International and National Security Law

Immigration and Identity Fraud

*By David Morgan Frost**

The Stranger within my gates,
He may be evil or good,
But I cannot tell what powers control—
What reasons sway his mood;
Nor when the Gods of his far-off land
Shall repossess his blood.
—Rudyard Kipling

Introduction

Identity fraud presents a host of problems to various parts of society. The commercial ramifications of this problem are well-known—indeed, financial institutions continue to spend (and lose) billions of dollars in connection with identity fraud. The impact of this problem on national security issues is also matter of growing public concern.

Indeed, under the heading of "national security concerns," identity fraud rears its head as a current or potential problem in terms of physical security (*e.g*., access to buildings, airplanes, etc.); cyber-security (*e.g*., access to databases and systems); or simply routine law enforcement (*e.g*., catching identity thieves). One of the largest and most significant areas where identity fraud can impact national security is immigration.

Ironically, the government's ability to combat identity fraud may be simultaneously augmented and restricted with regard to immigration. The absence of commercial data (or, indeed, any data) on most foreign visitors makes identity verification or authentication a great deal more difficult. However, the reduced expectation of privacy at national borders—together with the more limited rights enjoyed by non-citizens—tends to improve the government's position.

I. The Problem

Islamic extremists (the primary threat to this country's security), as a group, would be but short work for American military might. The very fact of terrorism is a function of this comparative weakness on the part of our enemies, who "must therefore resort to asymmetric means" in order to attack us, which is to say that they must resort to non-conventional strategy.[1] To put things more colloquially, they have to "fight dirty." The strategy of choice is terrorism; as Mark Krikorian puts it in an admirable article in "The National Interest," the "Holy Grail of such a strategy is mass casualty attacks on America."

Before the enemy can launch his "mass casualty attacks on America," he must first be in America. To get to America, the enemy must exploit or violate our immigration policies.[2] For the terrorist-immigrant, identity fraud may be a key part of his strategy to enter and remain in the United States. Immigration is thus a front-line battlefield in the war on terrorism while identity fraud and the efforts to prevent it are among the key weapons of the contending sides.

It is difficult to find a more compelling illustration of the potential dangers posed by immigration-related identity fraud than is found in the testimony of United States Attorney Paul McNulty, of the Eastern District of Virginia, before the House Judiciary Committee Subcommittee on Immigration, Border Security and Claims and the Subcommittee on Crime, Terrorism and Homeland Security.

Mr. McNulty described a seemingly mundane crime which took place at the end of the summer of 2001:

> Victor Lopez-Flores and Herbert Villalobos were sitting out front of the Dollar Store in Arlington, Virginia, across the street from … the Department of Motor Vehicles…. The reason why they hung out there was because of the location of the DMV across the street. You see, Victor and Herbert were in the business of helping people acquire false, fraudulent, driver's licenses or ID cards from the Department of Motor Vehicles.
>
> Well, one day …, as they were sitting in front of the Dollar Store, a van pulled up. … three men got out of the van, three Middle Eastern men, and they approached Victor.[3]

A quick transaction ensued; a few forms were filled out at a nearby attorney's office and notarized by a less-than-scrupulous notary public. The men then returned with their fraudulent forms and acquired genuine identification cards from the Commonwealth of Virginia. McNulty continues:

> A few weeks later, those three men were on Flight 77, and they were the alleged hijackers of that plane that flew into the Pentagon and killed 189 people, the worst violent crime in the history of Virginia, and part of the tragedy and attack of September 11.[4]

In conclusion, McNulty testifies that the three individuals in question were among seven of the 19 September 11 hijackers who had obtained false Virginia identification cards. McNulty suggested that the need for the cards " was that, in order to get the tickets at the counter, they needed to show proof of identity. And what better proof at Dulles International Airport than a Virginia identification card or a Virginia driver's license." [5]

As alarming as McNulty's illustration may be, it does not overstate the case. In fact, immigration violations (apart from the violation implicit in simply entering the United States with the intention of supporting or engaging in terrorism) have played a substantial role al Qaeda's activities in this country. Citing an analysis by the Center for Immigration Studies, Krikorian states that of the 48 known al Qaeda operatives involved in terrorist activities in the United States between 1993 and 2001 (including the 19 September 11 hijackers), one fourth were illegal aliens, and nearly half had, at some point, violated immigration law.[6]

It would be over-optimistic to state that the ability to confirm an individual immigrant's identity would be a panacea for the terrorist problem. Nevertheless, it would be foolish to suggest that such knowledge would not make the government's job of stopping terrorists before they are able to strike a good deal easier.

The knowledge itself may be difficult to obtain. According to CNN, there are some 7 million illegal immigrants in the United States (some 70% of these from Mexico).[7] Of the illegal population, nearly 115,000 are from Middle Eastern countries.[8] The numbers are large enough to be unmanageable without the use of technology.

II. The Challenges

In a thoughtful paper on terrorism and identity fraud, Norman Willox and Thomas Regan propose enhanced identity authentication as a means of fighting terrorism. In a telling passage, the authors point out that

> ...the most difficult identification environment is where the individual who is seeking identity verification is unknown to the verifier, and has not been previously verified. This initial phase of identity verification can only occur through a knowledge-based, authentication solution. … To utilize a biometric or token based system, without first authenticating an individual, simply provides an opportunity for an impostor to link a false name, or other false identifiers with the imposter's biometrics or token.[9]

In other words, without a fairly substantial knowledge base (*e.g*., such as would be available to credit card issuers from commercial data providers), authentication of an individual's identity is a fairly speculative prospect at best.

Not surprisingly, the availability of the kind of data used for the knowledge-based authentication described by Willox and Regan is less readily available outside the United States. Accordingly, while the ability to authenticate the identities of foreign visitors seems crucial, it is not so easily done as said. The numbers referenced above—115,000 illegal immigrants from the Middle East—lend an air of urgency to the matter.

III. The Advantages

Identity authentication has become routine in America, most notably in the financial community. The ease with which it is accomplished is, as indicated above, a function of the large available knowledge base against which data provided by an individual seeking authentication can be confirmed.[10] In the case of people who have not yet been to the United States, this advantage is, quite simply, absent; most countries do not have the wealth of commercial data that exists here. Moreover, in many countries (and, notably, throughout the EU), privacy considerations make it extremely difficult for such data sets to be aggregated.[11]

There are, however, certain advantages in the field of immigration which may remedy, or at least counterbalance, the difficulties posed by the absence of sufficient data for authentication purposes. In brief, the advantages lie in the far broader authority that the government enjoys in the immigration context than with regard to domestic policies.

Americans are generally suspicious of technologies used by the government that process personal information; we tend to see such technologies as violating, or at least likely to violate, our privacy. Accordingly, efforts to implement those technologies domestically are often greeted with suspicion, if not outright hostility.[12] However, as sensitive as Americans may be about their privacy rights, there is a general acceptance of the fact that aliens do not partake in these rights to the same extent as citizens or permanent residents.

Indeed, no less an authority than the Supreme Court has held that:

> Admission of aliens to the United States is a privilege granted by the sovereign United States Government. Such privilege is granted to an alien only upon such terms as the United States shall prescribe. It must be exercised in accordance with the procedure which the United States provides.[13]

Not surprisingly, Congress has determined that an alien who fraudulently procures or attempts to procure admission into the United States or any other immigration-related benefit is inadmissible to the country.[14]

The government's discretion with regard to aliens is not limited to the question of entry. Aliens, including those lawfully admitted for entry, may be compelled to leave for a host of different reasons, including, but not limited to, domestic violence, drugs, voting, failure to comply with registration requirements, and even "any activity a purpose of which is the opposition to …the Government of the United States by … unlawful means."[15] Needless to say, an alien who engages in document fraud in connection with his immigration status is subject to deportation.[16]

The government's authority with regard to immigration and immigrants extends even so far as to compel the production by aliens seeking to enter the country of significant personal information, including a biometric. The government has taken this step with regard to certain aliens in the so-called "United States Visitor and Immigrant Status Indicator Technology Program," or "US-VISIT."[17] This program represents a tremendous first step in addressing the problem of identity fraud and immigration.

IV. A Solution

Solutions to the problem presented by identity fraud in the immigration context must, at least to some extent, include a workable system of identity authentication. The inability to say with any degree of certainty just who a particular individual really is translates into a blanket permission for illegal aliens to disappear into the country in numbers that have already become unmanageable. To illustrate the point, it need only be noted that, of the 115,000 illegal aliens from Middle Eastern countries, a mere 6,000 were (as of January 2002) the focus of post-9/11 Justice Department efforts to enforce deportation orders.[18]

Obtaining biometrics from aliens (as is done with US-VISIT), certainly provides additional information that can be used in the identity authentication process. However, US-VISIT, as currently structured, has its limitations. The information collected by US-VISIT is, in fact, not collected at all from a substantial percentage of immigrants.[19]

Furthermore, as Willox and Regan point out, a biometric alone may be inadequate for identity authentication purposes. The perpetrator of an identity fraud might simply link any plausible story to his biometric, thus making the collector of the biometric an unwilling accomplice in the creation of a new false identity.

Finally, such information as is collected by US-VISIT (currently a photo and two fingerprints) may not be used as effectively as possible. A review of the US-VISIT Privacy Policy reveals that:

> The personal information collected and maintained by US-VISIT is accessed by employees of DHS—Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and United States Citizenship and Immigration Services (USCIS)—and Department of State who need the information to carry out mission-related responsibilities. In accordance with DHS's policy . . . DHS also shares this information with federal, state, local, tribal, and foreign government law enforcement agencies.[20]

In short, the system focuses on national security and law enforcement, even to the extent of denying access to state and local officials (and others) not directly charged with law enforcement responsibilities. This, unfortunately, is a glaring defect, and limits the ability of the system to defeat immigration-related identity fraud.

If the immigrant's interactions with this country were limited to the immigration and law enforcement contexts, then the information sharing restrictions on US-VISIT would be acceptable. However, immigrants and visitors (legal and otherwise) obtain driver's licenses, pay taxes, purchase property, obtain credit and, on occasion, seek access to secure areas. In short, they constantly find themselves in a position where identity authentication is vital—and, due to the lack of available data—hardly possible.

Ultimately, if the goal is identity authentication, then, as shown by Willox and Regan, a knowledge base must be available. Moreover, it goes without saying that the knowledge base must be available to the people responsible for authentication—and this is where US-VISIT falls short.

If the data collected by US-VISIT were made available on a broader level to authorities and institutions who have a need for identity authentication, then identity fraud in immigration could be greatly reduced. The first question with regard to this solution is the one raised by Willox and Regan —the biometric by itself is not an adequate solution to problems with identity authentication. The obvious response, of course, is that biometrics collected by US-VISIT must be accompanied by other information as well (*i.e.*, biographical data from the individual's passport, visa or other travel documents required for entry). This will make it much more difficult for the alien to escape his identity or create a new one. Further, US-VISIT should be expanded to cover a larger segment of the aliens arriving in this country.

Next, the Federal Government must recognize that the drivers license is the de facto "national identity card," and pass legislation regulating the circumstances under which it can be issued and to whom.[21] State motor vehicle authorities (not just law enforcement officers) should be provided access to the biometric and biographic data collected by immigration authorities, and should be required by law to authenticate an applicant's identity before issuing a driver's license; the license should contain a biometric such as a fingerprint, and licenses issued to non-citizens should contain a clear indication of the license-holder's immigration status.

Further, credit reporting companies, financial institutions and commercial data providers should be given access to the data collected in the immigration context—in other words, that data should become part of the overall body of knowledge used for identity authentication in the commercial context.[22] It might well be expected that the companies would be willing to pay for the information, thus defraying the costs of the additional collection.

Conclusion

While civil liberties and immigration advocacy groups may be troubled by the idea of increased federal regulation of drivers licenses and more intrusive immigration policies (which might well be reciprocated by other countries), the fact is that such policies are not a departure from, or alteration of, the fundamental liberties enjoyed by American citizens. A driver's license with a biometric is hardly an intrusion and, indeed, will help to prevent not only terrorism, but simple identity theft (enough of an inconvenience in its own right).

The easy availability of personal data on immigrants to commercial data providers will, without a doubt, be rather shocking to the sensibilities of European Union privacy authorities—a fact to which the United States should reply with a resounding "so what!" As shown above, immigrants and visitors to the country have no legal right that could be said to be violated by making it more difficult for them to engage in identity fraud. Ultimately, the additional data available on immigrants will have little or no appreciable effect on legitimate immigrants, and will enhance the security of the United States.

*David Frost works in the Office of the General Counsel at the U.S. Department of Homeland Security. The opinions expressed in this article are solely those of the author.

Footnotes

[1] Krikorian, M., *Keeping Terror Out—Immigration Policy and Asymmetric Warfare,* 75 The National Interest, (2004).

[2] It but states the obvious to note that, since terrorism is not (at least from the perspective of the U.S. government) a legitimate purpose for travel to the United States, one who enters the U.S. for the purpose of committing an act of terrorism does so illegally. *See* 8 U.S.C. §1182(a)(3)(B).

[3] McNulty, P. (2002) Statement before the Subcommittee on Immigration, Border Security and Claims and the Subcommittee on Crime, Terrorism and Homeland Security of the House Committee on the Judiciary, One Hundred Seventh Congress, Second Session, June 25.

[4] *Id.*

[5] *Id., See also*, Willox, N. and Regan, T. *Identity Fraud—Providing a Solution*, 1 Journal of Economic Crime Management, Issue 1, (2002).

[6] Krikorian, *supra* note 1.

[7] Frieden, T. (2003) INS: 7 Million Illegal Immigrants in United States. *http://www.cnn.com/2003/US/01/31/illegal.immigration/.*

[8] Marquis, C., *Census Bureau Estimates 115,000 Middle Eastern Immigrants are in the U.S. Illegally*, New York Times, January 23, 2003.

[9] Willox and Regan, *supra* note 5.

[10] Id.

[11] McCullagh, D., *U.S. Twitchy on EU Data Privacy*, Wired News, Oct. 16, 1998.

[12] Blumner, R., *Fly the Suspicious Skies*, St. Petersburg Times, August 31, 2003. *See also* the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o). A Congress that might be condemned as Luddites or praised as defenders of privacy (or, perhaps, both) restricted the use of personal data in "computer matching programs."

[13] United States *ex rel.* Knauff v. Shaughnessy, 338 U.S. 537, 542 (1950).

[14] *See* 8 U.S.C. § 1182(a)(6)(C)(i).

[15] *See id.*, § 1227 (general classes of deportable aliens)

[16] *Id.*, 1227(a)(3)(C)(i). Indeed, such an individual is subject not only to deportation but to prosecution for a felony. *See* 18 U.S.C. § 1546(a).

[17] *See* Federal Register, Vol. 69, No. 2, Monday, January 5, 2004, pp. 468 – 481.

[18] Marquis, *supra* note 8.

[19] The US-VISIT program is not used on foreign nationals entering the U.S. through land ports of entry, or who seek to enter under the Visa Waiver Program. *See* Fed. Reg., Vol. 69, No. 2, p. 472.

[20] US-VISIT Program, Privacy Policy, September 14, 2004, http://www.dhs.gov/interweb/assetlibrary/USVISITPrivacyPolicy.pdf.

[21] Congress has taken a step in the right direction by requiring the issuance by the Department of Transportation in consultation with the Department of Homeland Security of minimum standards for drivers' licenses and identity cards. *See* Pub. Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004, sec. 7212.

[22] Indeed, the government might well cover a significant part of the costs of the program by selling the data.