Legal Backgrounder

Washington Legal Foundation
effective advocate of free enterprise®
2009 Massachusetts Ave., NW
Washington, D.C. 20036
202.588.0302

Vol. 17 No. 1 January 11, 2002

SECURING PERSONAL INFORMATION KEY TO ANTI-TERRORISM EFFORTS

by

Barnaby Zall

After the first World War, France built an impregnable wall of fortifications to prevent future invasions. Known as the Maginot Line after its architect, Minister of War Andre Maginot, the wall was state of the art in communications, strength, and design.

The major impact of this massive undertaking? A false sense of security. Like a football team which puts all its defenders on the front line, the Maginot Line was fatally flawed; in 1939, the Nazi armies simply went around it and conquered France.

Though well-intentioned, many recent anti-terrorism proposals have similar gaping loopholes that can be exploited to defeat their protections. Increasing security checkpoints, for example, will not defeat those who commit identity fraud to obtain legitimate domestic documents. The September 11 terrorists, for example, were easily able to obtain genuine drivers licenses, which allowed them to board airplanes without further investigation. Without comprehensive protection for domestic documents, the only effect of these anti-terrorism proposals will be a false sense of security.

The Problem. Americans live in one of the most technologically-advanced societies in the world, yet we do not know who enters the United States. The vast majority of aliens who enter this country are welcome visitors and friends; unfortunately we have no way to separate friends from those who wish only death to America and Americans. As a result, terrorists and other unauthorized aliens enter the United States with minimal effort.

Our first line of defense against criminal aliens is supposed to be our embassies overseas, which gather information and issue entry visas. Yet embassies often neglect visa issuance duties, in favor of more glamorous foreign policy tasks; overworked embassy personnel have neither the resources nor the time to properly screen visas. One recent estimate suggested that visa applications are reviewed in about seven seconds, without computerized information or other aids in screening out terrorists or criminals. In addition,

---

Barnaby Zall is Of Counsel to the law firm of Weinberg & Jacobs, LLP, in Rockville, Maryland. He is an advisor to United to Secure America, a coalition of organizations seeking to reduce terrorism in America.

visitors and others from many countries are admitted to the United States without any visa at all — a well-intentioned effort designed to boost commerce by allowing travelers to save time, but which skips essential background checks which could identify unwanted visitors.

Once an alien arrives in the United States, the Immigration and Naturalization Service is supposed to double-check visas and eligibility to enter. Unfortunately, the INS computer systems are antiquated and do not recognize criminals identified by the FBI and other American intelligence agencies. The INS has a "lookout" system designed to identify terrorists and other aliens but it simply does not work, as shown by entry of the September 11 terrorists. A highly-touted system using "biometric" technology to identify persons entering the U.S. is available at a few airports, but is purely voluntary. At other ports of entry, people claiming to be citizens can simply walk by most inspections.

In other words, the border protection system is set up to stop people who declare themselves to be criminals, and is easily evaded by those with something to hide. Small wonder that the INS cannot even figure out how the September 11 terrorists entered the United States.

Even worse, once inside the United States, unauthorized aliens can easily obtain legitimate governmental documents and certifications which allow them to remain here illegally and to undertake activities, such as attending flight schools, which might expose Americans to danger. The September 11 terrorists obtained drivers licenses and identification cards from different States, apparently without much effort at all.

In fact, some States are even making it easier for aliens without legitimate documents to obtain drivers licenses. Document fraud rises immediately in direct correlation; for example, in 1996, Kentucky dropped a requirement that foreign applicants take drivers' tests, and within days a national immigrant smuggling ring identified the state as an easy mark for obtaining drivers licenses. Escorted groups from New York and other places came to Kentucky to obtain licenses; Louisville alone reported an increase of 200 applications per week.

For many Americans, this out-of-control border is unacceptable. Americans are willing to take significant steps to protect themselves and their country from this threat. A September 2001 Pew Research Center poll found that 70% of respondents favored requiring all citizens to carry national identity cards to be produced upon demand by police; similar responses were reported from *The New York Times*, CBS News, CNN and *Time* polls. Larry Ellison, chief executive of leading software company Oracle, offered to donate the software necessary to embed fingerprints on identity cards and update governmental databases.

Despite this widespread support, a national identification card might simply be another Maginot Line, with a high price for a false sense of security. A security system is only as strong as its weakest link. The weakest point of recent anti-terrorism proposals is their reliance on a flawed and vulnerable system of domestic documents. No recent reform proposal addresses needed improvements in domestic document security.

Solutions Are Available. There is little doubt that technology can provide significantly better protection for the United States and its people. Private companies and other countries (including modern, open democracies) have decades of experience in this area and have implemented inexpensive and effective ways to both maintain and use secure documents. Credit cards, for example, are increasingly fraud-resistant, both because of physical protections on the cards themselves, and backup systems which analyze usage patterns and known fraudulent histories. Companies employ a variety of employee, visitor, and user security measures which protect sensitive installations and data.

Government agencies, however, have been slow to adopt these protections. Basic documents like

birth certificates are easily forged, with no secondary verification of underlying information. Even a simple technique, like matching birth and death records to stop someone from requesting a birth certificate for a dead person, is impossible today. Extensive databases of information about criminals and terrorists are held by different agencies, but not cross-matched to share information, and not made available to embassies, immigration inspectors, or drivers license agencies.

One of the major factors slowing government use of simple protective techniques has been concern about citizens' privacy and bureaucratic misuse. Misuse of information can be prevented with stiff penalties and vigorous enforcement; the misuse of tax return information, for example, is rare because Internal Revenue Service officials are both trained to avoid misuse and severely punished (even jailed) for errors. Similarly, the Privacy Act of 1974 prevents most invasions of privacy by limiting the gathering and distribution of information collected by federal and State agencies.

These concerns can be easily addressed and protections integrated into new document security systems which protect Americans against terror and abuse. In addition to incorporating existing privacy and abuse protections, these systems would not require the gathering of new information, and would not be used to monitor the activities or movement of American citizens. More pointedly, they would only improve the security of existing documents, and would not require the use of a new national identification card.

Moreover, these new systems could be designed to maintain most information internally, rather than reporting substantive information beyond the normal investigative or enforcement needs of the agency; in other words, even in systems which were designed for access by persons outside the investigating agency, only the minimum necessary information would be given out. For example, a system which allowed licensing agencies or employers to verify the validity of a Social Security number would only report whether the number was valid or not, without providing additional information on the reasons for any invalidity; any investigation into misuse would be undertaken by appropriate enforcement authorities, rather than the original inquiring agency or person.

Some of these new systems require significant new technology for government agencies, but these devices have long been available outside of government. For example, government agencies are just now learning to use Internet access systems which have been perfected (in a secure manner) by private industry over the last ten years. Where previous cost estimates for linking government criminal databases with immigration records have been very high, modern software and Internet systems make such access inexpensive and reliable.

The basic elements of all these systems to protect domestic documents and identification are interconnectedness (so that information in one system is available to another), ease of access (so that the systems will be rapidly accessed at the point of use), and multiple verification of underlying claims (recognizing that a system is only as good as its underlying information). Technological innovations, such as fast communications networks, analysis and recognition software, and information compression, are essential both to increase efficiency and to make the systems as easy to use as possible.

Missing Steps to Protect Domestic Documents. There are five areas where improvements are necessary to make security systems work, none of which have been addressed in current anti-terrorism legislative proposals:

Vital Records. These basic documents are vital records of important life events, such as birth certificates, baptismal records, and immigration documents. Yet these basic documents are vulnerable to fraud and abuse; for example, because most States don't match birth and death records, someone can easily assume the identity of a dead person by requesting their birth certificate. The National Center for Health Statistics and the National Association for Public Health Statistics and Information Systems have prepared

a Uniform Model Vital Records Act which incorporates many of these simple protections against "breeder document" fraud, but the Act has not been adopted by many States. Federal assistance would enable States to standardize systems, computerize basic record-keeping and reporting, and share information.

Social Security Numbers. The Social Security number is ubiquitous in American life today. The common use and inexpensive availability of information on the Internet belies any contention that the Social Security number is either secret or not to be used as an identifier. Unfortunately, Social Security numbers are also among the least-protected and most abused of all domestic document systems. The Social Security Administration does not verify the authenticity of most documents presented to it before issuing a new number, and does not investigate or report when a misused or stolen number is used in identity fraud. The September 11 terrorists had Social Security numbers. The Social Security Administration must improve its internal security and number issuance procedures and make available its lists of stolen or misused numbers to those who need to verify a number's validity.

Drivers Licenses. Drivers licenses are the basic document used by most American businesses and government agencies to determine a person's identity. Airport security, for example, requires only that a prospective passenger show a drivers license. Although many States have recently improved the physical security of their licenses (generally making them more tamper-resistant), much more can be done. The September 11 terrorists easily obtained Florida drivers licenses. The American Association of Motor Vehicle Administrators has proposed a comprehensive set of reforms for drivers licenses, many of which were enacted by Congress in 1996; unfortunately, Congress repealed those reforms in 1999. Congress should work with the AAMVA's new anti-terrorism Task Force to implement needed security for drivers licenses. Recent efforts to grant drivers licenses to illegal immigrants should be reversed.

Improvement of Immigration and Terrorism Databases. The federal and State governments already collect significant information which could be used to fight terrorism, but that information is not shared between agencies or made available to those who protect against terrorists. For example, most immigration information on terrorism suspects is kept on paper index cards, and is not currently available at ports of entry or visa issuance sites; most of the September 11 terrorists who were listed on immigration or terrorist "watch lists" were nevertheless able to obtain valid entry visas. The information currently available from various government agencies should be integrated and distributed in "real time" to those who need to screen terrorists from entry. "Secondary verification" techniques should be used to detect aliens who are committing identity fraud or otherwise violating our laws. A few recent anti-terrorism proposals focus on this area of improvement.

Resume Interior Enforcement of Immigration Laws. It does little good to require reporting of terrorist activities if no one is available to investigate the problem or apprehend the suspects. In recent years, budget and policy changes have confined enforcement of immigration laws to borders and ports of entry. If an alien got past a border inspector, as the September 11 terrorists did, they were "home free" without fear of further investigation. As a result, there is neither immigration law enforcement within the United States, nor any incentive for reporting suspected abuse to the Immigration and Naturalization Service. The current immigration enforcement system is exactly like the Maginot Line: useless for stopping terrorism while engendering a false sense of security that simply passing tougher immigration laws will have some effect. If anti-terrorism investigations are to have any effect, INS must resume enforcing immigration laws inside the United States.

Coupled with effective international and domestic actions against terrorism, increasing domestic document security will help protect America and Americans against terrorism. Other side benefits, such as a reduction in the rapidly-increasing levels of identity theft and fraud, can be expected as well. Yet without swift action to improve current antiterrorism proposals, this vital area will be overlooked, and America will have constructed only a Twenty-first Century Maginot Line.

  ISBN 1056 3059