materials into the passport cover, which must completely encapsulate the document, will create a Faraday cage that minimizes unauthorized remote reading of the data on the chip.

The Department of State has hinted at some sort of protection against skimming stating, "[we] will work vigorously with other governments to encourage them to

[23] Federal Office for Information Security, *The Golden Reader Tool: the Basis for Interoperable Electronic Passports,, at* http://www.bsi.bund.de/literat/faltbl/F25GRT.htm.

eliminate the threat of eavesdropping by requiring all chip readers to be electronically shielded." Yet, it is not just the reader, but the passport that also needs shielding. While a Faraday cage will not prevent eavesdropping on legitimate passport-reader communication, it will significantly reduce the likelihood that unauthorized reading of the passport is being done at non-border points where a holder will not be expecting it. This will significantly decrease the opportunity for an adversary to skim data and the problems that flow from surreptitious access to personal information.

A Faraday cage can be easily implemented and will provide added security to the data on the passport chip. We suggest that the Department of State put some sort of Faraday cage passport cover or similar blocking mechanism, such as "Blocker Tags", into the guidelines for the creation of the electronic passport. Another approach is an electronic lock on the chip, which has just been endorsed by the European Union. With this lock, the passport would then have to be swiped through a special reader in order to unlock the chip and allow data to be read.[24]

C. Biometrics Options

The proposed rules do not demonstrate a clear plan of action for evaluating the risks and costs of incorporating biometrics into the electronic passport. The proposed facial recognition system does not qualify as a biometric. We urge the Department to explore the various security and privacy risks, as well as the utility of including specific biometrics and create a plan to address them.

Facial biometric systems, even when the pictures are taken in a highly controlled environment, have an accuracy rate of only 90%.[25] The systems' performance drops dramatically if there are differences in lighting, the angle of the camera, interference from personal eyewear, and differences in facial expressions.[26] Federal researchers report that improper lighting alone can cause an error rate of up to 50%.[27] This is compounded by the fact that State Department will not require new digital photos for new or replacement passports but will digitize the original printed photos.[28] As Prof. Wayman, Director of Biometric Identification Research at San Jose State University noted "if there's a 10 percent error rate with 300 people on a 747, that's a problem."[29]

Fingerprints and iris scans perform better, yet still have some inherent error. According to tests by the National Institute for Standards and Technology, two fingerprints provide an accuracy rate of 99.6% and are not as susceptible to environmental differences.[30] However, the GAO reports that at least two percent of the general population does not have well-defined fingerprints and that certain ethnic

[24] The Economist, *High-tech passports are not working,* Feb. 17, 2005.
[25] Washington Post, *Passport ID Technology Has High Error Rate*, August 6, 2004. http://www.itl.nist.gov/iad/Articles/Facial-Passports.html.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Washington Post, *Passport ID Technology Has High Error Rate.*

and demographic groups are more difficult to fingerprint.[31] A recent review of available fingerprinting systems reveal only few commercially systems have an error rate under three percent.[32] Furthermore, no one has tried to assess the feasibility of a database containing the fingerprints of over 450 million Europeans,[33] not counting the 300 million American and 130 million Japanese fingerprints that would be required to incorporate most of the VWP countries. Issues of false negatives and statistical errors have never been explored. Iris scans are also more accurate than facial images, yet the technology is still in its infancy and will require additional experimentation before it can be fully integrated.

While all the biometrics have some amount of error involved with their use, current research indicates that fingerprints and iris scans are less prone to errors from environmental factors. The Department of State should fully consider the impact of the biometric choice on travelers who will be wrongly singled out due to error rates. Regardless of the biometric chosen, the Department should have a detailed contingency plan for when the biometrics fail, considering the security and privacy risks inherent in this sensitive data.

III. Conclusion

By incorporating security measures, including data encryption and RF blocking schemes such as Faraday cages, into rules for the implementation of the electronic passport system, the Department of State will more effectively meet the goal of added security and better authentication for passport holders. It is incumbent upon the government to adequately address the new risks posed by the remote readability of the proposed electronic passports. Considering available alternatives such as 2-D barcodes and contact smart cards, we remain unconvinced that RFID is an appropriate technology to incorporate into passports. However, given that the international community led by the U.S. is moving to adopt RFID, we urge the State Department to use available technology to protect against known and obvious threats. The security measures mentioned above are necessary, but insufficient, to address the threats to privacy and security created by the adoption of the ICAO standard.

We thank the Department of State for the opportunity to present our views. We would welcome the opportunity to speak with you about our concerns. Please feel free to contact us for additional information or clarification.

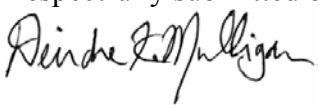
---

[31] United States General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, Nov. 2002.

[32] Fingerprint Verification Competition 2004, *Open Category Results: Average results over all databases*. *at* http://bias.csr.unibo.it/fvc2004/results.asp.

[33] European Digital Rights, *An Open Letter to the European Parliament on Biometric Registration of all EU Citizens and Residents*, *at* http://www.edri.org/campaigns/biometrics/eu.

Respectfully submitted by,



Deirdre Mulligan, Director
Marci Meingast, Clinical Intern
Esteban Mendoza, Clinical Intern
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley
School of Law (Boalt Hall)
Berkeley, CA

ON BEHALF OF:

Michael Angelo
Security Manager

Steven M. Bellovin
Prof. of Computer Science
Columbia University, NY

Josh Benaloh
Member of the Board of Directors
International Association for Cryptologic Research

Lorrie Faith Cranor
Associate Research Professor
Computer Science and Engineering & Public Policy
Carnegie Mellon University

Brian A. LaMacchia
Affiliate Faculty, Department of Computer Science & Engineering
University of Washington

Aviel Rubin
Prof. of Computer Science
Technical Director, Hopkins Information Security Institute
Founder & President, Independent Security Evaluators
John Hopkins University, MD

Bruce Schneier
Security Technologist
Founder and Chief Technology Officer of Counterpane Internet Security

Barbara Simons
Retired President of IBM Research & Ex-President of ACM
Palo Alto, California