

## The Debate Over a National Identification Card



Nothing written here is to be construed as necessarily reflecting the views of The Century Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

### THE HOMELAND SECURITY RATIONALE FOR A NATIONAL IDENTIFICATION CARD SYSTEM

Because some of the terrorists who carried out the September 11 attacks were known to be security risks or had visa violations and still were able to spend months undetected in the United States while traveling, attending flight schools, and renting apartments, proposals for creating a national identification card system have gained new attention.

Clearly, the nation's current system of documentation failed to impede the September 11 terrorists. Two of the hijackers were on a government watch list of suspects, two had overstayed their visas, and another violated the terms of his student visa by not showing up for classes, yet they were able to operate freely while in the United States. All of the nineteen hijackers had Social Security numbers, and thirteen of the terrorists obtained their cards legally. All obtained tourist or business visas in U.S. consulates. Most of them opened bank accounts and regularly used ATM cards. Two enrolled in flight schools and took flying lessons. Many flew all over the country on commercial airlines, often first class, and some of them flew several times in and out of the United States. One of the hijackers came in and out of the country seven times between 2000 and early 2001, and another came and left five times. Many of them were able to obtain drivers licenses and rent cars. On September 9, 2001—two days before helping to fly a plane into the World Trade Center—one of the group's leaders was stopped for speeding on I-95 in Maryland; the state trooper checked his records, found that his Virginia driver's license and rental car registration were valid, issued him a ticket, and released him.

Many believe that a national identification card could have helped prevent this national tragedy. As generally proposed, in addition to containing the usual information, such as name and address of the carrier, each card also would have a computer chip embedded in it that would contain a "unique identifier," such as a fingerprint or retinal image, that could be matched with the scanned fingerprint or retinal image of the person presenting the card to confirm his or her identity. The scanning system also would retrieve information about the cardholder from databases of government law enforcement and immigration agencies. The system would notify the operator if the cardholder turned out to be on any government "watch list."

The proposals vary as to whether everyone in the country would be required to possess and carry a card, whether the system would be voluntary but available to everyone, or whether it would be required only for noncitizens and thus integrated into the visa system. It also is unclear at this time when and where the card would be utilized. Some proposals call for its use only at airports, while others envision its use in a host of government and commercial transactions, such as when making purchases or in interactions with government offices.

## THE DEBATE

The debate over the merits of a national identification card system centers on four issues: (1) its potential effectiveness in deterring and apprehending terrorists, (2) the extent to which it would impinge on privacy rights, (3) whether it would be abused by law enforcement officials, and (4) the financial costs associated with implementing such an ambitious program.

### Effectiveness

National identification card advocates argue that it could help deter terrorists while catching plotters before they do harm. Those advocates argue, for example, that the September 11 terrorists who were violating immigration laws might have been caught when they tried to board a flight or made a credit card purchase. A national identification card also might have made it more difficult for the terrorists to use false identities to obtain Social Security numbers and Virginia driver's licenses.

Opponents of the national identification card respond that such a card would not help to catch would-be terrorists. They argue that an identification card that confirms identity and history may not be effective in anticipating intent to commit a terrorist act. Many of the September 11 terrorists were not on government "watch lists" or wanted for the kinds of violations that a national identification system might catch, and thus would not have been stopped.

The net result may be that an identification card system has the *potential* to catch would-be terrorists, but would not stop or catch *all* would-be terrorists. So it is certainly no complete panacea to the problem. It is unclear how many of the September 11 attackers would have been apprehended before carrying out their plans, but some might have been.

Opponents also argue that identification technology currently is not reliable. According to Professor David J. Farber, a technology expert at the University of Pennsylvania, reading of fingerprints through hand scans fails frequently.<sup>1</sup> Records obtained by the American Civil Liberties Union indicate that facial recognition technology used on the streets in Tampa, Florida, never identified a singled individual in the police department's database, and made many false matches that were obviously wrong to the naked eye. The INS experimented with facial recognition technology at the Mexican border and abandoned it after they found it to be ineffective. Studies by the National Institute of Standards and Technology and the Defense Department have also found low levels of effectiveness.<sup>2</sup>

Supporters point out that identification technology is being used effectively by private industry as well as in other countries, such as Israel. According to testimony of former State Senator Roy Goodman, chair of a special New York task force on improving security, when Israelis arrive at an airport, they go to a kiosk, insert their identification card and are subject to hand scan, facial recognition, and iris identification.<sup>3</sup> Indeed, the last time an El Al plane was hijacked was in 1968, and terrorists have never successfully targeted any of Ben Gurion Airport's planes.<sup>4</sup>

It seems likely that while none of the technologies is foolproof, some are clearly better than others and if this system is created, a tremendous amount of analysis will have to be done to determine what works best at any given time and state of technology. Moreover, certainly as the field of biometrics becomes now more profitable and expands, more resources will go into improving the systems. Any system that might be created will have to take into account the potential for advances in the future.

---

<sup>1</sup> Lorraine Woellert, "National Ids Won't Work," *Business Week*, November 5, 2000, p. 90.

<sup>2</sup> "Drawing a Blank: Tampa Police Records Reveal Poor Performance of Face-Recognition Technology," ACLU Press Release, January 3, 2002.

<sup>3</sup> Testimony of Honorable Roy M. Goodman, Chairman, Investigations Committee, New York State Senate, Hearing of the Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee of the House Government Reform Committee, November 16, 2001.

<sup>4</sup> Paul Marks, "Face Facts: Biometrics Is Future of Security; Digital Body-Part Scans Seen as More Reliable Ids," *Hartford Courant*, February 7, 2002, p. A1.

A potential hindrance to the effectiveness of a national identification card system relates to the reliability of government databases. First, there is little coordination among those databases. For example, the INS alone has several databases, many of which do not communicate with each other. Furthermore, the FBI and the CIA do not have the capacity to alert the database system used for visa applicants because their systems are not connected to the State Department's Bureau of Consular Affairs. Also, the INS database of immigrants with criminal and deportation histories is not linked to the FBI's files.

Moreover, each of the government's databases has been shown to be prone to error and breakdown. For example, a 1999 study by the Department of Justice found that, after checking tens of thousands of civil service job applicants against the FBI database, the system erroneously assigned a criminal history to 5.5 percent of those with no criminal history.<sup>5</sup> This type of problem is not unique to the United States: in the United Kingdom, the police national computer is said to have error in between 20 percent and 30 percent of its entries.<sup>6</sup>

Simon Davies, director of Privacy International,<sup>7</sup> adds that scores of private and government databases have been breached by hackers, and some publicized the data or used it in fraud schemes. In 1999, hackers penetrated the U.S. military's computer systems—what the Defense Department's second in command called the “most organized and systematic” attack ever.

The resolution of the technical efficacy question may come down to dollars. Any system created not only would need to use the technology with the highest level of security available, but would also require the spending of resources and energy on integrating the various databases, a task that is likely to cost a great deal of money and take a good deal of time.

## Privacy Concerns

Opponents of a national identification card system believe that it would enable the government, and potentially private companies and individuals, to collect and disseminate personal information. Even if the government did not voluntarily distribute the information associated with the card, government employees would have access to that information and might deliberately or accidentally release it or abuse it. For example, a *Detroit Free Press* investigation revealed that ninety Michigan police officers, dispatchers, federal agents, and security guards abused the police database over the past five years to stalk women, threaten motorists, and settle scores.<sup>8</sup> The town manager of Newport, Delaware, just recently was charged with giving gamblers access to the confidential police database so they could protect themselves from investigators and find people who owed them money.<sup>9</sup> According to the ACLU, in October 2001, a University of Montana employee accidentally posted the psychological records of sixty-two children on the Internet.<sup>10</sup> As a recent report of the General Accounting Office regarding the accessibility of proprietary government information pointed out:

---

<sup>5</sup> Margie Wylie, “Database Flaws Could Hamper Any National ID System, Experts Warn,” *Newhouse News Services*, 2001.

<sup>6</sup> Alan Travis, “Un-British or Vital? The ID Debate,” *Guardian*, September 25, 2001.

<sup>7</sup> Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns throughout the world on issues such as wiretapping and national security activities, to ID cards, video surveillance, data matching, police information systems, and medical privacy. Privacy International has received funding and support from a range of Foundations, academic establishments, and nongovernment organizations. The organization is also minimally financed through membership fees and newsletter subscriptions. Privacy International is administered through the Electronic Privacy Information Center in Washington, D.C.

<sup>8</sup> M. L. Elrick, “Cops Tap Database to Harass, Intimidate: Misuse Among Police Frequent, Say Some, but Punishments Rare,” *Detroit Free Press*, July 31, 2001.

<sup>9</sup> “Feds Accuse Newport Manager of Misusing Criminal Database,” *Associated Press*, December 6, 2001.

<sup>10</sup> Testimony of ACLU Legislative Counsel Katie Corrigan for the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Reform on the Establishment of a National ID Card System, November 16, 2001.

Evaluations of computer security published since July 1999 continue to show that federal computer security is plagued by weaknesses that put critical operations and assets at risk. Significant weaknesses were identified in each of the 24 agencies covered by this review. These weaknesses place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections. Weaknesses at the Department of Defense increase the vulnerability of various military operations that support its war-fighting capability. Information security weaknesses place confidential data at risk of inappropriate disclosure, such as the case of a Social Security Administration employee who pled guilty to unauthorized access of the administration's systems. The related investigation determined that the employee had made unauthorized queries, including obtaining earnings information for members of the local business community. Weaknesses cover the full range of computer security controls.<sup>11</sup>

Even in the absence of inadvertent or illegal leakage of private information, the precedent of misuse of Social Security numbers demonstrates the potential for national identification cards to be used in ways that extend beyond their original purpose. Social Security numbers originally were created to track the earnings of workers so that their taxes and benefit payments could be properly calculated. Now, however, Social Security numbers are used ubiquitously in private transactions of all kinds. The Internet has enabled private companies, investigators, and anyone else who exerts a modicum of effort to find any individual's Social Security number and then use it to access abundant personal information about that individual. Although the 1974 Privacy Act protects the use of personal information by the government, it places no restrictions on private companies or individuals. The relative ease of access to Social Security numbers contributes to credit card fraud and identity theft.

The Social Security precedent makes opponents of national identification cards worry that the reach of such a system might quickly evolve beyond stopping terrorism. Government agencies, employers, banks, insurance, health care companies, and other consumer businesses might want more information to be added to the cards for various purposes. One oft-repeated concern is that health care information might become traceable through the card in order to help medical professionals respond to a terrorist attack, thereby enabling also insurance companies to use that information in determining whether to cover an individual or how to price a policy.

Supporters of a national identification card system respond that such privacy issues exist anyway and would not be exacerbated by a new system. Private industry and government already gather so much personal information that they would not learn much more than they already do. For example, we already require presentation of driver's licenses or other forms of identification to cash checks, get a post office box, board an airplane, buy alcohol, register to vote in some states, enroll in college and drive.

Moreover, supporters argue that protections could be put in place that would help secure privacy. One way of determining how this could best be done is to look at what other countries do. European countries arguably have stronger privacy protections than the United States, and the European Commission enacted the Data Protection Directive, restricting how information can be processed and used, in 1995. The directive requires member states to "implement technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss,

---

<sup>11</sup> "Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies," GAO Report, AIMD-00-295, September 6, 2000.

alteration, unauthorized disclosure or access” and to establish judicial remedies for breaches. The directive further requires members to establish a public authority to monitor adherence to the directive.<sup>12</sup>

In the Netherlands, authorities use iris scanners to verify travelers’ identities. The scanners do not store records but rather just match the iris to a biometric print on a frequent flier identification card. The Dutch Data Protection Authority also acts as a watchdog to ensure that records are not kept or shared with third parties. Similar measures, advocates say, could be taken in the United States.

Supporters of the identification card system also argue that inappropriate misuse of records could be made a felony with very stiff penalties. In Belgium, for example, breaches carry penalties of between eight days and five years. Moreover, the law could require that any information could be disseminated beyond a particular point only upon the individual’s permission, as is the case with laws protecting medical and banking records.

The Constitution does not explicitly provide a right to privacy, but in *Griswold v. Connecticut* (1965), the Supreme Court held that “various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment,” and the Third, Fourth, Fifth and Ninth Amendments were held to give people a right to privacy, and this doctrine has been used in many cases since. However, there has been some debate over whether the constitutional right to privacy includes the right to anonymity. Alan Dershowitz, for example, makes the argument that the right to privacy is solely the right to control one’s personal information and its dissemination, not hide one’s identity. He said, “American taxpayers, voters, and drivers long ago gave up any right of anonymity without loss of our right to engage in lawful conduct within zones of privacy.”<sup>13</sup> However, the Supreme Court has at least intimated to a right to anonymous political speech under the First Amendment in a number of cases.

At the end of the day, the creation of a national identification card inevitably would require some forfeiture of privacy and anonymity. Hence, it will have to come down to a question of whether the American people are willing to forsake certain rights and freedoms they have heretofore enjoyed in order to see this system implemented. If the decision is made that the balance of considerations weighs in favor of the identification card system, those concerned with privacy will have to turn their attention to ensuring that a maximum amount of energy and resources are put into securing the system, and demanding that there be strict limitations on what kind of information can be gathered, who it can be gathered by, and to whom it may be given. They also will have to pursue measures that impose serious penalties for violations of privacy protections.

### **Law Enforcement Abuse**

Another concern that civil liberties advocates raise is the potential for law enforcement authorities to abuse a national identification system. They argue that with such a system in place, individuals who do not produce an identification card when stopped on the street by law enforcement officers might become subject to a search or even arrest. Not having the card would make the person an immediate suspect.

Some further argue that a national identification card system would increase the incidence of ethnic and racial profiling by law enforcement. For example, authorities might be more likely to stop people who look Arab to ask them for their card. Certain minorities would be increasingly subjected to having to constantly prove their citizenship or immigration status. ACLU Associate Director Barry Steinhardt has said,

---

<sup>12</sup> 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, Document 395L0046.

<sup>13</sup> Alan Dershowitz, “Why Fear National ID Cards?” *New York Times*, October 13, 2001.

Rather than eliminating discrimination, as some have claimed, a national identity card in any form would foster new forms of discrimination and harassment of anyone perceived as looking or sounding ‘foreign.’ . . . Latinos, Asians, Muslims, and persons of Middle Eastern descent [would] become subject to ceaseless status and identity checks from police, banks, merchants and others. Failure to carry a national ID card would likely come to be viewed as a reason for search, detention or arrest of minorities. The stigma and humiliation of constantly having to prove that they are Americans or legal immigrants would weigh heavily on such groups.<sup>14</sup>

In other parts of the world where there is a national identification program, even in democratic nations, police can demand the identification on the threat of arrest. A Privacy International survey found police abuse of the cards in virtually every country that has them. The organization reported, “Most involved people being arbitrarily detained after failure to produce their card. Others involved beatings of juveniles or minorities. There were even instances of wholesale discrimination on the basis of data set out in the cards.” Privacy International further stated that, “French police have been accused of overzealous use of the identification card against blacks, and particularly against Algerians. Greek authorities have been accused of using data on religious affiliation on its national card to discriminate against people who are not Greek Orthodox.”<sup>15</sup>

Supporters of a national identification system respond that it actually would reduce profiling, since an encounter would immediately halt upon production of the card. Indeed, Rudi Veestraeten, the counselor and consul at the Embassy of Belgium testified before Congress,

In case of police checks, if some things happen and people are stopped in the street in a car, the fact that we have the identity cards and a very efficient database does save a lot of time. People can be released after only two minutes, just checking if this person is really who he is. So it’s a matter there in our view of civil liberty that we can release people immediately if there is no need to keep them. We don’t need to take them to the office, to the police office.<sup>16</sup>

Whether there is or is not a national identification card system in the United States, the issue of ethnic and racial profiling and prevention of terrorism will be present. If law enforcement is not in a position to demand presentation of a card from certain individuals who look a certain way, they may well find other pretexts for stopping them, as they are alleged to do presently. While the creation of a national identification card system would fuel the debate over whether profiling is an effective law enforcement tool, this issue is vigorously fought over right now, without the identification card system in place.

## **Cost**

There is much disagreement over how much establishing and implementing a national identification system would cost. Those who oppose such a system say a national identification card would cost billions of dollars to administer, and that a system able to reliably identify forged cards would be

---

<sup>14</sup> The Uniform Driver's License as a National ID, Address by ACLU Associate Director Barry Steinhardt to the American Association of Motor Vehicle Administrators, February 10, 2002.

<sup>15</sup> “Identity Cards – Frequently Asked Questions,” Privacy International, August 24, 1996.

<sup>16</sup> Does America Need a National Identifier? Hearing of the Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee of the House Government Reform Committee, November 16, 2001.

particularly expensive. The Social Security Administration has estimated that creating counterfeit-resistant Social Security cards would cost \$4 billion.<sup>17</sup> The ACLU says the cost of such a system has been estimated at as much as \$9 billion.<sup>18</sup> Simple smart cards cost \$10-\$35 a person.<sup>19</sup> The costs of a national system would include paying for card readers, staff and overhead, essentially, opponents argue, creating a new bureaucracy to administer the system. Even implementing a biometric identification system just for immigrants would be costly. For example, the reader machines that the INS currently uses to scan “laser visas” used by some Mexican immigrants cost \$2,400 each.<sup>20</sup> Foreign tourists, workers and students enter this country more than thirty million times every year, so the cost of issuing the cards and assembling the databases could be enormous. Moreover, integration of the databases of the various government agencies would cost a great sum as well, given their current state of disconnect.

However, supporters say a national identification card system would not be expensive. GartnerGroup, a technology research and consulting company, says that a card might cost \$8 per person and a commercial reader \$50 (If a card were to be issued for every American, this would translate to a cost of at least \$2 billion for the cards).<sup>21</sup> This, supporters say, is a reasonable expense for greater security. The cost of the effects of a terrorist attack must also be taken into consideration when undertaking any analysis of the cost issue. The World Trade Center attack cost New York City dearly; while still not entirely known, it is certainly in the many billions of dollars.

Cost estimates of systems used in other countries vary widely, and are greatly affected by what they take into account. The UK Government’s Informational Technology Center said that a national smart card would cost between five and eight pounds (\$5-\$11) each, but this figure did not include such costs as administration and compliance. The Home Secretary at that time estimated the cost would be double this amount.<sup>22</sup>

## EXPERIENCES OF OTHER COUNTRIES

Many countries around the world have national identification cards, although the type of card and the purposes for which it is used varies. Interestingly, Privacy International has found that the economic and political development of a country does not closely correlate with whether it has an identification card.<sup>23</sup> The types of cards issued, the information they contain, and what they are used for vary widely across the globe. The type of identification used is moving rapidly from more traditional identification documents to plastic cards. In a small number of places, such as Singapore, cards contain a bar code. The French are moving toward a machine-readable card as well.

The majority of cards in developed nations contain name, sex, and date of birth. Some have photographs and fingerprints. Some nations have much more data on their cards. For example, the Korean card has name, birth date, permanent address, current address, military record, issuing agency, issued date, photograph, national identification number, and prints of both thumbs. The Italian card contains identity number, name, photo, signature, fingerprint, date and place of birth, citizenship, residency, address, marital status, profession, and physical characteristics. In Spain, when someone works under contract the identification must be used to demonstrate work eligibility, and it also is

---

<sup>17</sup> Testimony of ACLU Legislative Counsel Katie Corrigan for the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Reform on the Establishment of a National ID Card System, November 16, 2001

<sup>18</sup> Coalition Letter to the President opposing creation of a national identification system by state departments of motor vehicles, ACLU website, [www.aclu.org/congress/1021102a.html](http://www.aclu.org/congress/1021102a.html), February 11, 2002.

<sup>19</sup> Lorraine Woellert, “National Ids Won’t Work,” *Business Week*, November 5, 2000, p. 90.

<sup>20</sup> Jonathan Peterson, “High Tech, Low Effort at INS; Security: Critics Say the Agency Should Have Improved Its ID Procedures Long Ago,” *Los Angeles Times*, November 19, 2001, p. A1.

<sup>21</sup> Paul Magnusson, “Yes, They Certainly Will,” *Businessweek*, November 5, 2001, p. 90.

<sup>22</sup> “Identity Cards – Frequently Asked Questions,” Privacy International, August 24, 1996.

<sup>23</sup> *Id.*

used for the health care system. In Kenya, the national identity card is required to get a job, get married, purchase or sell land, or register to vote. In Belgium, everyone over the age of fifteen is required to carry the identification card at all times. The card is used for banking, billing, rental agreements, proof of age when buying alcohol and cigarettes, or entering an adult-only business. A police officer can ask to see the card of anyone in a public space and does not need to have any particular justification.

### Examples of Countries with National Identification Cards

Germany	Honduras	Luxembourg	Poland	Argentina
France	Guatemala	Portugal	Chile	Singapore
Belgium	Kenya	Spain	Malaysia	
Greece	Brazil	Italy	Pakistan	

### Examples of Countries without National Identification Cards

Canada	New Zealand	Ireland	Mexico	Korea
Australia	Great Britain (voluntary ID card --- compulsory system rejected in 2001)	Sweden	Bangladesh	Taiwan

## PROPOSALS FOR A NATIONAL IDENTIFICATION CARD

### Legislative

1. The USA Patriot Act of 2001—the comprehensive antiterrorism legislation signed last year—provides that the attorney general and secretary of state, with the National Institute of Standards and Technology, and in consultation with other law enforcement and intelligence agencies, develop a technology standard to identify visa applicants and report progress made to Congress. The attorney general also must report to Congress on the feasibility of improving current identification systems that seek to identify foreigners who are wanted criminally before a visa is issued or the person enters or exits the United States.
2. Senator Dianne Feinstein has expressed great interest in a national identification system and with Senator Jon Kyl has already introduced the Visa Entry Reform Act of 2001 (S. 1627). This legislation includes a provision requiring non-citizens to use high-tech visa cards containing a fingerprint, retinal scan or other unique identifier by October 2003. The bill also requires that all new “identification documents, licenses and permits” issued by the Departments of Justice, Transportation and Health and Human Services, and the Social Security Administration, adhere to common means for preventing fraud and alteration of such documents.

The House of Representatives passed the Enhanced Border Security and Visa Entry Reform Act (HR 1325) in December. It requires the State Department to issue alien visas with machine-readable biometric identifiers by next October, and for the INS to install machines to read them by the same time. A bill by the same name (S. 1618), introduced by Senator Edward Kennedy, similarly requires the attorney general to install biometric data readers and scanners

at every U.S. port of entry within one year of enactment. It mandates that the attorney general and the secretary of state must also issue machine readable, tamper resistant, travel documents with biometric identifiers. They must also require tamper resistant, biometric machine-readable passports for entry of individuals from countries participating in the visa waiver program.

Thus, while the USA Patriot Act identifies the goal of using a biometric identification method for immigrants and asks for further research and development on the possibility, these other legislative proposals take the concept much further and mandate that such a system be put into place in the next several months.

3. After conducting a hearing on the issue in November 2001, Representative Steve Horn called for a federal commission to study issuing national identity cards to every American. He proposed that Congress and the president appoint members of the commission. He introduced the Commission on Homeland Security Act (HR 3378) thereafter to establish a Commission that, among other things, would study the “accuracy, reliability, and security of personal identification information and systems used by the Federal Government under existing law.” Therefore, like the Patriot Act, Representative Horn’s bill advocates further study of the issue.

### **Association and Industry Proposals**

1. The American Association of Motor Vehicle Administrators is developing a plan to create a national identification system that would link all driver databases throughout the country and use a card that has a unique identifier. The association is asking Congress for up to \$100 million to create the system, and Senator Richard J. Durbin, Democrat of Illinois, is working on a bill to back the proposal. The group is pledging to work with the Office of Homeland Security on this, thus recognizing its use for security purposes. Indeed, association officials have argued that, since the attacks, driver’s licenses have already become a “de facto national identification card.”

Clearly, this proposal goes much further than anything that has emanated from Congress. The association actually seeks to establish a national identification system based on the driver’s license that would be issued to everyone, not just visa applicants. Moreover, if this proposal were in fact pursued, the system could potentially be in place more quickly since people generally already use their driver’s license as identification and at least some of the infrastructure for the system already exists through each state’s Departments of Motor Vehicles.

2. Due to customer dissatisfaction with longer security clearance lines at the airports, the American Transport Association, representing the airline industry, supports a voluntary “smart card” identification that frequent travelers can pay for and use to expedite check-in time. Such a system would separate travelers that are already known via the airline’s database, from unknown people who would be scrutinized more closely. The airlines already have been working on creating such systems individually. However, according to the president of the Air Travelers Association and other industry experts, with the federal government poised to take over much of airport security, a uniform system may emerge. Indeed, the government is already planning to establish a computer network that links all airline reservation systems to private and government databases. The network would analyze detailed information and assign a threat score to each passenger. The companies already developing these systems for private airlines would like to link the system to a national identification, a biometric identifier, or both. Establishing such a system would likely require a rollback of some current federal privacy laws.

The airline industry proposal is different in that it is ostensibly voluntary, although it would seem that anyone who flies with any frequency might feel quite compelled to enroll in the

program. It also does not distinguish between foreigners and citizens. It is unclear at this point whether an airport/travel based identification system would be run by private industry or the government, and this choice would have different implications for being able to place restrictions and protections on the system.

## **Corporate Proposals**

Naturally, companies that stand to benefit from increased use of high tech identification methods support the idea of a national identification card. The most prominent among the supporters is Larry Ellison, CEO of Oracle Corporation, the leading maker of database software, who has been meeting with a number of Washington officials to discuss the idea. He has offered to donate the software for the creation of the system, but not the maintenance or upgrades, or the other costs of implementation. Under his proposal, the cards would be mandatory for foreigners and voluntary for citizens.

The International Biometric Industry Association has not advocated a national identification card, but rather has argued for use of facial recognition technology at airports and improvements in current systems, such as the FBI's fingerprint system. The Biometric Foundation, a research organization that is directed and operated by biometric company heads, has testified before Congress in favor of using biometrics in "passports, visas identification cards, and other travel documents." Many industry executives also have testified before congressional committees about increasing the use of biometrics. Many companies have set up special divisions to pitch their wares and hired Washington lobbyists. The International Biometric Group expects that revenues for the industry will increase from between \$119 million and \$127 million in 2000 to \$523 million in 2002.

## **MOVING FORWARD**

As the debate over a national identification card system unfolds, it is likely that some sort of more extensive identification system will eventually be established in the United States. Legislation moving in that direction has already been introduced. The Association of the Departments of Motor Vehicles is establishing a system of biometric identification cards, and the private airline industry is starting to implement quick check-ins for travelers who apply for a special identification card.

If that is the case, efforts to reach a compromise on the areas of disagreement will focus on such issues as:

- specific restrictions on the types of information that either a private or public entity can collect
- restrictions on which public agencies are authorized to collect information
- requirements that any identification card put into use by private entities be of a voluntary nature
- laws and regulations regarding who may have access to the relevant data
- laws and regulations regarding to whom such data can be released
- laws and regulations as to who and what entities can demand presentation of the card
- measures to ensure that the data systems employed have the highest possible security
- specific guidelines for use by law enforcement and penalties for abuse by law enforcement

## RESOURCES/LINKS

ACLU:

<http://www.aclu.org>

Testimony of ACLU's Kate Corrigan:

<http://www.aclu.org/congress/1111601a.html>

[http://www.aclu.org/features/National\\_ID\\_Feature.html](http://www.aclu.org/features/National_ID_Feature.html)

Letter to the President from civil liberties and consumer groups

[www.aclu.org/congress/021102a.html](http://www.aclu.org/congress/021102a.html)

Privacy International:

<http://www.privacyinternational.org>

Senate Bill S. 1627:

<http://www.thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c10706dw90>

Feinstein statement:

<http://www.senate.gov/~feinstein/releases01/r-visas1.html>

House Bill H. 3525:

<http://thomas.loc.gov/cgi-bin/query/D?c107:3:./temp/~c107rxm0L>

House Government Reform Committee, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Hearings on National ID Card:

[http://www.house.gov/reform/gefmir/hearings/2001hearings/1116\\_nationa\\_id/1116\\_witnesses.html](http://www.house.gov/reform/gefmir/hearings/2001hearings/1116_nationa_id/1116_witnesses.html)

Watch the hearing:

[http://www.c-span.org/technology\\_science](http://www.c-span.org/technology_science)

Progressive Policy Institute proposal for a national ID card

[www.ppionline.org/ppi\\_ci.cfm?knlgAreaID=85&subsecid=108&contentid=250176](http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=85&subsecid=108&contentid=250176)

[www.ppionline.org/ppi\\_ci.cfm?knlgAreaID=140&subsecID=290&contentID=250175](http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=290&contentID=250175)

Information from New York State Senate Anti-Terrorism Special Committee, which recommends a national ID card

<http://www.roygoodman.org>

Comments from Representative George Gekas, Chairman of the House Subcommittee on Immigration and Claims

<http://www.house.gov/gekas/columns/September/2001/28-NationalID.html>

Testimony of Monte Belger, Acting Deputy Administrator of the FAA, which supports use of a traveler ID card, before the Senate Subcommittee on Technology, Terrorism, and Government Information

<http://www.faa.gov/apa/TESTIMONY/2001/1114temb.html>

Immigration and Naturalization Service

[www.ins.gov](http://www.ins.gov)

U.S. Department of State, Visa Information

[www.travel.state.gov](http://www.travel.state.gov)

GAO Report -- Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies. AIMD-00-295 September 6, 2000.

[www.gao.gov](http://www.gao.gov)

Cato Institute:

<http://www.cato.org/tech/tk/010928-tk.html>

Electronic Information Privacy Center:

[http://www.epic.org/privacy/id\\_cards](http://www.epic.org/privacy/id_cards)

Pew Research Center:

<http://www.people-press.org/terrorist01rpt.html>

## KEY ARTICLES

- Robert O'Harrow, Jr., "Rights Groups Oppose ID Card," *Washington Post*, February 13, 2002, p. A15.
- Robert O'Harrow, Jr., "States Seek National ID Funds," *Washington Post*, January 14, 2002, p. A04.
- Jonathan Turley, "Let's Not Rush Headlong Into a National ID," *Newsday*, January 14, 2002, p. A20.
- Jennifer Lee, "Upgraded Driver's License Are Urged as National ID's," *New York Times*, January 8, 2002.
- Joe Sharkey, "Class Consciousness Comes to Airport Security," *New York Times*, January 6, 2002.
- William Safire, "Threat of National ID," *New York Times*, December 24, 2001.
- Robert O'Harrow, Jr. and Jonathan Krim, "National ID Card Gaining Support," *Washington Post*, December 17, 2001, p. A1.
- Diane Feinstein and Jon Kyl, "We Can't Afford To Be Cavalier about Our Borders," *Los Angeles Times*, November 12, 2001, p. B11.
- Mike Francis, Heather Green, Jim Kerstetter, Jane Black, Alex Salkever, and Dan Carnery, "Privacy in an Age of Terror," *Business Week*, November 5, 2001, p. 82.
- Lorraine Woellert, "National Ids Won't Work," *Business Week*, November 5, 2001, p. 90.
- Paul Magnusson, "Yes, They Certainly Will," *Business Week*, November 5, 2001, p. 90.
- "Id Card Idea Attracts High-Level Support," *San Jose Mercury News*, October 17, 2001.
- Alan Dershowitz, "Why Fear National ID Cards?" *New York Times*, October 13, 2001, p. 23.
- Daniel J. Wakin, "National ID Cards: One Size Fits All," *New York Times*, October 7, 2001.
- August Gribbin, "White House Rules Out National ID Card," *Washington Times*, September 28, 2001.
- Robert O'Harrow, Jr., "Intricate Screening of Fliers In Works," *Washington Post*, February 1, 2002, p. A1.

---

Written by Tova Andrea Wang, Program Officer and Special Counsel for The Century Foundation.

All of the Issue Briefs in this series, along with a catalog of The Century Foundation's publications are available at <http://www.tcf.org>. For more information please contact Tina Doody at 212-452-7750 or [doody@tcf.org](mailto:doody@tcf.org).