PRIVACY INTERNATIONAL

The enhanced US border surveillance system: an assessment of the implications of US-VISIT

September 28, 2004

From September 30 2004, all visitors to the United States will be face-scanned and fingerprinted at the border. These measures are part of a vast integrated information storage, matching and profiling system. The increased surveillance at borders poses significant challenges to civil liberties, to race relations and to the functioning of a free and open society.

The U.S. Visitor & Immigration Status Indication Technology System (US VISIT) has been deployed in response to significant issues of security, but in spite of its public interest objectives the system places human dignity and privacy at substantial risk. U.S. authorities claim VISIT is a necessary weapon in the fight against terrorism. On closer analysis the system is fundamentally flawed and has the potential to be a corrosive and dangerous practice that will spread internationally.

* VISIT employs technology and techniques that are unreliable and unpredictable. The matching of information between a large number of systems generates substantial errors, while the use of biometrics such as finger-printing involves the risk of false accusations on a mass scale because of the inherent frailty of one to many systems.
* VISIT ignores the legal concept of proportionality by creating mass surveillance in order to identify a relatively small number of suspects.
* VISIT redefines due process. Where previously people would be fingerprinted and scrutinised upon suspicion, they are now all suspects until at least temporarily eliminated from suspicion. There is no meaningful oversight. While Europe has several mechanisms, such as the European Court of Human Rights, in North America protections are minimal as National Security interests trumps all rights of data protection.
* VISIT abolishes all principles of privacy. It accumulates personal information indiscriminately, collecting and sharing this information for unforeseen purposes, and retaining it over our lifetimes.

A child entering the U.S. on October 1 will have her fingerprints on record for the rest of her life. There is no end to the uses to which this sensitive information will be put, nor any meaningful borders or boundaries limiting the flow of this data. This is why governments around the world have expressed both concern and excitement by the system.

For these and other reasons Privacy International is providing a Q&A analysis regarding US-VISIT.

1. Will the U.S. Government protect my personal information against abuse?
2. Will this information only be used to combat terrorism?

3. What's wrong with the U.S. Government protecting its borders?
4. If I have nothing to hide, then why should I be worried?

Absent Protections, Lawless Promises
Will the U.S. Government protect my personal information against abuse?

Many countries around the world have strong privacy laws to provide protection against the abuse of personal information. The U.S. Privacy Act is designed to protect the privacy of Americans. Foreigners have no rights.

VISIT will collect and retain biographic, travel, and biometric information on all visitors. The purpose of this collection is to identify people who are believed to potentially pose a threat to the security of the U.S., are known or believed to have violated the terms of their admission to the U.S., or who are wanted in connection with a criminal act in the U.S. or elsewhere. This information will be shared with "other law enforcement agencies at the federal, state, local, foreign, or tribal level" who "need access to the information in order to carry out their law enforcement duties."[1]

This personal information will be retained for 75 to 100 years. It is kept alongside data collected from nationals of countries that threaten to wage war, or are or were at war with the United States.[2]

The Department of Homeland Security (DHS) claims that it will protect privacy in accordance with its privacy policy. It claims that its Privacy Impact Assessment is widely heralded. This is not true. The flawed policy was released moments before the VISIT system went live in January.

When VISIT first began, there were no rights of redress for individuals who faced any sort of adverse consequences.[3] Following an outcry by legal and civil rights advocates there is now a limited appeal process, including a human review of the fingerprint matching process, and provision for some correction of faulty information. These reforms however do not help in the case of expedited removal of individuals. Given that incomplete information is used to make decisions on visitors this situation is likely to occur increasingly.[4]

The implementation of US VISIT should be considered against the backdrop of existing travesties of justice at border entry points. Many people have been shackled and returned home immediately without due process of law because of problematic visa-status. There are other reasons, however hard they are to decipher. Consider the case of Mohamed Arar, a Syrian-born Canadian citizen. On a return trip to Canada that included a connection change in New York, he was interrogated and deported to Jordan on the condition that he be sent to Syria, where he was subsequently kept in prison and tortured for over a year. The decision to deport him, when he was merely connecting through the U.S. and was not even visiting the U.S., was based both on faulty information provided by the Canadian police and by a lack of accountability in U.S. decision-making processes and opaque watchlist procedures.[5] In an ironic turn of events, the Syrian justice system decided he was not guilty and sent him home to Canada.

The U.S. Government is now investing 15 billion dollars to create dossiers on all visitors to the U.S. (even though DHS had originally budgeted 7.2 billion [6]). Now the system is likely to include other biometrics in the future; according to the contract winner, *Accenture*: "Part of our approach is to continually assess technology innovations. For a 10-year contract that's a generation or two of technology, and biometrics is a very hot area."[7]

Function Creeping from Anti-Terrorism to the Kitchen Sink
Won't this information only be used to combat terrorism?

Once data resides in the U.S. it is open to use by any number of systems and programmes designed to mine such information. According to the General Accounting Office, there are 199 data mining programs currently in place within the various departments of the U.S. Government. 122 of these use personal information, 54 of these use private-sector information such as credit card information and credit reports. The primary purposes of these systems include detecting fraud, waste, and abuse; detecting criminal activities or patterns; analyzing intelligence and detecting terrorist activities; and increasing tax compliance.[8]

The GAO also assessed the US-VISIT system in March 2004 and declared that it is "inherently risky because it is to perform a critical, multifaceted mission, its scope is large and complex, it must meet a demanding implementation schedule, and its potential cost is enormous." Pointing to other data collection and mining initiatives, the GAO warned that the project is ‘increasingly risky’.

The focus of every system deployed by the U.S. Government since September 2001 has moved well beyond countering terrorism. Passenger data transfers from the EU were originally intended for national security and aviation security purposes, but this quickly spread to prevention and detection of crime. CAPPS II, the now (relatively) defunct passenger profiling system was to be used to process all people for all crimes. It is therefore a tool to enforce immigration laws, among any number of other purposes, not to identify terrorists.

In 1996 Congress called on the Attorney General to develop an automated entry and exit monitoring system for foreigners. This was expanded significantly by the USA-PATRIOT Act that suggested the use of biometrics. The Enhanced Border Security and Visa Entry Reform Act (EBSVERA, the less sexily named law that took the USA-PATRIOT Act even further) called for the integration of VISIT with other databases.

This system is to be used for a plethora of purposes. These include national security, law enforcement, immigration control, and "other mission-related functions and to provide associated management reporting, planning and analysis." It will assist in:

> "identifying, investigating, apprehending, and/or removing aliens unlawfully entering or present in the United States; preventing the entry of inadmissible aliens into the United States; facilitating the legal entry of individuals into the United States; recording the departure of individuals leaving the United States; maintaining immigration control; preventing aliens from obtaining benefits to which they are not entitled; analyzing information gathered for the purpose of this and other DHS programs; or identifying, investigating, apprehending and prosecuting, or imposing

sanctions, fines or civil penalties against individuals or entities who are in violation of the Immigration and Nationality Act (INA), or other governing orders, treaties or regulations and assisting other Federal agencies to protect national security and carry out other Federal missions."

This is not about terrorism; it is a sophisticated system of immigrant monitoring, amongst other things.

This information will be shared with other government departments and used in other programs of surveillance. This includes:

- "to the appropriate agency/organization/task force, regardless of whether it is Federal, State, local, foreign, or tribal, charged with the enforcement (e.g., investigation and prosecution) of a law (criminal or civil), regulation, or treaty, of any record contained in this system of records which indicates either on its face, or in conjunction with other information, a violation or potential violation of that law, regulation, or treaty,"
- "to other Federal, State, tribal, and local government law enforcement and regulatory agencies and foreign governments, and individuals and organizations"
- during the course of an investigation or the processing of a matter, or during a proceeding within the purview of the immigration and nationality laws, to elicit information required by DHS to carry out its functions and statutory mandates
- "in response to its request, in connection with the hiring or retention by such an agency of an employee, the issuance of a security clearance, the reporting of an investigation of such an employee, the letting a contract, or the issuance of a license, grant, loan, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision in the matter."
- "to assist such agencies in collecting the repayment or recovery of loans, benefits, grants, fines, bonds, civil penalties, judgments or other debts owed to them or to the United States Government, and/or to obtain information that may assist DHS in collecting debts owed to the United States government."

amongst many other recipients.[9]

The U.S. Government has already made Visa information available to law enforcement officials across the country, including photographs of 20 million visa applicants. This 'sensitive' information will be shared with 100,000 investigators across the country who will have access to seven terabytes of data on foreigners.[10] Access to this data is not merely intended to combat terrorism, but as stated above, to ensure that foreigners are in the U.S. legally. This process can be likened to a mass deployment of checkpoints across the country.

The integrity of these checks is questionable. The watchlists are numerous, and plagued with errors. Soldiers, ministers, and members of Congress (and anyone else with the name "T Kennedy") have been found to be on these lists, sometimes resulting in invasive searches and often resulting in deplaning or a refusal to permit boarding. The media stories and court cases to date have mostly focussed on U.S. citizens who have access to U.S. courts and who have standing in law; this is not the case for someone flying in to the U.S. who is sent back home after being wrongly identified. There are unclear procedures for placing someone's name on

these lists, and even less clear procedures for removing names from these lists. Could we even imagine a process of oversight over these numerous lists?

With extensive profiling and data-mining the problem only gets worse. Consider the Multi-state Anti-TeRrorism Information eXchange (MATRIX) programme. This system combines information from government databases and private-sector data companies about individuals, and makes that data available for search by government officials. Officials can then comb through billions of files in a search for "anomalies" that may be indicative of terrorist or other criminal activity.[11] The quality of the various information sources is demonstrably unsafe; but this information is combined nonetheless, including data from the FBI, and DHS, names and address record, driver license photos, links to associates, and even ethnicity. It was used in the months after September 11 to identify suspected terrorists residing in the U.S. Using a 'terrorist quotient' it identified 120,000 individuals who fit the 'characteristics' of a terrorist. Because of subsequent privacy concerns, two thirds of U.S. states that were originally part of the MATRIX programme have pulled out. Now US-VISIT, amongst other data mining programmes, threatens to supersede the discredited system.

None of these programmes are limited to combating terrorism, nor were many of them created with terrorism in mind. They are intended to increase surveillance for all purposes and reasons, while reducing oversight and accountability.

Setting the Standard for Surveillance
What's wrong with the U.S. Government protecting its borders?

There are right ways and there are wrong ways to improve safety and security. VISIT is another step down the wrong path to securing borders.

After September 11 the U.S. began a number of programmes that involved the 'registration' of Muslim and Arab immigrants, and others deemed to be of interest.

After the terrorist attacks, the Immigration Services identified 7602 individuals who shared similar 'characteristics' to the 19 hijackers, and aimed to interview them. These interviews were said to be 'voluntary', though few believed this to be true.[12] Law enforcement officials interviewed 3,000 Muslim and Arab immigrants in the U.S. and considered the programme a success. However a Congressional study found that only 20 immigrants were arrested, and most of these were on immigration violations, and none on terrorism charges.[13] Even at this time, however, the government list of individuals it intended to question contained many duplicate names and data entry errors. The practice was considered to have an adverse effect on relationships with these communities, however the response of the U.S. Government was to overplay the usefulness of this project.[14] The results of these interviews were not analyzed, nor are there any plans to do so.

Consider SEVIS, the Student and Exchange Visa Information Service that forces schools across the country to submit information on foreign students (of which there are over 500,000). The system is actually based on an earlier law, from 1996 but later amended by the USA PATRIOT Act, to keep track of addresses of students, their enrolment status, whether they have a reduced course load, and monitoring 'optional practical training',[15] on an Internet-based system.[16] Despite assurances that SEVIS was not complex, expensive or burdensome and that it would provide accurate, unambiguous and current information, the

polar opposite has resulted. In one situation, 1450 student files were stolen by malicious hackers from the University of Kansas.[17] INS also had to extend the deadline for implementing the system due to complaints from schools that the system was too cumbersome and was neither responding properly,[18] nor designed adequately.[19] There have been additional complaints regarding data integrity and data security.[20] Others have complained of unfair processes and students being wrongly thrown out of the country.[21]

Next came the 'Special Registration Procedures for Certain Non-immigrants'. This involved the forced registration, interviewing and fingerprinting of individuals. The programme originally started with fingerprinting and interviewing of citizens or nationals of Iran, Iraq, Libya, Sudan and Syria, but also "any other non-immigrant identified by INS officers at airports, seaports and land ports of entry", based on criteria designated by the Secretary of Homeland Security.[22] The programme was later extended to include individuals from Afghanistan, Algeria, Bahrain, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, North Korea, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, United Arab Emirates and Yemen.

Of the 82,000 men who were registered, more than 13,000 were found to be living in the U.S. illegally, and were to be deported.[23] The programme was later shut down in November 2003, one month before US-VISIT went live.[24]

The National Security Entry-Exit Registration System followed, targeting individuals specifically at the border. Ironically, registration was justified on the grounds that the European authorities have registered visitors for some years. According to the Department of Justice,

> “Our European allies have had similar registration systems in place for decades and know the value of ensuring that foreign visitors are doing what they said they would do and living where they said they would live. The NSEERS system takes the European model and combines it with a modern intranet system so that files may be updated in real time at any INS office in the country.” [25]

Under NSEERS, these individuals would be 'fingerprinted and processed'. It was not limited to 'terrorist nations', however. According to the Attorney General,

> “So far, [Immigration and Naturalization Services] has fingerprinted and registered individuals from 112 different countries. From the Baltic to the Balkans and from the Cape of Good Hope to the Rock of Gibraltar, visitors who may present elevated national security concerns will be included. No country is exempt. In the war against terrorism, we cannot afford to have tunnel vision”.[26]

The general response to this practice was negative. After considerable pressure from foreign governments[27] and civil liberties advocates, the programme was shut down.

Or so we were led to believe. In fact, in April 2003 NSEERS was renamed as the US-VISIT programme. Although the US-VISIT programme would end the domestic special registration, it would register all visa-holders to the U.S., and was later extended to all visitors to the U.S. This would circumvent prior concerns from civil liberties advocates and lawyers that the earlier programs were discriminatory.

Therefore, the history of this project is ensconced in discriminatory policies that were considered invasive and which led to problematic decisions, widespread concern, and technological chaos.

When originally implemented, VISIT was designed only for the verification of visas that included biometrics. According to one report[28] these new visa processes, are said to be causing delays in granting visas, and have cost U.S. firms at least 30 billion dollars since July 2002, According to some critics these burdens to entering borders are hurting the economy.[29]

When the adoption of biometric passports encountered delays, the Department of Homeland Security then decided to include all visitors to the U.S. under the VISIT registration regime.

The VISIT methodology is now going international. Ironically, Brazil retaliated to VISIT by fingerprinting U.S. citizens, which led to a complaint from Secretary of State Colin Powell because it was felt that Brazil was discriminating against U.S. citizens.[30] Greek, Swiss, and Chinese officials, amongst many others have complained about the forced registration of their nationals, whilst other governments have been conspicuously silent.

The U.S. has been calling for international co-operation on this scheme. According to Secretary Ridge,

> “I think it's critical that we move this along as quickly as possible, and the best way of facilitating that is not simply on a bilateral-by-bilateral basis, but to get as much multilateral buy-in as soon and as quickly as possible.”[31]

Canada is moving towards fingerprinting and face scanning, as part of its 'Smartborders' programme.[32] Britain is planning a similar system in order to deal with asylum seekers, possibly using iris scanning.[33] Japan has set up a working group to look into possible biometric solutions.[34] And the G8 and EU have been working on a standardising policy amongst member states, including the fingerprinting of their own nationals.

The U.S. is in favour of this internationalisation. Even as the New York Times claims that "[t]he government has wisely decided that [all visitors to the U.S.] will be included in [VISIT], which checks photographs and fingerprints against watch lists... it is hardly an onerous burden"[35], it fails to recognise that soon Americans will be fingerprinted when they travel, all because of the U.S. policy. In yet another case of policy laundering, Department of Homeland Security undersecretary Asa Hutchinson when warned of retaliatory measures by other countries against US-VISIT by fingerprinting Americans, declared that:

> "We welcome other countries moving to this kind of system. We fully expect that other countries will adopt similar procedures."[36]

Another U.S. official declared that the U.S. has no problems if similar requirements are imposed elsewhere.

> "We are in favour of these border measures generally. If there was such a requirement we would inform our citizens and it would be up to the traveller to decide."[37]

This was not discussed in any parliament anywhere around the world, but rather in a classic case of function creep, the U.S. is leading the charge in a renegotiation of the fundamental terms of what constitutes an open society.

Innocence is Guilt
If I have nothing to hide, then why should I be worried?

The technology of biometrics is still fraught with problems. A system the size and scope of US-VISIT has never been attempted. And as the system grows, the problems grow alongside it.

The inevitable problem facing large biometric systems is that biometric prints are often unstable and fallible. Some people cannot for physiological reasons be enrolled in a biometrics system. The physical characteristics and circumstances of numerous people means the biometric will change over time. This means there must be a margin of error in biometric registration and verification. And as the system grows in size, so must the margin.

There are three distinct problems that can result from deployment of a large biometric system. The first is described as the Failure To Enrol Rate (FTER). This occurs when a person's biometric is either unrecognisable, or when it is not of a sufficiently high standard for the machine to make a judgment. The second crucial indicator is the False Non-Match Rate (FNMR) that occurs when a subsequent reading does not properly match the properly enrolled biometric relating to that individual. The third problem is where there are so many biometric identities in a system – or where the margins are set so tightly – that people are falsely identified as someone else. This is known as a False Positive.

A GAO report makes the point that the FNMR for fingerprinting can be extremely high – up to 36 percent.

If major countries follow the U.S. lead, as appears to be likely, then it is probable that within ten to fifteen years a global biometrics and data system will contain a billion identities. The potential for mass error in such a system cannot be overstated.

The integrity of the entire process depends on the integrity of each individual part. Fingerprinting is not a simple process, and matching fingerprints to an individual is even more difficult. Two percent of all humans cannot be fingerprinted, particularly if they are manual labourers. Facial recognition is even less reliable. It incurs a 15% error rate as a person ages. When combined with other information sources, the problem increases dramatically. Some reports claim that 70% of credit information is inaccurate. Criminal records bureaux are also faulty; in the United Kingdom 200 people were wrongly branded as having a criminal record. Even identifying the life-status of individuals is difficult: a system in London for the administration of social services had a 3% error rate on the death status of Londoners. Even the highly researched passenger profiling system in the U.S. has a predicted 4% error rate.

Even if you have nothing to hide, you may be wrongly identified as a suspect individual. You may be prevented from travel or prevented entry to the U.S. In December 2003 a flight from Paris was prevented from taking off because the authorities identified a 13 year old boy as a terrorist suspect. In the U.S., the *Identix* fingerprinting system led to the wrongful

imprisonment of an individual for 43 days on the charge of carrying a firearm as a convicted felon; even through the felony on his record had been committed by someone else. Another individual had his restaurant business destroyed by a false record of a criminally negligent homicide conviction.

Most interesting is the case of Brandon Mayfield. After the Madrid Bombings of March 11, 2004, Spanish National Police managed to lift a fingerprint from an unexploded backpack. They asked for international assistance in identifying the fingerprint. Three highly skilled FBI fingerprint experts declared that Oregon lawyer Brandon Mayfield's fingerprint matched. U.S. officials called it "absolutely incontrovertible" and a "bingo match."[38] As a former U.S. soldier, his fingerprint was on the national fingerprint system. The FBI searched his home, vehicles, and safe deposit box, and found a variety of items that supported their belief that Mayfield was linked to the Madrid bombings. Mayfield was imprisoned for two weeks. The fingerprint, however, was not his.

According to one law professor,

> "The Mayfield misidentification also reveals the danger that extraneous knowledge might influence experts' evaluations. If any of those FBI fingerprint examiners who confidently declared the match already knew that Mayfield was himself a convert to Islam who had once represented a convicted Taliban sympathizer in a child custody dispute, this knowledge may have subconsciously primed them to "see" the match. ... No matter how accurate fingerprint identification turns out to be, it cannot be as perfect as they claim".[39]

And yet this system is deemed infallible for use in identifying problematic individuals at the U.S. Border. According to Secretary Ridge in September 2004,

> "[B]ecause we acted swiftly and we included biometrics, more than eight million people have been admitted to the United States with biometric identification of their identity and more than a thousand people have been matched to watch lists. And again, speed of action and the hard work of many extraordinarily dedicated people have made America safer."[40]

Later in this same statement, however, the Department of Homeland Security claimed that

> "This new tool means that we have a much better idea of who is entering our country. If a traveler's finger scan hits a match on the terrorist watch list, the Department is able to stop them from entering the country at the border. Over 200 people have already been turned away from our borders using this new system."[41]

What happened to the other 800? Without open reporting of the effectiveness of the measures in US-VISIT, we cannot accurately determine the scope and implications of wrongful identification of individuals. The wrongful identification of fingerprints is likely to increase as the number of biometric identities held in the U.S. government databases increases. With 300 million visitors to the U.S. every year, this will result in the largest fingerprint database in existence. The likelihood of wrongfully matching fingerprints increases exponentially.

Even future developments in technology do not promise better results. Recently, experts have even come out against even more credible forms of identification. In a recent speech, the

father of DNA fingerprinting warned that DNA fingerprinting was increasingly problematic and inaccurate, particularly as more and more of these fingerprints are collected. He warned against collecting DNA indiscriminately,[42] even as countries around the world are amassing this information on just about anyone.

Security expert Bruce Schneier concludes that the 15 billion dollars being used to develop this system would be better spent on other projects. This is particularly so because 200,000 people illegally enter from Mexico every year, while he claims that we are merely alienating allies. He contends that the reason US-VISIT exists is only because 'politicians like big-ticket security programs'.[43] Politicians need to wake up and recognize the risks of this program and call for its dismantling.

Concluding Remarks

In interpreting a 1996 law in the light of the post-September 11 legislative environment, the U.S. Government is making fingerprints and face scans the currency of travel. Without disclosing this information you will not be able to travel. And the system will be extended to other biometrics. This process will wrongly identify individuals as being 'of interest'.

US-VISIT is not a system for countering terrorists; it is an immigration control system that will be used for an increasing number of purposes, with fingerprints being traded around the world, particularly as other countries take the torch from the Americans and establish similar systems.

This information will be used and abused, and even if you have nothing to hide, you can find yourself in prison or in shackles on a return flight to your home.

US-VISIT is the gold standard for privacy invasion.

---

[1] U.S. Department of Homeland Security. 2003. US-VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary, December 18.

[2] Federal Register. 2003. DEPARTMENT OF HOMELAND SECURITY [DHS/ICE–CBP–CIS–001] Privacy Act of 1974; System of Records, Federal Register, Volume 68 Number 239. December 12.

[3] CDT. 2004. Comments Of The Center For Democracy And Technology on US-VISIT Program, Increment 1, Privacy Impact Assessment, Center for Democracy and Technology. February 4.

[4] American-Arab Anti-Discrimination Committee, American Immigration Lawyers Association, Asian Pacific American Legal Center of Southern California, Association of Asian Pacific Community Health Organizations, Center for Democracy and Technology, Electronic Privacy Information Center, Empowering the Korean American Community New York, Friends Committee on National Legislation, Fairfax County Privacy Council, Human Rights First, Irish Immigration Center Boston, Korean American Coalition, Korean American Resource and Cultural Center Chicago, Korean Resource Center Los Angeles, National Asian Pacific American Legal Consortium, National Black Police Association, National Council of La Raza, National Employment Law Project, National Federation of Filipino American Associations, National Immigration Law Center, National Korean American Service and Education Consortium, People For the American Way, Presbyterian Church (USA) Washington Office, Privacy Activism, Privacy International, Privacy Rights Clearinghouse, Privacy Journal, Sikh Mediawatch and Resource Task Force, The Multiracial Activist, and World Privacy Forum. 2004.

Letter to Nuala O'Connor Kelly, the Chief Privacy Officer of the Department of Homeland Security, Washington: April 22.

[5] Salot, Jeff. 2004. Mounties bungled Arar file. *The Globe and Mail*, September 25.

[6] GAO. 2004. Data Mining: Federal Efforts Cover a Wide Range of uses, GAO-04-548, May.

[7] Lichtblau, Eric, and John Markoff. 2004. Accenture Is Awarded U.S. Contract for Borders. *The New York Times*, June 2.

[8] GAO. 2004. Data Mining: Federal Efforts Cover a Wide Range of uses, GAO-04-548, May.

[9] Federal Register. 2003. DEPARTMENT OF HOMELAND SECURITY[DHS/ICE–CBP–CIS–001] Privacy Act of 1974; System of Records, Federal Register, Volume 68 Number 239. December 12.

[10] Lee, Jennifer 8. 2003. State Department Link Will Open Visa Database to Police Officers. *The New York Times*, January 31.

[11] Steinhardt, Barry. 2004. Privacy and The Matrix. *Washington Post*, May 27.

[12] GAO. 2003. HOMELAND SECURITY: Justice Department's Project to Interview Aliens after September 11, 2001, GAO-03-459, April.

[13] Rachel Swarns. 2003. Report Raises Questions on Success of Immigrant Interviews. *The New York Times*, May 10.

[14] GAO, 2003, p.16.

[15] INS. 2002. Final Rule for Student and Exchange Visitor Information System Announced, Immigration and Naturalization Services. December 11.

[16] INS. 2002. STUDENT AND EXCHANGE VISITOR INFORMATION SYSTEM (SEVIS): Final Rule Implementing SEVIS, Immigration and Naturalization Service. December 11.

[17] Ferguson, Brandon. 2003. FBI Probes U. of Kansas Theft of Data. *Associated Press*, January 24.

[18] Sainz, Adrian. 2003. INS Extends its Foreign Student Deadline. *Associated Press*, January 30.

[19] Clayton, Mark. 2003. Colleges begin tracking foreign students' status. *The Christian Science Monitor*, February 4.

[20] Greene, Marcia Slacum. 2003. Computer Problems Slow Tracking of Foreign Students. *Washington Post*, March 26.

[21] Sutherland, John. 2003. Nowhere has post-9/11 paranoia struck more deeply than in American universities. Just ask Ali. *The Guardian*, September 1.

[22] Title 8 of Code of Federal Regulations (8CFR). Part 264.1.f.

[23] Swarns, Rachel L. 2003. More Than 13,000 May Face Deportation. *The New York Times*, June 7.

[24] Swarns, Rachel L. 2003. Special Registration for Arab Immigrants Will Reportedly Stop. *The New York Times*, November 21.

[25] Department of Justice. 2002. Attorney General's Remarks on the Implementation of NSEERS, Niagara Falls, New York: November 7.

[26] Department of Justice. 2002. Attorney General's Remarks on the Implementation of NSEERS, Niagara Falls, New York: November 7.

[27] Gedda, George. 2003. Powell: U.S. Aware of Registration Fears. *Associated Press*, January 29.

[28] BBC News. 2004. Visa delays 'cost US firms $30bn'. *BBC Online*, June 2.

[29] Shapiro, Gary J. 2004. Business Needs a Better Visa System. *Washington Post Editorial Section*, July 6.

[30] Khalip, Andrei. 2004. Samba Beat Keeps U.S. Tourists Coming to Brazil. *Reuters*, January 16.

[31] Ridge, Tom. 2004. Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University "Transatlantic Homeland Security Conference", Department of Homeland Security. September 13.

[32] Government of Canada. 2004. Securing and Open Society: Canada's national Security Policy, Ottawa: Privy Council Office. April.

[33] Hennessy, Patrick. 2004. Blair backs electronic border checks. *The Daily Telegraph*, June 13.

[34] Reuters. 2004. Japan Eyes Biometrics to Tighten Immigration Steps. *Reuters*, June 23.

[35] The New York Times. 2004. Visitors and Their Fingerprints. *The New York Times*, April 26.

[36] Swarns, Rachel L. 2004. Millions More Travelers to U.S. to Face Fingerprints and Photos. *The New York Times*, April 3.

[37] Waterfield, Bruno. 2004. e-Communications 'focus of terror threat'. EUPolitix, March 19.

[38] Mnookin, Jennifer L. 2004. The Achilles' Hell of Fingerprints. *Washington Post*, May 29.

[39] Mnookin, Jennifer L. 2004. The Achilles' Hell of Fingerprints. *Washington Post*, May 29.

[40] Ridge, Tom. 2004. Remarks for Secretary Tom Ridge at National Press Club, Department of Homeland Security. September 7.

[41] Department of Homeland Security. 2004. Fact Sheet: An Overview of America's Security Since 9/11, September.

[42] Jha, Alok. 2004. DNA fingerprinting 'no longer foolproof'. *The Guardian*, September 9.

[43] Schneier, Bruce. 2004. US-VISIT Is No Bargain. *eWeek*, July 6.