COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to
THE FEDERAL TRADE COMMISSION

ID Workshop: Comment, P075402
Notice Announcing a Two-Day Public Workshop and
Requesting Public Comment and Participation

By notice published on February 26, 2007, the Federal Trade Commission ("FTC") requested public comment and participation in "Public Workshop: Proof Positive: New Directions for ID Authentication."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to recommend against using radio frequency identification or biometrics technology in identification documents; urge the restriction, rather than expansion of the use of Social Security numbers as identifiers; and advocate an identity metasystem in which authentication is confined to specific contexts in order to limit the scope for potential misuse.

Introduction

EPIC is a non-profit public interest research organization founded in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, free speech and constitutional values. For many years, EPIC has played a leading role on the issue of identification and authentication issues, testifying before Congress, submitting comments to federal agencies, urging the adoption of stronger privacy laws and more effective technologies that would safeguard the privacy of American consumers.[2]

---

[1] Fed. Trade Comm'n, *Notice Announcing a Two-Day Public Workshop and Requesting Public Comment and Participation*, 72 Fed. Reg. 8381 (Feb. 26, 2007) ["FTC Public Comment Notice"], *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/E7-3238.htm.

[2] In 2001, EPIC Executive Director Marc Rotenberg traced the history of the SSN as an identifier and raised privacy issues associated with the Social Security Administration's Death Master File and in 2002,

I. Radio Frequency Identification Technology Increases Vulnerability of Data

EPIC urges the Commission to reject the use of radio frequency identification ("RFID") technology in identification documents. There are significant privacy and security risks associated with the use of RFID-enabled identification cards, particularly if individuals are not able to control the disclosure of identifying information. Threats to individual privacy and security include the risks of "skimming," and "eavesdropping." The Department of State recognized these security and privacy threats and changed its E-Passport proposal because of them; the Department of Homeland Security ("DHS") has just abandoned a plan to include RFID chips in border identification documents because the pilot test was a failure; and the Department of Homeland Security's Data Privacy and Integrity Advisory Committee has recommended against the use of RFID in identification documents.

Privacy and security risks associated with RFID-enabled identification cards include "skimming" and "eavesdropping." Skimming occurs when an individual with unauthorized RFID reader gathers information from an RFID chip without the

---

EPIC testified that the problem of identity theft had grown worse, with the states acting to limit collection and disclosure of the SSN. In 2003, EPIC again testified in favor of privacy protections, highlighting recent abuses, the continuing unnecessary use of the SSN as an identifier by private and public sector entities, and the developing trends of state legislation crafted to limit collection and use of the identifier. *See also*, Marc Rotenberg, Exec. Dir., EPIC, *Testimony at a Joint Hearing on Social Security Numbers & Identity Theft, Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001), *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Chris Jay Hoofnagle, Deputy Counsel, EPIC, *Testimony at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the H. Ways & Means Subcom. on Social Security and the H. Judiciary Subcom. on Immigration, Border Security, & Claims*, 105th Cong. (Sept. 19, 2002), *available at* http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html; Chris Jay Hoofnagle, Deputy Counsel, EPIC, *Testimony at Hearing on Use and Misuse of the Social Security Number, Hearing Before the H. Ways & Means Subcom. on Social Security*, 106th Cong. (July 10, 2003), *available at* http://www.epic.org/privacy/ssn/testinomy7.10.03.html; Marc Rotenberg, Exec. Dir., EPIC, *Testimony at a Hearing on Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy, Before the H. Commerce Comm.*, 109th Cong. (May 11, 2006), *available at* http://www.epic.org/redirect/ec_ssn_epic.html.

cardholder's knowledge. Eavesdropping occurs when an unauthorized individual intercepts data as it is read by an authorized RFID reader. The Government Accountability Office has said that, "without effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users."[3]

In the absence of effective security techniques, RFID tags are remotely and secretly readable. Although the creation of a small, easily portable RFID reader may be complex and expensive now, it will be easier as time passes. For example, the distance necessary to read RFID tags was initially thought to be a few inches. In the now-abandoned pilot test, the Department of Homeland Security said, "reliable reads can be received from a few inches to as much as 30 feet away from the reader."[4] Other tests also have shown that RFID tags can be read from 70 feet or more, posing a significant risk of unauthorized access.[5]

Some attacks already have succeeded against so-called "strengthened" identification documents. In one case, a computer expert was able to clone the United Kingdom's electronic passport by using a commercially available RFID reader (which

[3] Gregory C. Wilshusen, Dir. of Info. Sec. Issues, Gov't Accountability Office, *Testimony at a Hearing on Ensuring the Security of America's Borders through the Use of Biometric Passports and Other Identity Documents Before the Subcom. on Economic Sec., Infrastructure Protection, and Cybersecurity of the H. Comm. on Homeland Sec.*, 108th Cong. 8 (June 22, 2005), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-05-849T (last visited Mar. 21, 2007).
[4] Dep't of Homeland Sec., *Notice with request for comments*, 70 Fed. Reg. 44934, 44395 (Aug. 5, 2005), *available at* http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve (last visited Mar. 21, 2007).
[5] *See* Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems* (Feb. 22, 2005), *available at* http://eprint.iacr.org/2005/052 (last visited Mar. 21, 2007); Scott Bradner, *An RFID warning shot*, Network World, Feb. 7, 2005.

cost less than $350) and software that took him less than a couple of days to write.[6] In assessing the new RFID-enabled U.S. passports, one expert cloned the RFID tag and another used characteristics of the radio transmissions to identify individual chips, and, as security expert Bruce Schneier has pointed out, the researchers spent only a few weeks attacking the RFID-enabled passport.[7] The aforementioned security and privacy threats are important reasons why RFID technology should not be used in identification cards.

Another security risk of RFID-enabled identification cards is that of clandestine tracking. An unauthorized RFID reader could be constructed to mimic the authorized signal and then be used to secretly read the RFID tag embedded in the identification card. The Government Accountability Office has highlighted this security problem unique to wireless technology:

> The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated.[8]

So long as the RFID tag or chip can be read by unauthorized individuals, the person carrying that tag can be distinguished from any other person carrying a different tag.

This approach is contrary to the recommendation of the International Civil Aviation Organization ("ICAO"). ICAO had earlier proposed that strong security features be implemented in all machine-readable travel documents.[9] Specifically, ICAO

---

[6] Steve Boggan, *Special Report: Identity Cards: Cracked It!*, Guardian, Nov. 17, 2006.
[7] Bruce Schneier, Opinion, *The ID Chip You Don't Want in Your Passport*, Wash. Post, Sept. 16, 2006.
[8] Gov't Accountability Office, *Report to Congressional Requesters: Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (May 2005), *available at* http://www.gao.gov/new.items/d05551.pdf (last visited Mar. 21, 2007).
[9] ICAO, Machine Readable Travel Documents, *Technical Report: PKI for Machine Readable Travel Documents Offering ICC Read-Only Access*, version 1.1 (Oct. 1, 2004), *available at*

recommends incorporation of Basic Access Control in identification documents. ICAO explains, "[a] chip that is protected by the Basic Access Control mechanism denies access to it's [sic] contents unless the inspection system can prove that it is authorized to access the chip."[10]

The authorization needed could be a secret key or password used to unlock the data. To obtain the key, the border officer would need to physically scan the machine-readable text that is printed on the RFID-enabled PASS card. The RFID tag reader would then hash the data to create a unique key that could be used to authenticate the reader and unlock the data on the RFID chip. Basic Access Control prevents skimming by preventing remote readers from accessing the data on the document. The data cannot be read unless the document is physically opened and scanned through a reader. Basic Access Control also prevents eavesdropping by encrypting the communication channel that opens when data is sent from the chip to the RFID reader. The Basic Access Control solution does not, however, solve all security and privacy concerns, but the principle of Basic Access Control is critical to the design of identification systems. Individuals, unlike commercial products with RFID tags, should have the right to control the disclosure of their identifying information.

The Department of State ("DOS") should be fully aware by now of the problems raised by an insecure RFID scheme. In April 2005, EPIC, the Electronic Frontier Foundation, and other groups submitted comments urging the State Department to abandon its E-Passport proposal, because it would have made personal data contained in

---

http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf (last visited Mar. 21, 2007).

[10] *Id*. at 16.

hi-tech passports vulnerable to unauthorized access.[11] After DOS received more than 2,400 comments on its notice for proposed rulemaking on RFID-enabled passports, many of which criticized its serious disregard of security and privacy safeguards, the agency said it would implement Basic Access Control in an attempt to prevent skimming and eavesdropping.[12] The use of RFID-enabled identification documents, without including Basic Access Control and other safeguards, contravenes the Department of State's incorporation of basic security features into new U.S. passports.[13]

In 2005, DHS began testing RFID-enabled I-94 forms in its United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program to track the entry and exit of visitors.[14] The RFID-enabled forms stored a unique identification number, which is linked to data files containing foreign visitor's biographic information, including name, date of birth, country of citizenship, passport number and country of issuance, complete U.S. destination address, and digital fingerscans.[15] EPIC warned that this flawed proposal would endanger personal privacy and security, citing the plan's lack of basic privacy and security safeguards. In October 2005 comments to the Department of Homeland Security, EPIC explained that use of the wireless technology meant that anytime a person carried

---

[11] EPIC, EFF, et. al, *Comments on RIN 1400-AB93: Electronic Passport* (Apr. 4, 2005), *available at* http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf.
[12] Dep't of State, *Notice of Proposed Rule,* 70 Fed. Reg. 8305 (Feb. 18, 2005), *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm (last visited Mar. 21, 2007).
[13] *See* Kim Zetter, *Feds Rethinking RFID Passport*, Wired, Apr. 26, 2005; Eric Lipton, *Bowing to Critics, U.S. to Alter Design of Electronic Passports*, N.Y. Times, Apr. 27, 2005.
[14] Dep't of Homeland Sec., *Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry*, 70 Fed. Reg. 44934 (Aug. 5, 2005), *available a*t http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve (last visited Mar. 21, 2007).
[15] Dep't of Homeland Sec., *Notice of Availability of Privacy Impact Assessment*, 70 Fed. Reg. 39300, 39305 (July 7, 2005), *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-13371.htm (last visited Mar. 21, 2007).

his I-94 RFID-enabled form, unauthorized individuals could access his unique identification number, and thus the biographic information linked to that number.[16]

The Department of Homeland Security's Inspector General echoed EPIC's warnings in a July 2006 report. The Inspector General found "security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data" associated with people who carried the RFID-enabled I-94 forms.[17] A report released by the Government Accountability Office in late January identified numerous performance and reliability issues in the 15-month test.[18] The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony on February 9th that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security.[19]

In December, the Department of Homeland Security Data Privacy and Integrity Advisory Committee adopted a report, "The Use of RFID for Identity Verification," which included recommendations concerning the use of RFID in identification documents.[20] The committee outlined security and privacy threats associated with RFID

---

[16] EPIC, *Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf.

[17] Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006), *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_06-53_Jul06.pdf (last visited Mar. 7, 2007).

[18] Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Terrorism, Tech., & Homeland Sec., S. Comm. on the Judiciary*, 110th Cong. (Jan. 31, 2007), *available at* http://www.gao.gov/new.items/d07378t.pdf (last visited Mar. 21, 2007).

[19] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal Year 2008 Dep't of Homeland Sec. Budget Before the H. Comm. on Homeland Sec.*, 110th Cong. (Feb. 9, 2007), *available at* http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.

[20] Dep't of Homeland Sec., Data Privacy & Integrity Advisory Comm., *The Use of RFID for Human Identity Verification (Report No. 2006-02)* (Dec. 6, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf (last visited Mar. 21, 2007).

similar to the ones discussed below, and it urged against using RFID technology unless the technology is the "least intrusive means to achieving departmental objectives."[21]

II. Use of Biometrics Will Not Strengthen Identification Procedures

Universal identifiers, such as biometrics, will not solve the fundamental problem of how much damage an identity thief can do once a victim's identifiers are compromised.[22] Biometric authentication involves comparing the previously captured physical characteristics of a consumer with newly provided samples of that same characteristic.[23] In Congressional testimony in July 2002, EPIC explained the unique problems that are associated with biometrics technology, which are still important today.[24] First, the uniqueness of biometric data is affected by time, variability and data collection. This leads to the second problem: the technologies available are subject to varying degrees of error, which means that there is an element of uncertainty in any match. Third, there are several ways to circumvent a biometrics system.

Biometric data is affected during collection by many factors including time, variability and data. Changes in the environment, such as positioning, lighting, shadows

---

[21] *Id*. at 2.
[22] Universal identifiers have also generated significant criticism on grounds of human rights. *See, e.g.* Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U.J. SCI. & TECH. L. 37, 48 (2002). *See also* Nat'l Research Council, IDS – NOT THAT EASY: QUESTIONS ABOUT NATIONWIDE IDENTITY SYSTEMS (Stephen Kent & Lynette Millett eds. 2002), *available at* http://www.nap.edu/catalog/10346.html?opi_newdoc041102 (last visited Mar. 21, 2007).
[23] EPIC & PRIVACY INT'L, PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 49 (EPIC ed., 2006).
[24] Marc Rotenberg, Exec. Dir., EPIC, and Carla Meninsky, IPIOP Fellow, EPIC, *Statement at a Joint Hearing on Identity Theft Involving Elderly Victims Before the S. Special Comm. on Aging*, 105th Cong. (July 18, 2002) ["EPIC 2002 Statement"], *available at* http://www.epic.org/privacy/biometrics/testimony_071802.html.

and background noise can affect data collection.[25] However, an individual's biometrics are also susceptible to change through aging, injury and disease.[26]

As EPIC Executive Director Marc Rotenberg explained in July 2002, there is an element of uncertainty in any biometric match:

> The accuracy of biometric systems is measured by their *false acceptance* and *false rejection* rates. A false acceptance is when the wrong individual is matched to a stored biometric. A false rejection is when an individual is not recognized who should have been. The two measures are dependent. In reducing false acceptances, the false rejection rate will increase. Reducing false rejections will cause the false acceptance rate to go up. Most biometric systems adjust false acceptances or false rejections to the type of application and the amount of security required. High security areas, such as bank vaults and military installations are protected by biometric systems that minimize fraudulent acceptances. The false acceptance rate must be low enough to prevent imposters, but as a result, people who rightfully should be accepted, are often refused.[27]

Executive Director Rotenberg also explained that there are several ways to compromise the effectiveness of a biometric system. Biometric systems can be circumvented by false identification at enrollment, physical alteration of a personal biometric, skewing the sample collection by not cooperating, and hacking into or falsifying the database. The effectiveness of system of biometric identification will be determined by how the system is set up, protected and maintained.[28]

It is also important to recognize that the creation of a database linked to an individual and containing sensitive information creates privacy issues and would be a tempting target for identity thieves. Information in the database could be altered by administrators of the database or by those who gain unlawful access to the information.

---

[25] Cynthia Traeger and Howard Falk, *Biometric Technologies Tutorial*, Faulkner Information Services (Feb. 2002).
[26] *Id*.
[27] EPIC 2002 Statement, *supra* note 24.
[28] *Id*.

In fact, if a biometric system were properly designed to safeguard privacy rights, it would enable the data subject to have easy access to all records concerning the individual. In other words, if the agency is able to accurately identify an individual with a biometric identifier, the agency should have the necessary assurance that it can provide to that individual whatever information he or she may be entitled to under the Privacy Act.

EPIC has previously warned that biometric identification will create new, more severe identity theft problems.[29] Among other considerations, biometric identifiers have elaborate enrollment requirements that create new vulnerabilities when, for example, authenticating documents are collected. Biometrics are also difficult to reissue when they are compromised.[30] Once a biometric identifier has been compromised, there can be severe consequences for the individual whose identity has been affected. It is possible to replace a credit card or Social Security numbers, but how does one replace a fingerprint, voiceprint, or retina scan? It would be difficult to remedy identity fraud when a thief has identification with a security-cleared federal employee name on it, but the thief's biometric identifier. Or, in a more innocuous scenario, the identities of employees with different security clearances and their biometric identifiers are mismatched in their files due to human or computer error. Allowing employees access to their records would help ensure the accuracy of the information collected and used.

Government agencies have also urged caution in the use of biometric identifiers.[31] While biometric technologies may improve the reliability of authentication when

---

[29] EPIC, *Comments In the Matter of FACT Act Biometric Study File No. Before the Dep't of the Treasury* (Apr. 1, 2004), *available at* http://www.epic.org/privacy/biometrics/factabiometrics.html.
[30] EPIC, *Comments on Docket No. TSA-2005-20485* 8 (Mar. 17, 2005), *available at* http://www.epic.org/privacy/biometrics/tsa_comments31705.html.
[31] *See, e.g.,* Keith A. Rhodes, Gen. Accounting Office, *Testimony on the Challenges in Using Biometrics before the Subcom. on Tech., Info. Policy, Intergovernmental Relations, and the Census of the H. Comm.*

compared with alphanumeric alternatives, universal identifiers increase the potential for misuse once biometric data has been illegitimately obtained.[32] For example, a fingerprint can be used as a universal identifier to authenticate a consumer. While a fingerprint may be more difficult for thieves to obtain than a traditional password, it remains vulnerable to anyone with sufficient motivation and expertise.[33] A stolen fingerprint would prove enormously valuable to an identity thief should it become a widely adopted authentication method. Increasing the value of identifiers inevitably attracts professional, international criminals.[34] Moreover, a biometric identifier cannot be changed by a victim once his or her identity has been breached – a fingerprint is unalterable. Any move toward universal identifiers, while potentially deterring amateur thieves, increases the potential for misuse once determined criminals steal that data.

III. Use of Social Security Number As Universal Identifier Will Harm Identification and Authentication Security

Social Security numbers ("SSNs") have become a classic example of "mission creep," where a program designed for a specific, limited purpose has been transformed for additional, unintended purposes, some times with disastrous results. The pervasiveness of the SSN and its use to both identify and authenticate individuals threatens privacy and financial security. EPIC urges against the use of the SSN as a universal identifier, because such use would harm, rather than help, security efforts.

---

on Gov't Reform, 106th Cong. (Sept. 9, 2003), *available at* http://www.gao.gov/new.items/d031137t.pdf (last visited Mar. 21, 2007).

[32] Simon Davies, *The ID Card is the Fraudster's Friend*, Sunday Tel., July 7, 2002; *see also*, OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (Westview 1993).

[33] Robert Lemos, *This hacker's got the gummy touch*, Cnet News.com, May 16, 2002, http://news.com.com/2100-1001-915580.html (last visited Mar. 21, 2007).

[34] Kim Cameron, *The Laws of Identity*, Identity Weblog, Dec. 9, 2004, http://www.identityblog.com/stories/2004/12/09/thelaws.html.

In testimony last year, EPIC Executive Director Marc Rotenberg explained that the SSN "was created in 1936 for the purpose of administering the Social Security laws. SSNs were intended solely to track workers' contributions to the social security fund."[35] Rotenberg said that, "[p]ublic concern over the potential abuse of the SSN was so high that the first regulation issued by the new Social Security Board declared that the SSN was for the exclusive use of the Social Security system."[36] Over time, legislation has broadened the uses of the SSN. However, it is important to note that the SSN and its basic card still are not intended to be used for authentication and identification purposes, and yet far too many entities rely upon it for just those purposes.

The uses of a universal identifier are not limited to government uses, Executive Director Rotenberg explained. "In fact, it is commercial enterprises that have made the SSN synonymous with an individual's identity. Despite the fact that the cards were never intended to be used for identification purposes, they are considered the 'keys to the kingdom' for records about individual consumers."[37] For example, the financial services sector has created a system of files containing personal and financial data on nearly 90 percent of the American adult population and keyed these files to individuals' SSNs. This information is sold and traded freely, with virtually no legal limitations.

This widespread use, combined with lax verification procedures and aggressive credit marketing has lead to widespread identity theft. "The root of this problem is that the SSN is used not only to tell the credit issuer who the applicant is, but also to verify the applicant's identity. This would be like using the exact same series of characters as

---

[35] Marc Rotenberg, Exec. Dir., EPIC, *Statement at a Hearing on Social Security Number High-Risk Issues Before the Subcom. on Social Sec. of the H. Comm. on Ways & Means*, 109th Cong. 2 (Mar. 16, 2006), *available at* http://www.epic.org/privacy/ssn/mar_16test.pdf.
[36] *Id*.
[37] *Id*. at 3.

both the username and password on an email account. The fact that this practice provides little security should not be a surprise," Rotenberg said.[38] EPIC urges the FTC to reject further expansion of the use of the SSN as an identification or authentication devise and recommends the FTC try to curtail the use of SSNs as identifiers.

IV. A Centralized Identification System Increases the Risk of Identity Theft

EPIC and others have explained that it decreases security to have a centralized system of identification, one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.[39] Using a national ID card would be as if you used one key to open your house, your car, your safe deposit box, your office, and more.[40] "The problem is that security doesn't come through identification; security comes through measures – airport screening, walls and door locks – that work without relying on identification"; therefore, a centralized system of identification would not increase national security, security expert Bruce Schneier has said.[41] A large data breach affects the confidence and trust of consumers. People will recoil from systems that create privacy and security risks for their personal data.

We have seen countless data breaches that have left the personal data of millions of Americans vulnerable to misuse. In February 2005, databroker Choicepoint sold the

---

[38] *Id*. at 4.

[39] Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, *Prepared Testimony and Statement for the Record at a Hearing on "Maryland Senate Joint Resolution 5" Before the Judicial Proceedings Comm. of the Maryland Senate* (Feb. 15, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_021507.pdf.

[40] Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, *Prepared Testimony and Statement for the Record at a Meeting on "REAL ID Rulemaking" Before the Data Privacy & Integrity Advisory Comm., Dep't of Homeland Sec.* (Mar. 21, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf

[41] Press Release, EPIC, After Long Delay, Homeland Security Department Issues Regulations For Flawed National ID Plan (Mar. 2, 2007), *available at* http://www.epic.org/press/030207.html.

records of at least 145,000 Americans to a criminal ring engaged in identity theft.[42] Also that year, Bank of America misplaced back-up tapes containing detailed financial information on 1.2 million employees in the federal government, including many members of Congress.[43] Last May, an information security breach by a Veterans Affairs employee resulted in the theft from his Maryland home of unencrypted data affecting 26.5 million veterans, active-duty personnel, and their family members.[44] The laptop and an external hard drive contained unencrypted information that included millions of Social Security numbers, disability ratings and other personal information.[45]

A centralized identification system would be a tempting target for identity thieves. If a criminal breaks the system's security, then the criminal would have access to the personal information of every single person in that database. If this one, centralized system is used across the nation, this would put hundreds of millions of people at risk for identity theft.

There is another significant security risk, besides that of attacks by unauthorized users, and that is of authorized users abusing their power. A 2005 scandal in Florida highlights risks associated with large database systems. A woman wrote to a newspaper criticizing a Florida sheriff as being too fat for police work and condemning his agency's use of stun guns.[46] Orange County Sheriff Kevin Beary ordered staffers to use state driver's license records to find the home address of his critic.[47] The sheriff sent her a

[42] Robert O'Harrow Jr., *ID Theft Scam Hits D.C. Area Residents*, Wash. Post, Feb. 21, 2005, at A01; *see* EPIC's Page on ChoicePoint, http://www.epic.org/privacy/choicepoint/.
[43] Robert Lemos, *Bank of America loses a million customer records*, CNet News.com, Feb. 25, 2005.
[44] *See* EPIC's Page on the Veterans Affairs Data Theft, http://www.epic.org/privacy/vatheft/.
[45] Statement, Dep't of Veterans Affairs, A Statement from the Department of Veterans Affairs (May 22, 2006).
[46] *Called fat, sheriff tracks down reader*, Associated Press, Apr. 6, 2005.
[47] *Id*.

letter at her home address, and she reported being surprised that he was able to track her down so easily.[48] In a case in Maryland just last year, three people – including a Maryland Motor Vehicle Administration official – were indicted on charges of "conspiring to sell unlawfully produced MVA-issued Maryland identification cards."[49]

The consumer harm that results from the wrongful disclosure of personal information is very clear. For the seventh year in a row, identity theft is the No. 1 concern of U.S. consumers, according to the Federal Trade Commission's annual report.[50] Over 104 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to a report from the Privacy Rights Clearinghouse.[51] A centralized system of identification creates a "one-stop shop" for identity thieves. Centralizing authority over personal identity into one database and one card increases both the risk of identity theft as well as the scope of harm when it occurs. The confidence and trust of consumers will fall when such a breach occurs; people will withdraw because of privacy and security questions.

V. EPIC Recommendations for Better Security Practices

Once consumer data has fallen into the hands of an identity thief, the potential for its misuse is proportionate to the extent that the information can be used for illegitimate authentication. We have already explained why a universal identifier will not improve security. Rather than promoting the use of universal identifiers, EPIC advocates the distribution of identity or an identity metasystem in which authentication is confined to

---

[48] *Id*.
[49] *Fake ID Cards*, Wash. Post, Mar. 15, 2006, at B02.
[50] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf (last visited Mar. 21, 2007).
[51] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Mar. 21, 2007).

specific contexts in order to limit the scope for potential misuse. The danger of a single identifier is that the harm will be magnified when it is compromised.

A system of distributed identification reduces the risks associated with security breaches and the misuse of personal information. For example, a banking PIN number, in conjunction with a bank card, provides a better authentication system because it is not coupled with a single, immutable consumer identity. If a bank card and PIN combination is compromised, a new bank card and PIN number can be issued and the old combination cancelled, limiting the damage done by the compromised data. Drawbacks of such structures, including the possibility for the existence of multiple cards, are currently being addressed by the creation of an identity metasystem in which multiple identities can be loosely coupled within a single secure system.[52]

Distributing identity in this way allows for different profiles to be used in different authenticating contexts. New profiles can be created as required within a single identity metasystem. Misuse is therefore limited to the context of the information breached, whether it is a single bank account, online merchant, or medical records.

Possibilities for data misuse can also be limited at the data collection stage. EPIC has previously called attention to the need for Web sites to stop storing customer credit card information.[53] Amassing large databases of credit card numbers creates an attractive target for potential identity thieves. One simple response to identity theft is to require a PIN to be used in conjunction with all credit cards. An identity metasystem would further reduce the value of such aggregated database targets, because authenticators would be separate and distinct from all personally identifiable information.

---

[52] Kim Cameron, *supra* note 25.
[53] *See* EPIC's Page on Identity Theft: Causes and Solutions, http://www.epic.org/privacy/idtheft/.

Finally, technological measures can be used to improve the reliability of authentication while respecting consumer privacy. International research efforts are currently underway to create authentication systems that preserve anonymity, and include the development of new privacy enhancing technologies for use in such schemes.[54] These privacy enhancing technologies allow for the separation of authentication and identification and are being deployed in response to security vulnerabilities. Such technologies may plug in to identity metasystems, such as Microsoft's CardSpace. While the default settings of CardSpace do not currently meet recognized standards for privacy preservation,[55] this model should be studied in detail during the Commission's workshops on authenticating technologies.[56]

Conclusion

For the above reasons, EPIC strongly advises the Federal Trade Commission to reject the use of RFID technology or centralized systems in identification and authentication programs. We urge the FTC to restrict the use of the Social Security number as an identifier, and to reject the use of the SSN, biometrics or anything else as a universal identifier or authentication system. Instead, we recommend the distribution of

---

[54] *See, e.g.*, Carlisle Adams, *Delegation and Proxy Services in Digital Credential Environments*, Presented at the 7th Annual Privacy and Security Workshop, *Your Identity Please: Identity Theft and Identity Management in the 21st Century* (Nov. 2, 2006), *available at* http://www.idtrail.org/files/cacrwkshpdigcred02nov06.pdf; Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004), *available at* http://www.idtrail.org/files/cross_domain_identity.pdf; David Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Presented at ITL Seminar Series*, Secret-Ballot Receipts: True Voter-Verifiable Elections*, Nat'l Inst. of Standards & Tech. (May 19, 2004); Paul Van Oorschot and S. Stubblebine, *Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling*, Fin. Cryptography & Data Sec. (2005), *available at* http://www.scs.carleton.ca/~paulv/papers/pvoss6-1.pdf (all last visited Mar. 21, 2007).

[55] Stefan Brands, *User centric identity: boon or worst nightmare to privacy?*, Identity Corner, Nov. 17, 2006, http://www.idcorner.org/?p=142.

[56] *See generally*, NAT'L RESEARCH COUNCIL, WHO GOES THERE? AUTHENTICATION THROUGH THE LENS OF PRIVACY (Nat'l Academies 2003).

identity or an identity metasystem in which authentication is confined to specific contexts in order to limit the scope for potential misuse.

Respectfully submitted,

_____
Marc Rotenberg
Executive Director

_____
Melissa Ngo
Director, Identification and
Surveillance Project

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140