The US/Mexico Border Crossing Card (BCC): A Case Study in Biometric, Machine-Readable ID

(Preliminary Notes)

Andrew Schulman*

Software Litigation Consultant
Santa Rosa CA
http://www.undoc.com
undoc@sonic.net

March 30, 2002

The terrorist attacks of Sept. 11 were quickly followed by calls for a national ID card in the United States. Though the best-known advocate of a national ID card is now Larry Ellison, CEO of Oracle, efforts by the American Association of Motor Vehicle Administrators (AAMVA) to "produce a uniform, secure, and interoperable driver's license/ID card to uniquely identify an individual" are more likely to hit their target.[1]

Many groups and individuals, from all parts of the political spectrum, have expressed concerns over the privacy implications of a possible national ID card. However, the discussion feels stuck in an abstract consideration of security/privacy tradeoffs. Often, both opponents and supporters of National ID (and of similar proposals, such as widespread facial recognition) make it appear that there is some kind of privacy vs. security sliding scale that individuals or societies can fine-tune to a desired setting.

Rather than engage in what are often sterile "privacy vs. security" debates over proposed technological solutions to the Sept. 11 crisis, let's first see if the proposed technology is even going to *work* (and work in the Sept. 11 sense, i.e., would implementing this or that proposal have stopped the terrorists from getting on the planes?). Privacy advocates often abdicate discussions of practicality to security vendors, and in fact often take the vendors at their word for claims of how technology will work; vendors can then sometimes rely on the dire predictions of privacy advocates for a kind of scarecrow marketing.

To assess what National ID for the US might look like, and how effective it might be, it makes sense to first look at an *existing* ID program run by the US government. This study will examine the biometric, machine-readable Border Crossing Card (BCC), a joint project of the US State Dept. and the US Immigration and Naturalization Service (INS, a branch of the Justice Dept.).

About four million new BCCs, also called Laser Visas, *micas*, or *pasaportes locales*, are held by Mexican citizens, allowing them to cross into the US for up to 72 hours, within 25 miles of the border (65 miles for Tucson AZ); BCC holders are not supposed to work in the US. On October 1, 2001, all older, non-machine-readable versions of the BCC became invalid. The BCC is probably the largest mandatory biometric ID program run by the federal government (there is also a new biometric version of the so-called "green card," but older versions of the card are still valid). The card manufacturer, Drexler Technologies, calls it the "World's Most Secure ID Card" and the "World's Most Counterfeit Resistant Card"[2] – so, clearly, this is being held up (at least by the vendor) as a good test case.

National ID has, before Sept. 11, traditionally been proposed in the context of illegal immigration from Mexico. To extent we have history of semi-rational debate on this topic, it involves the Mexican border, and the widespread employment of unauthorized workers from Mexico and Central America. Past proposals for National ID have been in the context of illegal immigration, not only for border control, but also to weaken the US jobs "magnet" with an ID card that all employers would require of their new hires.[3] Some of the same advocates for a National ID to combat illegal immigration, such as Sen. Diane Feinstein (D-CA), are today advocating a National ID, to combat terrorism. Concerns have been raised that terrorists can enter the US via its 2,000-mile (and in some ways unprotectable) border with Mexico.[4]

Using the US/Mexican border as a way to study the larger issue of using IDs to secure the US against terrorists, is not meant to imply that immigration control is necessarily an appropriate way to fight terrorists. While this view is held for example by Phyllis Schlafly ("It should be repeated over and over again: The terrorism threat is from illegal aliens who are allowed to live in our midst"),[5] this

would, for one thing, overlook the US's own history of homegrown (and typically anti-immigrant) terrorists.

• The study will look at the BCC with a "process" view: how is a card initially issued, when and where is it checked, how is it checked, what is it checked against, how is it enforced. More specifically:

  • How are the cards *issued*? Assuming the cards themselves are counterfeit-resistant, how easy or difficult is it to fraudulently obtain a genuine laser visa? What documents must be supplied when applying for the card? What background checks are performed?

  • *Where* are the cards checked? Just on entry to the US? How about on exit, as part of a program to control visa "overstays"? How is the card's 72 hour/25 mile/no work policy enforced? How much card-checking and enforcement within the US itself, away from the border, is required to secure the border? What are the penalties for violations? (You can't say much about a policy without knowing about the penalties for non-compliance.)

  • *How* are the cards checked? Are the cards visually inspected, or are they swiped through a card reader? Are the on-card biometrics being employed? How do officials verify that the cardholder and card match? Against what criminal databases is each card checked?

This paper will be able to only give a hint of the complexities involved in even this relatively small biometric ID project. It seems likely that these complexities would be magnified many times over in a National ID to be issued to perhaps 200 million or more people.

National ID advocates frequently claim – as, come to think of it, do some National ID opponents, particularly of the "Mark of the Beast" school[6] – that we really *already have* a National ID, in the form of the Social Security Number (SSN) or state drivers' licenses. National ID advocates say that this *de facto* National ID merely needs to be made more secure.

One of points that emerges from a study of the BCC, however, is that the gap between the existing state of affairs and a true national ID system is enormous. Under National ID, all cards would need to be machine readable, card readers (and, likely, fingerprint readers) would need to be widely deployed, and the cards would need to be checked against a national database. This is a far cry from our current desultory visual inspection of cards.

The INS has in the past dismissed concerns that the BCC has broader implications. According to the *Washington Post* (Feb. 18, 1998), an INS spokesman said that "linking a travel document used only by Mexicans to a national ID card for Americans is 'kind of a leap.... It's technology that's available to the credit card companies and anybody who wants to pay for it.'"

But the US State Dept. says that its joint BCC project with the INS "has given us the opportunity to conduct important research on a potential biometric visa for the future" and goes on to discuss facial recognition software also being tested.[7] And, according to the US Consulate General in Cuidad Juarez, Mexico, "the future may require that all visas eventually be placed on these machine readable cards." Thus, the BCC is already seen as a kind of pilot project for all visas (of which the US issues about 30 million each year[8]).

What, though, do BCCs, or even visas in general, have to do with ID for US citizens? As shown in this study, it is difficult to enforce the BCC's 72 hour/25 mile/no work policy without also checking IDs of *non*-immigrants within about 100 miles of the border; after all, BCC holders are not wearing special

"BCC" tattoos on their foreheads. As also explained below, a BCC holder must carry the card at all times; it will be seen that would really need to be a feature of any *effective* (i.e., not just for show) National ID.

Because one can't tell by looking if someone is a citizen (and if an employer for example acts as if they can tell, it's discrimination), situations requiring ID from non-citizens will, in fairness, require ID from everyone. The discussion below of employment eligibility verification shows that, more generally, effective ID for non-citizens is — unless we have discriminatory "profiling" — a slippery slope to mandatory ID for everyone. Thus, anti-discrimination can be, ironically, a slippery slope to wholesale (as opposed to selective) privacy invasion.

In sum, the US/Mexican border, and Border Crossing Cards in particular, provide an useful real-world way to think about and discuss National ID. This makes sense; it is often said that borders and immigration are at the forefront of social issues.

The Border Crossing Card (BCC)

The United States has issued over four million new machine-readable biometric Border Crossing Cards (BCCs), form DSP-150, also called "laser visas," to Mexican citizens for the purpose of multiple short trips to the US. Starting on October 1, 2001, all old versions of the BCC became invalid, and holders of the old BCC were turned back at the US border. According to INS commissioner James Ziglar, about 1,600 visitors are being turned back each day for lack of the new card.[9] The new cards started to be issued in April 1998; since then, on average, the US has issued about 100,000 cards each month. Over 15% of applicants for the card are not approved.

The biometric BCC is a joint project of the State Dept. and the Immigration and Naturalization Service (INS; an agency of the Justice Dept.), and is mandated by by Section 104 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996.[10]

The IIRIRA required that every BCC issued after April 1, 1998 contain a biometric identifier such as a fingerprint, and be machine readable. However, widespread opposition from the business community, which feared that the security features of the new system would result in less border crossing — and hence fewer shoppers and reduced low-cost labor availability — produced several delays in the system's implementation. Congress would likely have approved another year's delay, had it not been for the Sept. 11 terrorist attacks.

The Border Trade Alliance (BTA) sent an appeal, dated Sept. 10 (!), 2001, asking for implementation of HR 2276 to extend the BCC deadline by another year. Rep. Silvestre Reyes (D-TX), himself a former Border Patrol sector chief, had been pushing to delay the BCC switchover to "prevent an economic disaster" (*Dallas Morning News*, Sept. 28, 2001).

Interestingly, having declined to extend the deadline, and thereby finally having allowed the new card to become mandatory for BCC holders, Congress is now apparently again rethinking its decision. The Enhanced Border Security Act and Visa Entry Reform Act, approved by the House, and now before the Senate, includes a re-extension of the BCC deadline to Oct. 2002. Declared Rep. Solomon Ortiz (D-TX): "Merry Christmas to the Southwest border from the House of Representatives ... We know the economic damage the refusal to extend the deadline has done to the border."[11]

Clearly, US businesses near the Mexican border are going to be hurt when some shoppers can't

cross the border until they get the new biometric BCC. It seems more likely (though unspoken in the Congressional debate) that the real opposition to implementing the new BCC has come from employers of BCC holders who now can't get to their jobs. As is discussed below, while BCC holders are not supposed to work in the US, many apparently do; attempts to implement the BCC law have led to an informal NIMBY (not in my backyard) movement by their employers.

The delays in, and local opposition to, implementing the BCC switchover – even after Sept. 11 – perhaps holds some lessons for the likely resistance there would be (not all of it high-minded) to National ID.

The Laser Visa

Like the older BCCs (form I-186 and I-586; see Figure 1 and Figure 2), the new "laser visa" (DSP-150; see Figure 3) shows the cardholder's name, photo, and fingerprint on the front, but the back of the new card has a mirror-like optical stripe. Embedded in the optical stripe is the person's biographical data, digital photo, fingerprints, and a control number.[12]

Figure 1 — Old BCC, no expiration (I-586)

Figure 2 — Old BCC, with expiration (I-586)

Figure 3 — New BCC (DSP-150)

Figure 4 — New "green card" (I-551)

There is also a new biometric Permanent Resident Card (see Figure 4); this is the famous "green card," though it hasn't actually been green since 1964. As noted above, this study focuses on the less well-known BCC in part because the new biometric green cards are not mandatory. An interesting look at the new green card as a prototype for a National ID appeared in the Feb. 2002 issue of *Harper's* (Gregory Dicum, "A Study in Green: My National I.D. Card, Your Civil Liberties"; according to Dicum, fake copies of the new green card can be purchased in Tijuana for $500).

There were apparently rampant counterfeiting problems with the old BCC. As noted by the *Washington Post* (Feb. 18, 1998), "At least five versions of the card have been issued, all but the latest with no expiration date. Many have decades-old photographs and are easily used by imposters. Over the years, the Border Crossing Card also has become one of the most counterfeited U.S. documents."

The new card's manufacturer, the LaserCard division of Drexler Technology (Nasdaq:DRXR, LaserCard.com), states that the LaserCard "places huge technological and financial barriers in the path of counterfeiters." According to the *San Diego Union-Tribune* (Sept. 29, 2001), a Drexler VP states that, "because each card's digital information is tailored to each cardholder, it would be highly expensive and impractical for a counterfeiter to try to reproduce them.... 'It's not something that you can make in a basement.'"

Indeed, as noted above, and as shown in the figures, Drexler calls its product the "World's Most Secure ID Card" and the "World's Most Counterfeit Resistant Card." (While the figures happen to show the Permanent Resident Card, the same technology is used for the BCC.)

Figure 5 — From the vendor's web site, LaserCard.com

One key feature of the card is that the cardholder's photograph is digital, and part of the media itself; it is not pasted in. There is 4.1 megabytes of Write Once Read Many (WORM) optical storage on the card, allowing an audit trail with up to 35,000 updates. Any unauthorized attempt to alter the card is supposed to lead to either a clear audit trail or destruction of the card.

Interestingly, Drexler also is responsibility for Italy's smart-card ID, the Carta d'Identità Elettronica (CIE). According to *Wired* (Dec. 2001), though, Italy had only issued about 200,000 CIEs, though the goal was to issue a CIE for all 55 million citizens before 2004.

Issuing the Card

To use the BCC as a way of seriously asking how a National ID would work, we should first look at how the new biometric BCCs are issued. Even if the BCC experience held no direct lessons for a National ID, thinking through the processes involving the BCC – how is it issued?, when is it checked?, how is it checked?, etc. – would still give us a better handle on what the phrase "National ID" really means. The monolithic abstraction "National ID" needs to be broken down into its component parts in order to understand it.

The Interview

How does someone get a BCC, or if they already have an old BCC, how do they get one of the new biometric cards?

They must have an in-person interview. No phone or mail (and certainly no internet) applications are accepted. This makes perfect sense. If we are interested in having secure ID, we have to have some confidence in the process by which the ID is handed out in the first place. Each request for a National ID – all 200 million or so of them — would have to be carefully handled. (Contrast for example the initial SSN project, in which over 35 million SSN cards were generated, largely by the post office, in 1936-37.[13])

Figure 6 – Also from the vendor's web site, LaserCard.com

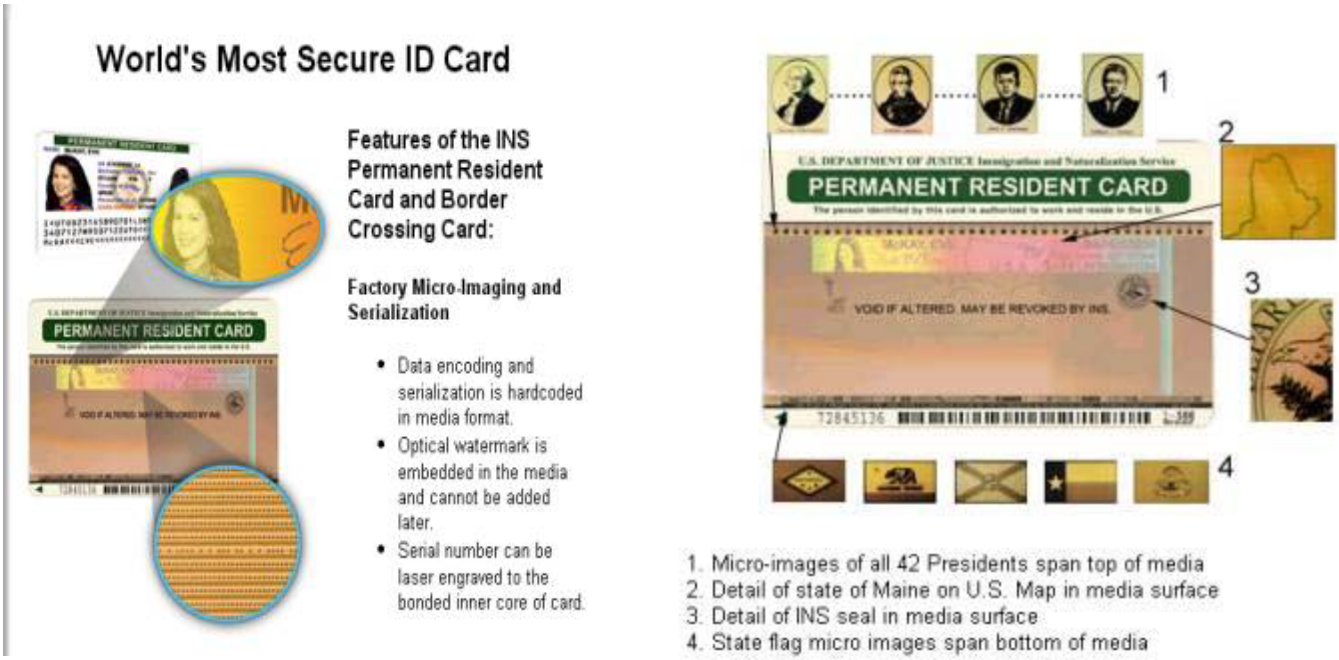

Figure 6 - Also from the vendor's web site, LaserCard.com

This has led, however, to very long delays. In early October 2001, AP was reporting that US consulates in Mexico were not able to schedule appointments until March 2002. Already, scams are being reported, such as a business in a Brownsville TX strip mall that charges over $100, supposedly to help set up application appointments, after which one still has to wait the same number of months.

The consulates could in theory hire a lot more people, but quick hiring of personnel responsibility for security decisions leads to "insider" problems (see below). It has also been noted that some consulates might be easier to get a card off of than others ("consular shopping").

When someone has their BCC interview at a US consulate in Mexico, they must present their ID (see "Breeder Documents," below), and have their photograph and fingerprints taken. They must present proof of a fixed address in Mexico, such as utility bills and/or pay stubs. While these would appear to be easily counterfeitable, only about 70% of regular BCC applicants get the card; applicants are most commonly rejected because they cannot prove a fixed address. Obviously, there is some genuine deterrance. At the same time, one in-depth study from the US Commission on Immigration Reform states: "Several informants we interviewed in both El Paso and in Juarez averred that the purchase of false pay stubs, birth certificates, employment letters, utility receipts, and the like was not uncommon among persons who desired a BCC but not could not otherwise obtain the necessary documents."[14] While this statement is from 1994, the switchover to the biometric BCC would not in itself affect the availability of fake pay stubs and the like.

A criminal background check is run on all BCC applicants. However, this apparently wasn't the case as recently as 1995, when a GAO investigation found that routine background checks were not being conducted, "in order to promite 'facilitation' across the border."[15] It is worth noting that you can have the best biometrics in the world, and they wouldn't help at all with this problem; it has to be addressed separately.

Even when criminal background checks are being run, it matters a great deal *what* is being checked. Do you take the name profered by the applicant, and run that through the system to see if anything turns

up under that name? Clearly, applicants could be presenting incorrect names. Therefore, their biometric itself (e.g., fingerprint), not the name, must be used as a database lookup. This is discussed in more detail below (see "1:1 vs. 1:N Lookup").

There's one interesting twist to the BCC interview: the role of *maquiladoras* (foreign-owned factories along US border in Mexico). According to the *Houston Chronicle* (July 22, 2001), the US "effectively delegates responsibility for administering the special visas to foreign-owned factories in Mexico.... Daunted by the task of replacing the old documents and issuing new ones, the border consulates began allowing maquiladoras to do a lot of the paperwork and applicant vetting…. some Mexicans work in a maquiladora long enough only to get a laser visa and then disappear." The article notes that "an 'interview' … seldom consists of more than typing each applicant's data into a computer. Later, the information is cross-checked against United Stats law-enforceement records to eliminate those who have run afoul of the INS. Photos are taken for applicants' identification cards, and each applicant submits to a fingerprint scan. The whole process takes less than 15 minutes per person" According to researchers at Tijuana's Colegio de la Frontera Norte, of the more than 40,000 workers commuting daily to jobs in neighboring San Diego, at least 4,000 do so with a laser visa; "Those using their visas to earn a casual income in the United States effectively subsidize the payrolls of companies employing their relatives in maquiladoras."

Interestingly, in contrast to the 30% rejection rate noted above, the rejection rate for those applying via maquiladro is only 1% (*Migration News*, August 2001). This would seem to be an area ripe for fraud.

Even if the maquiladoras' rapid rate of 15 minutes per person is taken as a model for vetting this valuable ID, extrapolating this to a National ID in the US means that about 3,000 employees would need to work for ten years, just to conduct the interviews. If it is thought that the National ID has limited usefulness until everyone is carrying one, then cramming all the interviews into a single year would require something like 30,000 employees.

If we perhaps can't extrapolate from BCC issuance to a National ID, note that a Sept. 1997 Social Security Administration report estimated it would cost $10 billion, and take 10 years, to issue tamper-proof social security cards with pictures, fingerprints, work history and earnings for the 270 million social-security accounts. For $4 billion, the agency said it could issue simpler IDs that resemble credit cards.[16]

Breeder Documents

It was noted above that, during the BCC interview, someone must present ID. To get ID, you must present ID. Documents, on the basis of which other documents are issued, are called "breeder" documents. The birth certificate is the classic breeder document.

What documents must be presented during the BCC interview? The applicant can either present an old-style BCC along with a recent photo ID, such as a Mexican passport, or "In lieu of a passport, a voter registration card is the preferred identity document." If applying for a first-time BCC, the applicant must have valid Mexican passport. "We were willing to accept the Mexican Certificate of Nationality, issued by SRE (the Mexican Foreign Ministry), but the Ministry decided that the Certificate was not intended for general issuance."[17]

What, then, are the requirements for a Mexican passport? Men must present a birth certificate,

photocopies of their military card, and photocopies of another picture ID. Married women must present their birth certificate and marriage certificate. Single women present a birth certificate and a photo ID.[18]

The mention of the Mexican voter registration card is interesting because it has been claimed that this sophisticated piece of biometric ID, issued to 60 million voters, was successfully used in the 2000 elections to prevent voter fraud. Since this was the first Mexican election since 1929 not won by the PRI, this is a significant claim that deserves further research.[19]

At any rate, birth certificates appear to be at the root of the ID system. Any insecurities in birth certificates percolate up through the system. Though we're talking about Mexican birth certificates here, it is worth noting that, according to Gideon Epstein, chief foreensic document analyst with the INS, birth certificates are issued by 7,000 different jurisdictions in the US.

The *New York Times* (May 29, 2000) ran a lengthy article by Renwick McLean on the birth certificate problem in the US:

> "the birth certificate to be the soft underbelly of America's interior defenses against illegal immigration.... the birth certificate can open the door to other documents... The birth certificate is the document most frequently presented as evidence of American citizenship by first-time applicants for a passport, the State Department says.... California, home to 40 percent of the 5 million to 6 million illegal immigrants that the immigration service estimates live in the United States, is particularly vulnerable to birth certificate fraud. An official at the Ventura County recorder's office said that to get a certified copy of someone's birth certificate, 'you just need to know the name on the birth certificate and the date of birth.' The cost is $12, and the wait about 15 minutes, she said.... While studying the issue as a member of the Commission on Immigration Reform, a bipartisan group formed by Congress in 1990 to study United States immigration policy, Michael S. Teitelbaum was so shocked to hear how easy it was to get someone's birth certificate in California that he decided to try it. He went to the county clerk-recorder's office in Orange County and requested the birth certificate of someone he knew was born in the area. Within 15 minutes, he had a certified copy of the person's birth certificate. 'I basically walked out of there shaking my head in disbelief,' said Mr. Teitelbaum... Now that office says that people asking for birth certificates in person may be asked to show picture identification. But all that is needed by mail is 'the person's full name, date of birth, and a credit card number,' an official said.... In most states, however, the full names of both parents, including the mother's maiden name, must be provided to get a birth certificate. But critics say that the system is only as strong as its weakest link, because a birth certificate from a state with loose restrictions can be used to establish residency and employment eligibility in any other state. And even in the strictest states, the information required for obtaining a birth certificate can often be found easily, critics say. One way is to scan the obituary pages of a local newspaper and write down the background information on a person of the appropriate age. Since most states do not match death and birth records, or do so very slowly, experts say, illegal immigrants assuming the identity of the recently deceased face little risk of detection. The fraudulent acquisition of valid birth certificates is only part of the problem. The I.N.S. says that birth certificates are vulnerable to counterfeiting, largely because there is no single national standard for them. Instead of one version, thousands of different but valid birth certificates flow from the more than 7,000 local and state agencies authorized to issue them. That makes detection of counterfeits difficult, Mr. Hesse said. In 1994, the Commission on Immigration Reform recommended that the federal government adopt one standard design for all certified copies of birth certificates. Almost six

years later, no such design exists. The commission also recommended a nationwide system for matching birth and death records..."

Any National ID system in the US would first have to fix the birth certificate problem: for example, have at most a small handful of standard birth-certificate formats, so that examiners gain a better sense of whether they are looking at a genuine certificate or not; and check all birth-certificate requests against death records, to prevent the *Day of the Jackal* identity vampirism (identity theft of the dead). Some states allow persons born there, whose births were never registered, to create a "delayed certificate of live birth";[20] this is perhaps another security hole. Sometimes baptismal certificates are accepted as substitutes for birth certificates; these seem easy to come by (for example, Ahmed Rassam obtained a valid Canadian passport on the basis of a stolen blank baptism certificate; *Coyotes*, Ted Conover's travelogue on illegal immigrants, mentions in passing the apparently successful use of a Mormon Certificate of Baptism as ID).

Given this well-known breeder document problem, then, it seems odd that Larry Ellison, interviewed by Steven Levy ("A Techie's Solution," *Newsweek*, Oct. 29, 2001), cannot imagine any way that terrorists could spoof his National ID card:

"What if terrorists or criminals learned to 'spoof' the system? Is there a danger of putting too much trust in such a system?"

"I do this for a living. If you can explain to me how the system can be spoofed, I'm ready to listen."

"Any system can be compromised."

"I don't know how it can. Maybe there's someone smarter than I am and knows more about this than I do, but I can't figure it out."

It's good to have counterfeit-resistant cards, but is this really where the vulnerability is? Yes, if the card is easy to counterfeit, then this is an obvious hole. But even if you make an ID card nearly impossible to counterfeit, then the vulnerability moves: you now have to ensure that it is not easy to get a valid card, on an invalid basis. As long as insecure documents such as birth certificates are the root of the ID system, then securing higher-level documents like the BCC seems to be at best a partial measure, and at worst an illusion.

The Insider Problem

Another way the system can be subverted, without attempting to manufacture the cards themselves in one's basement, is through bribery. A Dept. of Justice (DOJ) audit report on "Document Fraud Records Correction" (Sept. 1996), discusses several cases in which INS employees sold legitimate INS documents to illegitimate recipients. The DOJ audit report notes that "The temptations and rewards for selling these official documents are great"; an old BCC would apparently sell for about $325. The newer laser visa has many more steps in its production process which should make such insider jobs more difficult to pull off, but the same DOJ audit also pointed to "inadequate inventory records and security for controlled documents and for equipment," cases in which equipment went missing, lax security with respect to unauthorized database access, uncertainty over how to deal with fraudent database entries, and so on.[21]

The DOJ inspector general, noting the doubling of INS personnel along parts of the border since 1993, warned in 1997 that "Experience in other contexts indicates that massive law enforcement hirings

may be accompanied by increased police corruption because of the great susceptibility of new recruits to temptation or because corners may be cut in screening and training the new hires."[22]

The DOJ inspector general also noted that "The mix of low paid employees, easy money in big sums, and relatively low risks makes for an extraordinarily volatile and risky situation…. An INS or Customs employee is not required to do very much or take much of a risk in order to earn a bribe. One or two bribes a year can effectively double an employee's income."

Even if the vast majority of INS employees are honest, clearly there is a potential "insider" problem. In computer security, it has become clear over the years that the old firewall model of the "hard crunchy shell with the soft, chewy inside" (as described by Bellovin and Cheswick in their *Firewalls and Internet Security*) makes the unwarranted assumption that all insiders are to be trusted.

Delays and the Sticker Problem

We've just seen that quickly adding more employees, as part of a campaign to beef up security, can ironically lead to additional security problems among susceptible new recruits. Another example of the same phenomenon – adding security can, in certain circumstances, reduce security – has to do with the complex process needed to manufacture the new counterfeit-resistant BCCs.

A Drexler VP was quoted earlier to the effect that the new card is "not something that you can make in a basement." But this also means that producing the cards is a fairly slow process. According to Drexler's annual report, it is currently producing about 200,000 per month.[23] As noted above, over the life of the program, about 100,000 cards have been issued per month. (To be unfair, at this rate it would take over 100 years to issue a similar card to everyone in the US.)

Partially as a result of the time-consuming production process, and also because of the in-person interviews needed to apply for the card, there is a substantial backlog. Long delays are not simply a matter of inconvenience: they can also subvert the whole security process. Between the time of someone's approval for a card, and the time they actually receive their new security-enhanced card, officials at the border will accept their old "mica" BCC, if it bears a sticker indicating that they have been approved for the new card (AP, Oct. 1, 2001). (An INS press release from Sept. 2001 states that the stickers were due to expire on Dec. 31, 2001.[24])

The use of stickers on older cards raises obvious questions about how counterfeit-proof such stickers are. (A national ID card would obviously have similar backlog and "catch up" issues, lasting many years longer.)

The DOJ is already familiar with this problem from the history of replacing old green cards. An OIG audit report from August 1997 notes a "6 months to 1 year waiting period between replacement card application and receipt of a card. *The delays undermine the integrity of the identity card system*, as the INS must use easily counterfeited temporary stamps so applicants may obtain employment and public benefits in the interim.... INS Forensic Document Laboratory personnel suggested to us that a sticker with a holographic label affixed to temporary documents could improve the security of these documents. In our judgment, a reduction of the waiting period from application to card receipt would be the best solution."[25]

While referring to green cards, this clearly shows the security dangers of long delays in the card

issuance process: “The delays undermine the integrity of the identity card system.” Delays are not simply a matter of inconvenience. When these delays are themselves caused by security measures, it nicely points up the way that increased security measures can themselves sometimes undermine security.

Interim Conclusion on Card Issuance

We’ve seen that, even assuming the card itself is counterfeit-resistant, there are several holes in the card issuance process: it appears to be readily spoofable with invalid downstream “breeder” documents such as birth certificates; the *maquiladora* program seems open to abuse; it’s unclear if criminal background checks are being done on identities, rather than on given names; there is a potential for bribery (caused partly by overly-rapid hiring to beef up security); and delays in producing secure cards necessite the use of insecure temporary stickers.

This set of potential holes matches to some extent the findings of the Office of the Inspector General (OIG):

> “The new biometric identification card, known as the laser visa, has shown to be more tamper-proof than previous documents. However, many problems reduce the effectiveness of the program, such as the lack of laser visa processing equipment at consular posts in Mexico, an inadequate criminal database against which to check applicants, and delays with biometric card production.”[26]

A National ID program would need to carefully address each of these issues. Most of them are not really technical, but social issues. They cannot be finessed with biometrics.

Checking the Card: How, and Against What?

Okay, we’ve been issued our BCC. Now what do we do with it?

(Actually, we are skipping over an important step here: delivery of the card from the manufacturer to the cardholder. Is there anything that could go wrong here? Yes, the *San Diego Union-Tribune* (March 16, 2001) reported that a DHL delivery truck, carrying 6,000 BCCs worth as much as $9 million on the black market, was seized in an armed heist. Smugglers were expected to obtain many of the stolen BCCs, “and if you want to get across the border they will look through their piles for one that has a photo that looks like you.” This apparently works, despite the biometrics on the card, because of implementation problems at the border that we’ll discuss in a moment. Even with these problems, though, you would think that the stolen card numbers could be retired, and detected if anyone tries to use them. By the way, it later turned out that the heist was an inside job involving a DHL employee and Tijuana police.)

Earlier, we saw that there has been widespread local opposition to the BCC switchover, and that Congress may even repeal it. In the meantime, however, BCC holders are required to have the new biometric, machine-readable card. What happens as we approach the border with our BCC, for example at the Tijuana/San Ysidro crossing just south of San Diego?

Swiping Cards, Reading Fingerprints

The amazing thing, after all the talk of hightened security, is that, if we “look American,” we’re waved through with barely a glance at our ID. Anyone who can pass as an American citizen, based

perhaps on some fairly narrow prejudice as to what an American looks like, won't have their ID swiped through a card reader. You might be asked what you were doing in Mexico, and how long you were there, but that's about it. Given the long lines of both cars and pedestrians (there are about 800,000 legal crossings *each day* from Mexico into the US, about 16% of them on foot), there's not much more that the border inspectors can do. It's important to note that long delays are not just a matter of inconvenience: in late October, two children reportedly died from carbon monoxide asphyxiation while waiting in line to cross from Ciudad Juarez to El Paso; others have become dehydrated from long waits in the sun.

What if you present a BCC? How are the biometrics employed? Section 104 of the IIRIRA said, "an alien presenting a border crossing identification card is not permitted to cross over the border into the United States unless the biometric identifier contained on the card matches the appropriate biometric characteristic of the alien."

Yet, several trips through the Tijuana/San Ysidro crossing in February 2002 showed that while BCCs were being swiped through card readers, there were no fingerprint readers, so the inspector has maybe 45 seconds to see if the picture on the card looks like the cardholder. At least in primary inspection (there's a separate building if you get bounced over to "secondary"), there is no automated way to see that the cardholder matches the card.

The same thing was observed in an AP story (Oct. 1, 2001) describing the Tijuana/San Ysidro crossing:

> "Inspectors there have machines that can read basic data from the new cards with a small, tabletop device. They do not have the advanced readers that show a digitized photo and fingerprint.... Some border points still lack the machinery to read the cards. Without the machines, US authorities must eyeball them the same way they did the old ones, in essence rendering the new security features meaningless."

According to the *New York Times* (Oct. 29, 2001), in El Paso, the INS had yet to install card readers. Rep. Silvestre Reyes stated, "They haven't identified the equipment they need. They don't even know yet much it'll cost." Richard Duran, who oversees the El Paso crossing at the Bridge of the Americas, "said the installation of the machines to read the laser visas might actually lengthen inspection times because inspectors checking cars full of passengers would have to swipe several visas through the machine" rather than just one for the driver.

Without fingerprint readers, the card really can't be verified against the cardholder. It was noted earlier that the widest form of misuse of the old non-machine-readable BCCs, and a major reason for the switchover to the new card, was not counterfeiting the card, but having a valid card that wasn't yours. According to a US Commission on Immigration Reform report from 1994, "While almost no one attempts to cross with an altered or fraudulent BCC, a fair number of people seem to attempt to cross with someone else's card, presumably betting on lax inspection of the photograph it bears on the part of INS personnel at the port of entry."[27] For example, a card can be legally acquired, then sold to a document "gang," who can then rent the card out to someone who looks like the picture on the card, who can use the card to cross the border, and then mail the card back (what happens then, if the person is found inside the US, without the BCC, is discussed below in the section on "interior enforcement").

Without fingerprint readers, then, it appears as if the new BCC with its sophisticated Drexler technology, solves the wrong problem. Instead of making it more difficult for the wrong person to use

a valid card, instead it was made more difficult to create illegitimate cards.

Why does the INS apparently not have enough machines to read the new machine-readable cards, and not have equipment to compare every BCC holder's fingerprint with the biometrics on their card?

Like many sagas involving the INS, this one appears to be long and complicated. According to the INS, Congress and the General Accounting Office (GAO) won't give it the money. Each reader cost only about $3,000; the INS probably needs around 1,000 of them. According to the New York Times (Sept. 29, 2001), the INS

> "asked Congress for money to buy the machines two years ago but was turned down because the agency did not know exactly what kind of equipment it needed, said Russ Bergeron, a spokesman for the immigration service. Now the agency knows what it needs to scan the border cards but does not have the money, Mr. Bergeron said.... The immigration service hopes to get financing for the scanning machines as part of a budget request that the Justice Department, the agency's parent, is putting together to help deal with the terrorist attacks, Mr. Bergeron said."

But why would Congress be so stingy over a few million dollars? Embattled INS commissioner James Ziglar has repeatedly asserted that Congress had declared a "moratorium" on machine readers to go with its machine-readable cards? In fact, it appears that Ziglar is referring to a moratorium on further deployment of the separate IDENT system, and that Ziglar would like to get 1,100 IDENT workstations (with a two-fingerprint recognition system) to also check BCCs.[28]

So what is this moratorium on IDENT? This will be discussed below in more detail (see "The Central Database"). In essence, at the time of the nine serial murders in 1998-9 by the so-called "Railroad Killer," Rafael Resendez-Ramirez, it was found that Resendez had been repeatedly apprehended by the Border Patrol illegally crossing the border, and then voluntarily returned to Mexico, unaware that he was wanted by law enforcement. INS employees had been contacted by caught by police about Resendez, but had apparently not placed a "lookout" for him in the IDENT database.[29] IDENT is the INS's database that maintains information on every apprehension; it includes fingerprints for each apprehendee; IDENT also includes a "lookout" section in which, for example, criminals and recidivists (those with a dozen or more illegal crossings) are noted.

In July 1999, the House Committee on Appropriations raised doubts about IDENT's ability to identify wanted criminals apprehended by Border Patrol, and in particular asked why IDENT was not integrated with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) database; the committee directed that the INS suspend further deployment of IDENT until it submitted a plan for integration of IDENT with IAFIS. The congressional conference report for the DOJ's 2000 appropriations included a moratorium on further deployment of IDENT.[30]

While it is commendable for the INS to want to use an existing system such as IDENT to do double-duty for checking BCCs, it sounds passive aggressive for the INS to apparently insist on using technology on which a moratorium has already been placed, and then to turn around and complain that it can't intelligently use the biometrics on the BCC because a moratorium has been placed on the technology.

The current troubled state of the INS should make us cautious about extrapolating from its experience with the BCC to the US as a whole. It may seem as if we have picked, for our case study in

National ID, a notoriously "incompetent" agency (though, as noted towards the end of this study, there are structural reasons for the INS's difficulties, rooted in the US's deeply conflicted attitude toward illegal immigration). Surely the INS's inability to get card readers to go with its machine-readable cards is of a piece with the INS's approval of student visas for two notorious dead hijackers, Mohamed Atta and Marwan Al-Shehhi (*Boston Globe*, March 13, 2002). What can this troubled agency really tell us about National ID?

But the INS is not alone in having biometrics that are all dressed up with nowhere to go. For example, the California State Auditor in Oct. 2001 reported that while it had been collecting fingerprints for the past 20 years, California's DMV "does not obtain the benefits of such technology" because many of its fingerprints are of poor quality; the state takes thumbprints, but basically does nothing with them; the state has photographs, of course, but it also fails to use these sensibly.[31]

National ID advocates point to such ironies as *precisely why* we need a national ID system. It is often said that "we already have National ID, in the form of drivers license and social security cards; we just need to fix it." The author will point how many times that week he had to show someone his drivers license. But *show* is the key word here. How many times have they had their drivers license, not quickly eyeballed, but *swiped* in a card reader, which is linked back to a central database?

It definitely does happen. See an interesting *New York Times* (March 21, 2002) article by Jennifer 8. Lee, "Finding Pay Dirt in Scannable Driver's Licenses," that describes how bars in Boston are buying $2,500 Intelli-Check systems – presumably like the ones that INS doesn't have – and using them to make sure that patrons are over 21, and then also using the scanned-in personal data for marketing). The technology is cheap enough, and becoming cheaper: Moore's Law is often what drives the adoption of new ID systems.

But a National ID would require that the equipment that the INS had not managed to acquire in the year 2001, despite passage of the original law in 1996, would need to available nearly everywhere. How realistic is this? Or, perhaps the lesson of the Boston bars is that this will only happen if card reading is turned over to the private sector, who would also be allowed to use personal data for marketing as they see fit.

In any event, there is an enormous difference between having someone take a quick glance at an ID card, and feeding it through a card reader, linked to a central database, and connected to a fingerprint reader (or other biometric input device) that matches the cardholder with the card. It may possibly be that National ID is a good idea, but if it is, it would represent an enormous change from the current situation. National ID advocates frequently downplay the significance of their proposal with claims that "we already have national ID, we just need to fix it." That the INS has the cards, but not the equipment, should tell us something – and not just that the INS has problems. It tells us that we currently have nothing at all like National ID.

1:1 vs. 1:N Lookup

Let's say that there are fingerprint readers. What exactly are they checking? If it is simply that the cardholder's fingerprints match the fingerprints stored on the card, that seems like an easy enough task. The new BCC not only has a visible photo of a fingerprint, but also contains a machine-readable representation of the fingerprint – this, in a way, was the whole point of the new cards. This type of verification involves a 1:1 check: does this cardholder match this card? The accuracy rates for such a check are pretty good, even though we're dealing with non-discrete, real-world data.

If you read through the claims made for biometric ID cards such as the BCC, though, it becomes clear that the popular (and congressional) expectation, and the promises upon which the technology is sometimes sold, is a little different from this mere 1:1 check.

For example, what is to keep someone from applying for multiple cards under different names? Note that many names having multiple forms and spellings: Arabic names for example are transliterated, and Mexicans frequently but not always use both the mother's and father's last name. The promise of biometrics is that you can basically discard the given name, or ID number, and use the fingerprint itself, for example, as a database lookup: has anyone with this fingerprint already applied for a card? This is a 1:N check, using real-world data as the database index. How good is it, when N is large? In a large population, how difficult is to balance false negatives (catch everyone who needs to be caught) against false positives (don't create 10-hour waiting lines)?

How long would it take to uniquely identify one of the four million BCC holders, given only the fingerprint of a BCC holder? This may not seem to be an issue. After all, when someone presents their BCC, you can first do the 1:1 check that the cardholder matches the card, and then use the card number as a database lookup. But what happens when someone isn't carrying a BCC? This was one of the big problems with the BCC: "Mexicans headed for big cities in the north are also using such cards to cross the border, then mailing the cards back to their homes in Mexico before proceeding north to look for work. If they are captured, the aliens tell the INS that they slipped across the border illegally."[32] To have any hope on stopping this mis-use of the BCC, all apprehendees would need to have a 1:N check done of their fingerprints (stored in IDENT) against the BCC database.

If such 1:N checks are widely used, then the ID card itself becomes irrelevant; your fingerprint *is* your ID. How feasible is this for the 200 or 250 million people who would have a National ID in the US? Not just technically feasible, but also socially: would it be able to overcome the "Mark of the Beast" overtones?

One alternative is to just have a (presumably) smaller database of the people you *don't* want in, rather than a larger database of the people who you do. This has been one of the approaches of facial-recognition companies, which assert that — had facial recognition systems been in place in Portland ME on Sept. 10 and the morning of Sept. 11, when security cameras at ATMs, gas stations, and the airports caught last images of some of the terrorist hijackers – the attacks could have been prevented. What this claim overlooks, however, in addition to the unreliability of many facial-recognition systems, is that your "keep out" images must already be in your watchlist database.[33]

The Central Database

We've seen *how* the BCC is checked. The next question is, *what* is the BCC checked against?

The earlier discussion of database "lookouts" in the case of the "railway killer" ought to sound familiar. This was an earlier version of the database-linkage debate fueled by the Sept. 11 attacks. On April 26, 2001, Mohamed Atta was stopped in Broward County FL for a traffic violation and was given a citation for driving without a license; on May 2, he acquired a Florida drivers license. Yet his visa had expired. If we could somehow rewind history, we would want the routine stop on April 26 to have led to something more than a citation; we would want the drivers license to be refused on May 2 because of the expired visa. Perhaps without the drivers license, he wouldn't have been able to board Flight 11. It seems so simple: if only one database had known what the other database knew.

This is really the heart of the National ID idea. It's not so much the cards, as the idea of a single, centralized database. The card would just be a handle into a national database. According to Larry Ellison, "The single thing we could do to make life tougher for terrorists would be to ensure that all the information in myriad government databases was integrated into a single national file" (*Wall St. Journal*, Oct. 8, 2002). In an amazing speech to Oracle employees, available on the web,[34] besides asserting that we've made it impossible for the CIA and NSA to do their job, that we've made it impossible for the government to protect us, Ellison states that we have "too many databases," that it's impossible to correlate and cross-check them, that there really is no such thing as a federal "watch list," but instead a disparate collection of lists like IBIS (Interagency Border Inspection System) and NAILS (National Automated Immigration Lookout System).

We saw earlier (see "Swiping Cards, Reading Fingerprints") that the INS doesn't have all the machines it needs to read and fingerprint-verify BCCs, because it wants to use IDENT workstations, and that it can't use IDENT because of a congressional order that it first figure out how to correlate IDENT and the FBI's IAFIS. What all this means is that a BCC may be checked against the BCC database (of course, there's no such check when the card is just eyeballed by a harried border inspector), but it is likely that there is little integration with the other databases maintained by the INS. Precisely in the way National ID advocates complain, someone could "waltz" into the US on a BCC, even if they're known to be wanted (though not necessarily under the same name) in another database like IDENT or IAFIS.

IDENT maintains biometric information on every INS apprehension. According to its developer, the Belgian company Keyware (apparently working with Lockheed Martin), "IDENT is an exclusive automated biometric identification system that uses advanced fingerprint and facial identification technologies to search for matches among over 400,000 'wanted person' files and more than 2,000,000 files for people who have been previously detained."[35] The system was originally adapted from the US Navy's Deployable Mass Population Identification and Tracking System (DMPITS), which in turn was originally designed by FingerPrint USA, for use in POW-type camps holding mass refugees from Haiti and Cuba.[36]

This sounds like exactly what would be wanted for National ID. Yet we saw earlier that there was a hole in the system in the Resendez "railway killer" case. There has been debate over what the problem was, exactly. In some accounts, it appears the problem was as much one of training INS employees to properly use IDENT. In any case, clearly the biometrics by themselves don't solve the problem.

In March 2000, the DOJ announced a plan to link IDENT with the FBI's database, but said it could take five years and more than $200 million to complete. Furthermore, "because the INS Border Patrol agents apprehend approximately 1.5 million aliens a year entering the United States illegally, INS requires a process that can record and identify a high volume of individuals in a very short period of time, generally two minutes or less."[37] It is not clear how this can be matched up with IDENT, since a Keyware official has bragged that the IDENT system delivers "response time in *days*, not weeks" for law-enforcement collaboration (*Federal Computer Week*, Nov. 14, 2000; emphasis added).

Thoroughly assessing the call for a single national database would also require an in-depth look at the history of database linkage in the US, including not only other INS programs such as "Systematic Alien Verification for Entitlements" (SAVE), but also the history of widening use of the SSN.

Checking a card against a single national database, rather than against an individual agency database (and even more in contrast with simple checking of the card against the cardholder), raises impor-

tant security issues. Any type of central database check requires a network connection; what happens if this connection goes down, or is compromised? One touted security feature of the current BCC is precisely that it's *not* checked against a central database. Richard Norton of the International Biometric Industry Association (IBIA) testified at a Senate immigration subcommittee hearing that BCCs are "virtually immune to compromise, and the process can be conducted without having to establish a network connection to a central database."[38]

Another security issue is the insider problem: there would presumably be huge financial incentives for insiders to alter records in the single national database. The INS has a history of bribery leading, not just to documentation fraud (INS employees improperly providing ID cards such as BCCs, or even blank INS documentations), but also to *database fraud*: paying an INS employee to make entries or deletions in databases such as SAVE and NAILS.[39] Oracle's advertisements boast, "Can't break it; can't break in," but this is a different issue. As a database becomes more important (and the single national database Ellison proposed would be the mother of all databases), the incentives grow for its maintainers to make improper changes. Any national ID would require sophisticated audit trails and employee monitoring.[40]

Still, the basic idea behind a single national database seems simple enough: in the case of the BCC, someone provides the card at the border, the card is swiped, they put their finger on a reader which ensures that they match the fingerprint on the card, and the immigration officer immediately knows everything the US government knows about this person. That, even with a lot of the component technology having already been deployed, we are still quite far from this scenario (recall that simply linking with IDENT is estimated as a five-year project, and note that Section 1008 of the PATRIOT Act only calls for a feasibility study on IAFIS use at consulates and ports of entry), tells us that this scenario would actually represent an enormous undertaking.

It also would have dramatic social implications, discussed at the end of this paper. For now, it's simply worth noting that such a large undertaking would inevitably have to be used for more than keeping terrorists off airplanes, and for keeping housecleaners and nannies from getting to their jobs in the US. The drive to use Ellison's single national database for all sorts of goals — from the "war on drugs," to eliminating welfare fraud, to tracking deadbeat dads, to combatting tax evasion, to stopping illegal gun sales, to stopping underage drinking and smoking – would be irresistible. Even if every one of these goals is good, we can question whether American society is really ready for this level of consistency and accountability.

Checking the Card: Where and When

We've seen *how* the BCC is checked, and we've looked at some implications for a National ID. Now, *where* is the BCC checked? This may seem at first like a foolish question, since obviously Border Crossing Cards are checked when someone crosses the border. But that this is in fact not at all obvious becomes clear as soon as we ask whether BCCs are checked when *leaving* the US, as well as when entering; and when we ask the related question of how the card's 72 hour/25 miles/no work policy is enforced.

Exit Controls and Overstays

The quick answer here is that the BCC is checked when someone enters the US, but not when they leave. There is in fact essentially no check of any kind when someone crosses from the US into Mexico. On several recent (Feb. 2002) trips across the border crossing at Tijuana/San Ysidro, the long pedes-

trian ramp leading from the US to the Mexican side was equipped with a single private security guard, from Holiday International Security.

Well, why should there be any checking when someone leaves the US? We only care when someone comes in, right?

This sounds obvious, but recall, for one thing, that the BCC limits the cardholder to staying in the US for only 72 hours. How can the cardholder's compliance be verified, much less enforced, without checking people when they leave the country?

An "automated entry and exit control system" was, according to the Section 110 of the IIRIRA of 1996 (discussed earlier), supposed to be developed by 1998. This system was supposed to collect a departure record from every non-citizen leaving the US, and each departure record was supposed to be matched-up with an arrival record to determine who, upon leaving, had overstayed. The system was also supposed to be able to enable online searching to locate the entry records of those who had overstayed. Notice that such a system doesn't by itself provide any means for actually finding people still in the US who have overstayed. Basically, it would allow catching them only when they try to exit. In any case, this system clearly does require checking everyone when they leave as well as when they enter the US.

BCCs were supposed to play a role in this entry/exit control system. Having a BCC lets cardholders avoid filling out an I-94 arrival/departure card. At the same time, the BCC is intended to be used not only for entering the US, but also upon depature. Because the cards are machine readable, they can — assuming card readers are in place — be swiped upon exit from, as well as entry into, the US, thus giving the INS some handle on the problem of cardholders overstaying the 72-hour limit. According to the US Consulate General in Ciudad Juarez, Mexico, the new cards "will be used to facilitate the implementation of Section 110 of IIRIRA requiring an automated exit and entry control system to be established by the INS."

On other hand, as noted earlier, people using the BCC to work in the US may mail their cards back home, and present themselves as having illegally crossed the border, rather than as having legally crossed the border and then overstayed. In this they, they will still be returned to Mexico, but they won't lose their BCC. But this would also diminish the BCC's effectiveness for exit controls, except if the card itself were basically ignored, and a person's biometric always relied upon for the database lookup (see "1:1 vs. 1:N Lookup," above).

Like the biometric visa itself, mandated by Section 104 of the IIRIRA, the entry/exit controls mandated by Section 110 were also opposed by the business community; for example, the Travel Industry Association of America, the US Conference of Mayors, and the US Chamber of Commerce opposed Section 110 in the name of "efficient borders." A fellow of the Alexis de Tocqueville Institution predicted that, if entry/exit controls were implemented, "the borders between America and its neighbors would effectively close.... Americans can say good-bye to inexpensive produce in the markets," and further denied that entry/exit control has anything to do with countering terrorism.[41] The Senate voted three times to repeal Section 110, and while the House voted against repeal, the system has not been implemented.

Now that the Sept. 11 terrorist attacks have highlighted the question of visa overstays, and many of those who opposed Sections 104 and 110 of the IIRIRA in the name of "efficient borders" are now

angrily asking how the INS could have possibly allowed some of the terrorists to overstay their visas, and how it could have "lost track" of them. As noted several years ago by *Migration News* (Aug. 1998), a superb publication from UC/Davis, "Many Congressional representatives continue to criticize illegal immigration in general, and then criticize the INS when it engages in enforcement actions that affect their constituents."

In 2000, Congress passed the "Border Improvement and Immigration Act," under which Section 110 was amended so that entry/exit controls won't be required at airports until 2004, and at land borders with Mexico and Canada until 2005.[42] Even after the terrorist attacks of Sept. 11, and the attention they drew to the issue of visa overstays, Section 414 of the PATRIOT Act calls merely for the integrated entry/exit data system of Section 110 of the IIRIRA to be implemented "with all deliberate speed and as expeditiously as practicable," and makes the "Office of Homeland Security" part of an entry-exit "task force."

Thus, after five years, and even after Sept. 11, there is really nothing being done to even learn about overstays, much less enforce the rules against them. One reason, as noted above, is opposition from the business community, which sees exit controls as contrary to the spirit of NAFTA, and "free trade" generally. Another reason may be that visa overstays are too small a problem for such a large solution as exit controls. In one test of an automated I-94 system in Philadelphia with selected US Airways flights to and from Munich, 99.6 percent of the 50,896 entry-exit records matched, i.e., only about 214 travelers did not leave as required (and some of these may have left through other airports, or a land border).[43] Meanwhile, EDS testimony on the cost of implementing an entry/exit system points out that this would be a very large undertaking:

> "We assume that at least 700 million traveler arrival and departure records will be captured in the system annually. For example, the automated I-94 pilot demonstrates that an arrival record for a non-citizen traveler uses 360 bytes of storage and the departure record uses 152 bytes. Extrapolating this estimate to the annual volume of non-citizen travelers suggests that a terabyte of storage may be needed for a nationwide system. To put some perspective on the magnitude of this number, the information in this system at the end of one year would be equal to the amount of data stored in the US Library of Congress."[44]

When suggestions are made for large-scale projects such as National ID, we should ask why other large ID projects, required by law, have not been implemented. Sometimes our data-retention eyes are bigger than our stomach.

Address Registration

As noted above, an entry/exit system would at best let the INS know whether a given cardholder has overstayed a visa such as the BCC. It provides no help in actually *locating* a "visa jumper" or overstay. Yet, the INS is roundly denounced for having "lost track" of the Sept. 11 terrorists, and of "illegal immigrants" generally. For example, a guest editorial in the *Seattle Times* (Oct. 4, 2002) discusses ways to "learn the whereabouts of millions of illegal immigrants that the Immigration and Naturalization Service admits it has lost track of."

What does this mean, "lost track"? Is the INS supposed to know the whereabouts of each of the millions of non-citizens present in the US?

Technically, yes. The Immigration and Nationality Act (INA) requires that all noncitizens must

notify the INS within 10 days of a change of address. The form to use in reporting an address change is AR-11 (INA § 265(a)).[45] This does include the BCC, though of course BCC holders are not supposed to be in the US for more than three days.

Address registration can also be required during an emergency. During the Iranian hostage crisis, the DC Circuit Court of Appeals in *Narenji v.Civiletti* (1979) upheld the Attorney General's authority to order nonimmigrant Iranian students to report to INS district offices and to demonstrate their lawful status.

However, the INS has stopped reminding non-citizens that they ought to notify the INS of their address and effectively has ceased administering the address-notification requirement. Although failure to give the written notice of address required by INA § 265 is a ground for removal, an INS operating instruction provides that failure of an alien to comply with the § 265 requirements regarding notification of address "shall not normally serve as the sole basis for initiating prosecution" or removal proceedings."[46]

The Alien Registration Act of 1940 and Internal Security Act of 1950 had required the annual registration of all aliens living in the US, but this annual registration requirement (whether or not one had moved) was suspended in 1981. At the time, the INS apparently "acknowledged that it didn't much matter, that the alien registration requirement had been mostly for show, that the registration cards had never been matched up with the aliens' files anyway."[47]

Thus, the US is, for better or worse, a long way from knowing where non-citizens here. There are probably practical reasons for this.

Yet a National ID card would probably require address registration. Just as Sept. 11 was followed by angry questions over how INS could have lost track of the hijackers (some of whom had given "Marriott Hotel, New York" as their address), presumably the first terrorist attack to be committed (perhaps by another Timothy McVeigh, Unabomber, or anthrax mailer) under the regime of a National ID, would be followed by angry questions about why can't we get our hands on this guy: we've got a National ID card now; you mean we don't know where each cardholder is at least supposed to be living? For the system to be more than a "mostly for show," feel-good activity, this would eventually have to evolve into something like residential registration offices in Germany;[48] hotels and other forms of lodging would presumably need to take the ID number of each occupant, as happens in some countries. It's difficult to see how, without such extreme measures, any handle could be kept on someone's whereabouts.

In the meantime, note that we *already* have a national address registration, in the form of the New Hire Database (see "Employment and Employer Sanctions" below).

"Papers, please": Interior Enforcement

We've seen that the current system provides no way of enforcing the BCC's 72-hour policy, or of locating those who overstay. What about the 25-mile policy?

For one thing, just as INA § 265 ineffectually requires that non-citizens inform the INS of address changes (see above), INA § 264(e) requires that they carry their ID with them at all times. This includes the BCC.

What good does this do in enforcing the BCC? According to the INS:

> "When passing through *the Border Patrol checkpoints typically located at least 25 miles from the border*, those Mexican BCC holders not in possession of an approved Form I-94 will not be allowed to pass and may be processed for administrative action."[49]

In other words, in addition to the border itself, there is in essence a "second border." For example, on I-5 at San Onofre CA, about 70 miles north of the border (and near the former Nixon home in San Clemente), there is a 24-hour inspection of cars traveling between San Diego and Orange County.[50]

The INA gives the Border Patrol broad authority to conduct searches within a "reasonable distance" from the border. The Supreme Court has generally held that such searches do not violate the Fourth Amendment, and that probable cause is not required to justify a stop or search. The INS has defined "reasonable distance" to be *100 miles*. The Supreme Court has given fixed checkpoints (as opposed to roving patrols) very wide discretion.[51]

Why is there this second border? One reason would be to attempt to enforce the 25 mile and 72 hour BCC policies. More important, the Border Patrol is responsible for locating immigrants who have bypassed an official port of entry, and snuck in somewhere along the 2,000 mile border. As noted elsewhere, the practice of mailing one's BCC back home during an overstay means that some BCC violations will appear as if they were simple cases of someone sneaking under a fence or across the Rio Grande, for example, without any ID at all.

It turns out, in other words, that simply checking IDs at the border is insufficient. Most illegal immigration doesn't actually happen at the border, but inside the country, when someone overstays their visa, for example. Or, to put it differently, the border turns out to be much thicker (100 miles wide) than one would have thought. At least according to some, within this area, pretty much anyone can be stopped and asked to present ID. The phrase "deconstitutionalized zone" has been angrily used (see, for example, *US v. Newell*, 1975, quoted in a dissent to *US v. Guerrero-Barajas*, Jan. 2001[52]) to refer to this 100-mile strip. The phrase "Driving While Mexican" has also been used (*New York Times*, Jan. 26, 2000). If you live within this area, and fit a certain profile, we today have one aspect of National ID, in that you can be stopped at any time and demanded, "papers, please."

In his discussions of a National ID, Larry Ellison dismisses the idea that the card would have to be carried at all times, and could be demanded at any time: "I'm not saying that police can stop you and ask you for your ID card when you're walking your dog. I'm saying you must produce the ID when you're going into a secure location like an airport" (*Newsweek*, Oct. 29, 2001).

But a National ID would have to be carried and presented much more frequently than Ellison thinks. For one thing, if we're just worried about terrorists getting on planes, we may end up "fighting the previous war"; for example, perhaps we now (again) need to be more worried about truck rentals. Consider too Mohamed Atta's traffic-violation stop in Broward County FL: since this incident has been cited as an apparently perfect illustration of the failures of our current disjointed ID system, then (if we now try to replay the events of 2001 with a hypothetical National ID in place) obviously whatever ID Atta had with him that day would have to have been linked back to the central database. This is effectively the same thing as having to carry a National ID at all times. Or, since Atta actually was cited for driving *without* proper ID, then whatever biometric the police might have chosen to use from him, would have to have been used as a database lookup; again, this is functionally equivalent to having to present one's ID at any time.

Again: if the biometric itself is the ID, and if it acts as an index into single central database, then in effect we carry ID at all times, despite reassurances that National ID wouldn't represent a "papers, please" scenario. The protection against having to present our biometric at any time would then be the Fourth Amendment's restrictions on stop and search. Racial and ethnic "profiling" show that parts of the population are already not truly covered by the Fourth Amendment, and statements by National ID advocates such as Ellison that we've "made it impossible for our government to protect us"[53] sound an awful lot like traditional protests against the Fourth Amendment and its Supreme Court interpretation as an impediment to law enforcement.

The BCC presents another example of how one form of ID — if its policies were actually enforced – would require everyone to have at least some form of ID. How could the BCC's 25-mile policy be enforced without also checking IDs of *non*-BCC holders within the 100-mile "second border"? It's not as if BCC holders have "BCC" tattoos on their foreheads. Since BCC holders can't be assumed to be always carrying their card, then either ID checking must be outwardly discriminatory based on some "profile," or everyone's ID must be checkedable. Note that it is really only ethnic profiling – i.e., a double standard — that keeps everyone in this area from having to carry ID at all times. In his book *No Justice*, David Cole makes a reasonable case that "privacy" and Fourth Amendment protections are currently based on inequality.

As with the discussion of address registration, these notes on interior enforcement are obviously half-baked; these parts of the study require more work.

Employment and Employer Sanctions

It appears so far that the exit controls that would be necessary to even begin to enforce the 72 hr. BCC policy have been wildly unpopular, and are unlikely to be implemented any time soon, and that the "second border" measures necessary, *inter allia*, to enforce the 25 mile BCC policy have possibly already produced a civil-liberties nightmare within 100 miles of the border, all probably without keeping BCC holders within the 25-mile perimiter.

How about enforcing the BCC's no-work policy? According to Adelita Sandoval, who lives in Tijuana and cleans houses in San Diego, "The pass allows you to cross to the other side in order to spend money, but they don't want you to come over to earn money. So you have to convince them that you're doing one when you're really doing the other." Such workers, "dressed attractively — even elegantly — for what would be, in fact, a workday of scrubbing floors and toilers." *La migra* (the INS) "almost never even ask to see our papers. They look at our hands."[54] Note that the INS is not looking at their hands for the fingerprints; it is looking to see if the BCC holder's hands look like those of a middle-class shopper, or a worker. Real-world biometircs? *La migra* is also reputed to be alert to whether someone wearing fashionable clothes looks like they really "belong" in those clothes; literally the "fashion police."

For the most part, though, the BCC no-work policy would be enforced as part of a larger effort that gives the appearance of preventing unauthorized work by non-citizens, essentially by deputizing employers are immigration officers.

As the reader probably knows, employers in the US are supposed to check the ID of every new hire, and fill out an I-9 form which is kept on file. If they fail to check ID, or if they accept obviously fake ID, they can face fines. This policy is known as *employer sanctions*. According to the INS:

> "The landmark 1986 Immigration Reform and Control Act (IRCA) legislation changed forever the concept of traditional immigration interior enforcement, making it unlawful to employ an individual without verifying the identity and employment eligibility of an employee at the time of hire, thereby shifting emphasis from the alien violator to the employer."[55]

Meanwhile, several sectors of the US economy depend vitally on the work performed by illegal immigrants, and by legal immigrants, such as BCC holders, who are not supposed to be working. The "Nannygate" cases of Zoe Baird, Kimba Wood, and Linda Chavez were newsworthy examples of the prevalence of unauthorized work in the US. It is generally held that the construction, hotel/restaurant, garment, agricultural, and meatpacking industries would collapse without their large reserve army of "undocumented" workers.

While the crucial role of undocumented labor in the US shows that this is all something of a farce, the fact remains that every new hire is supposed to have their ID checked. (This should make the earlier discussion of address registration sound a little less unrealistic than it probably did. Given that we already have employment registration, does residential registration really sound like such an impossibility?)

It is sometimes asked, in all seriousness, why check everyone's ID, if we're only interested in keeping out unauthorized workers? Why not just check the ID of non-citizens? Hello?! It seems obvious, but this mistake underlying these questions was made a while back by the INS:

> "In the mid-1990s, the INS began to experiment with a system to verify employment eligibility prior to hiring. Employers voluntarily communicated I-9 form information for prospective or new hires to an office in Washington, DC, which then verified that the documents supplied, such as alien employment authorization numbers, were authentic. *However, only non-U.S. citizen employment eligibility was verified. The documents of individuals claiming to be U.S. citizens were not verified.* All an unauthorized alien had to do was to borrow bona fide documents or purchase forged ones and claim that he or she was a U.S. citizen. Firms would duly record the corresponding information on I-9 forms, which could be inspected. But alien workers falsely claiming U.S. citizenship could circumvent the verification system in this way."[56]

This illustrates the point made earlier, that ID systems present slippery slopes. Disciminatory double standards are not just discriminatory: they create loopholes. To truly enforce the BCC and other no-work policies, everyone's ID needs to be checked.

While I-9 forms are hardly ever checked by the INS, which keeps the process miles away from constituting any kind of national employment database, it is worth noting in passing that the US *does* have a national employment database, connected not with immigration, but with the important goal of locating deadbeat dads and making them provide financial support for their children. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 created a "National Directory of New Hires" (NDNH), better known as the New Hire Database. Within twenty days of each new hire or rehire, the employer must report the SSN, name, *and address* of the new hire, along with the employer's name, address, and employer ID number. While there are also state databases, the NDNH exists because 30 percent of child-supprt cases involve parents who live in a different state from their children.[57] It would be worth studying this system in more detail, to see whether it meets its goal of arranging child-support payments, whether there have been pressures to use the system for additional purposes, and so on.

Getting back to employer sanctions, while the large amount of under-the-table employment in the US indicates that they have not been a rousing success, have they at least perhaps helped enforce ID systems such as the BCC?

Ironically, the effect of employer sanctions, as currently implemented, has been almost the opposite. A GAO report from 1999 observed that allowing a wide variety of documents to fulfill I-9 requirements had resulted in widespread counterfeiting.[58] Peter Andreas, who has written several important works on immigration and the US/Mexican border, states:

> "The perverse impact of the law was to generate an enormous business in fake documents. Since IRCA did not require employers to check the authenticity of documents, they could simply continue to hire illegal workers at minimal risk – as long as the documents looked genuine and they made sure to fill out the proper forms. In the short term, IRCA helped to defuse some of the domestic pressure to 'do something' about illegal immigration. But the law's failures would help make immigration control an even more daunting task in years to come."[59]

And:

> "the primary impact of the poorly designed and minimally enforced employer sanctions was to create a booming business in fraudulent documents. IRCA's perverse consequences helped set the stage for a powerful backlash against illegal immigration in the 1990s, most acute in California."[60]

What went wrong? Clearly, the law really didn't deputize employers as immigration officers, as claimed facetiously at the beginning of this section. But for the employer sanctions to have any effect on unauthorized employment, it would have had to. Because there were no sanctions placed on an employer who accepted anything but the most obviously fake ID, the result was, as Andreas notes, to create a booming market in plausibly fake ID. To have had any other result, the system would have required that there be some verifiable form of ID, and ubiquitous card readers with which to do the verification: eyeballing a cards wouldn't be good enough. This sounds just like the National ID, so National ID advocates may want to view the experience of employer sanctions as another reason for adopting their proposals. But notice that suddenly we see another scenario in which the card would be mandatory: not just to get on an airplace, but also to get a job (shades of Revelation 13:16).

Preventing non-citizens from working would require rigorous document checking by employers (or by third-party background checking services, such as Interquest). The 1999 GAO report quoted above states:

> "According to an INS official in Los Angeles, that office has already seized counterfeit versions of the new green card INS began issuing in April 1998. According to this official, the counterfeit cards do not have all of the security features of the new INS green card. While they are easily detectable by trained INS employees, they will appear genuine to untrained employers."

In other words, ither each employer, or the third-party services, would need machine readers for this scheme to work. Note that background-check companies right now appear to depend on the employer having accurate I-9s, and aren't placed to verify the ID itself.[61] This appears to even be true of services such as www.i9check.com that specialize in I-9 forms.

Why is there so little incentive for employers to properly inspect employee IDs? Fines are gener-

ally sufficiently minimal – especially given the money saved by paying below US minimum wage, avoiding overtime pay, and avoiding environmental, health, and safety regulations — that some employers view any possible sanction as "the cost of doing business." The INS has only a small number of workplace inspectors. *Migration News* (Jan. 1999) relates two telling points:

> "The INS did not request more inspectors to enforce employer sanctions in the FY99 budget; in its FY98 proposal, 130 more inspectors were requested, but Congress did not provide funding for them. In spring 1998, when the INS in Georgia tried to enforce sanctions laws against onion growers, Congress intervened and the INS agreed to stop its raids so that Vidalia onions could be harvested."

There is a long history of immigration doubletalk in the US, where a supposed "flood" or "invasion" of illegal aliens is deplored out of one side of the mouth, while agriculture and other businesses are guaranteed the undocumented workers they want out of the other. A prime example is the so-called "Texas Proviso" to the INA, which states that "for the purposes of this section, employment (including the usual and normal practices incident to employment) shall not be deemed to constitute harboring" an alien. This amazing exemption, written in 1952 apparently by then Sen. Lyndon Baines Johnson, was eliminated in 1986, but its spirit lives on. No-work policies are enforced sufficiently to help keep down wages, but not enough to seriously reduce the flow of undocumented labor.

Enforcement of the BCC's no-work policy would likely come only as part of a larger reduction in employment of unauthorized workers in the US, and would represent a major social and economic change (not necessarily a desirable change, either). Even the small amount of enforcement we currently have has entailed going through the motions of seeing ID from every new hire, producing new incentives for false documentation. This charade shows some of the obstacles that, for better or worse, would stand in the way of a genuine national ID.

Results

Has the switchover to a biometric, machine-readable BCC made a significant change in the use and misuse of these cards?

The answer appears to be that it hasn't. One might say that this is only because implementation has been half-hearted: machine-readable biometrics on the card, but no fingerprint readers to use them; no exit controls; and other seeming mistakes detailed earlier. Perhaps if everything were done right, then the cards would work. Yet we've also seen how adding security features can sometimes reduce security (long manufacturing times for ID cards spawn the use of insecure temporary stickers). It is also possible to fix the wrong problem, for example by making BCCs counterfeit-proof while leaving birth certificates and other breeder documents untouched.

We have to ask, *why* has implementation been so seemingly half-hearted? The reasons are really social, political, and economic; a technical fix is unlikely to change the fact that (as noted in more detail below) immigration policy in the US is the result of conflicting interests. For example, we've seen that significant business opposition has delayed exit controls for year after year, and had delayed the BCC switchover. National ID advocates would need to show why this time it would be different; how would National ID overcome the same opposition that has (for better or worse) hampered previous ID efforts? Why would this one not end up becoming another expensive and yet largely ineffectual show?

Probably the best that can be hoped for from an ID like the new BCC is that it would speed up the

processing of regular users, so that inspectors could spend more time on a small set of selected individuals. This is more realistic than hoping that the card itself would provide security. However, such "fast lane" cards would be abused by determined terrorists, unless the interview process, by which one gets the card in the first place, were far more sophisticated (with much more rigorous inspection of "breeder documents") than, e.g., the current BCC interviews.

Calling efforts to reinforce the border ineffectual doesn't mean that they have no effect. Rather, they have been ineffectual in the way that alcohol Prohibition was, or that the "war on drugs" is. Some "Prohibition" effects have already been noted, such as the way employer sanctions helped to solidify and professionalize the fraudulent-document business. Another Prohibition effect has been the way that installation of IDENT has apparently led to higher fees for *coyotes,* who are in the business of smuggling people across the border. Indeed, the coyote business itself was created by efforts to prevent unauthorized border crossing.[62] Higher fees for coyotes means also more money available for bribes. (Note to libertarians, however: not every rule or regulation has "Prohibition" effects.)

Efforts to control border crossing appear to simply move the problem (if it is a problem) from one place to another. For example, "entry without inspection" (EWI) was seen as the big problem for a while – recall media images of people sneaking through fences – but attempts to solve this problem, by making EWI more difficult, had the unintended consequence of increasing misuse of documents like the BCC. David Spener notes that "Making 'entry without inspection' more difficult raises the salience of the use of fraudulent immigration documents or the misuse of valid documents," and he gives the use of BCCs to get to jobs in the US as a key example.[63] (Note to libertarians: not every rule or regulation has unintended consequences.)

Alternatively, if the focus swifts to more carefully checking the IDs of each person entering at an official port of entry into the US, then illegal immigration is pushed back to "entry without inspection." As noted in an August 2001 GAO report, the current INS strategy is to

> "incrementally increase control of the border in four phases to make it so difficult and costly for aliens to attempt illegal entry that fewer individuals would try.... The primary discernable effect of the strategy, based on INS' apprehension statistics, appears to be a shifting of the illegal alien traffic. Between 1998 and 2000, apprehensions declined in three Border Patrol sectors, San Diego, CA, and El Paso and McAllen TX, but increased in five of the other six Southwest border sectors. The extent to which INS' border control efforts may have affected overall illegal entry along the Southwest border remains unclear, however.... although INS has realized its goal of shifting illegal alien traffic away from urban areas, this has been achieved at a cost to both illegal aliens and INS. In particular, rather than being deterred from attempting illegal entry, many aliens have instead risked injury and death by trying to cross mountains, deserts, and rivers."[64]

In addition to shifting illegal immigration to more dangerous, less controllable areas, INS's strategy (combined with the 12:1 wage disparity between the US and Mexico) has, ironically, tended to make illegal immigrants stay *longer* in the US than they had intended. According to Douglas Massey, codirector of the U. of Pennsylvania's Population Studies Center:

"The massive militarization of the border has not had the effect of deterring Mexicans from coming to the U.S. but has deterred them from going home. What we've seen since 1993 is a sharp decline in the probability of return migration once Mexicans are in the U.S."[65]

Strictly enforcing immigration laws would raise prices of many goods and services, and/or would lower profits for many businesses. On the other hand, legalizing currently unauthorized workers might well have same effect. Thus, the current situation of widespread — but not total — non-enforcement suits the needs of US society.

All US immigration law is the result of compromise between competing interests. Even after Sept. 11, the same set of competing interests revealed in study of BCC also would apply to a national ID. Given that the much smaller BCC system has so many holes, how could we expect national ID to "work" in the sense that advocates want, i.e., well enough to prevent future Sept. 11-type attacks? National ID would inevitably represent a compromise, not so much of "security vs. privacy," as one of security vs. the many US interests that depend on lax enforcement of the laws.

The IRCA of 1986 is a perfect example of such compromises. As noted in one book on immigration law, "It represented a political compromise between four interests — (1) those people seeking to deter illegal immigration by discouraging unauthorized employment in the U.S.; (2) those seeking a one-time amnesty for aliens who, for years, had been locked out as illegal immigrants; (3) those who wanted to insure continued access to low-cost agricultural labor without elaborate federal regulation; and (4) those who wished to insure that penalizing employers for illegally hiring aliens who not encourage discriminatory employment practices."[66]

Many INS actions which look incompetent are the direct result of this compromise at the heart of our immigration laws. Our immigration legislation is the product of several competing interests and policies, and INS is left to sort out (and catch the flak for) the mess. Perhaps this explains the Border Patrol's conflicting reputations for both brutality (Amnesty International has investigated the US Border Patrol, and according to one work on Chicano folklore, "many Chicanos grew up being threatened by their parents that if they didn't behave, '*te vay llevar la migra*', *la migra* would come and take them away, presumably to Mexico"[67]) and laxness.

The INS is not given the resources to "do their job," because it's not really its job (as mandated by immigration legislation from 1986, 1990, and 1996) to have a secure border. If Congress really desired a secure border, it would have voted for tough employer sanctions, for example.

The end result is profound US ambivalent about its border controls, and INS reflects that ambivalence; its structural role is that of a "Dept. of Surplus Labor," keeping labor both illegal and flowing. Because of the compromises in US immigration law, INS's role in the US economy is to make illegal immigrant difficult, but not *too* difficult. Looked at structurally, its role is to provide a reserve army of cheap, docile labor for the construction, hotel/restaurant, garment, meatpacking, and agricultural businesses. This might also be accomplished with a guest-worker program (such as the old *bracero* program administered by the INS for agricultural employers between 1942 and 1964[68]), but right now it's accomplished through difficult-but-not-impossible illegal entry.

How could something like biometrics hope to resolve the conflicted over-150 year history of migration between Mexico and what used to be northern Mexico, but which is now part of the US?

National ID in the US faces analogous structural impediments. For one thing, countries with sophisticated national ID are often small. What works in Singapore, Hong Kong, or Israel may not scale to the US. The strong US tradition of "states rights," which was for example part of massive resistance to federally-ordered desegregation, combined with a strong anti-government tradition (which led in part to the Oklahoma City bombing), combined with fundamentalist fears over the "Mark of the Beast," may all make National ID impossible for the wrong reasons. Add in the NIMBY protests like those that

have hampered biometric BCC and exit-control implementation, and it's difficult to see what hope there would be for National ID.

Of course, for a rule or regulation to not work, or to produce the sorts of Prohibiton effects and unintended consequences we've seen with border controls, there has to be some sort of *demand* or *pull* for whatever it is that the rule or regulation forbids. Is there really any *demand* in the US for shoddy documentation, for easily-forged birth certificates, for databases that seemingly should be linked together but aren't?

Surprisingly, there *is* large demand in the US in essence for shoddy documentation. As noted earlier, key sectors of the economy rely upon illegal immigration: there's not so much a demand from business to make it legal, not is there a business demand to stop it, but instead the curious combination of the two, which produces a large, cheap, docile labor force. Having reliable documentation in the form of a National ID, on which I-9 forms could be based, for example, would represent a massive change to our current situation of large-scale under-the-table, off-the-books employment.[69]

Such a massive change would in turn require multiple uses. "Feature creep" is built into the idea of a National ID, because the expense and the extensive coverage that would be necessary before the system started to work, would dictate more uses than simply checking people getting on airplanes. National ID card adoption would involve the phenomenon of "parasitic vitality" that was seen in Britain's experience with ID cards: adoption of the card means that "it must be made obligatory in regard to as many as possible of the organised activities in close touch with the life of the people," as a British bureaucrat put it in 1923.[70]

Perhaps every use to which a National ID would be put is good: keeping terrorists off planes, making deadbeat dads pay for child support, preventing underage drinking, making sure that gun purchasers don't have criminal records, stopping tax evasion. But the sum total of all these goods may not be desirable. Moore's Law makes it possible to have something like Total Accountability: many of the everyday things we do or say could be recorded, cross-linked, and searched (Google.com, with its complete searchable archive of all newsgroup messages going back to 1981, may be a small example of this). A true National ID card, linked to a single national database, could help tie together all the disparate little pieces of our lives. Somone declares three dependents on their 1040, but the database "knows" that they only have one child living with them. The five-year history of resistance to implementing the biometric, machine-readable Border Crossing Card is a small example that almost no one truly wants even much lower levels of consistency.

Further Reading

Peter Andreas, *Border Games: Policing the U.S.-Mexico Divide*, Ithaca: Cornell U. Press, 2000

Peter Andreas and Timothy Snyder, eds., *The Wall Around the West: State Borders and Immigration Controls in North America and Europe*, Lanham: Rowman & Littlefield, 2000 (See especially Joseph Nevins, "The Remaking of the California-Mexico Boundary in the Age of NAFTA"; David Spener, "The Logic and Contradictions of Intensified Border Enforcement in Texas")

Jane Caplan and John Torpey, eds., *Documenting Individual Identity: The Development of State Practices in the Modern World*, Princeton: Princeton U. Press, 2001 (See especially Jon Agar, "Modern Horrors: British Identity and Identity Cards"; Dita Vogel, "Identifying Unauthorized Foreign Workers in the German Labor Market")

David Carliner et al., *The Rights of Aliens and Refugees* (ACLU Handbook), 2nd Ed., Carbondale IL:

Southern Illinois U. Press, 1990
Ted Conover, Coyotes: *A Journey Through the Secret World of America's Illegal Aliens*, NY: Vintage, 1987
John Crewdson, *The Tarnished Door: The New Immigrants and the Transformation of America*, NY: Times Books, 1983
Mariam Davidson, *Lives on the Line: Dispatches from the U.S.-Mexico Border*, Tucson: U. of Arizona Press, 2000
Mike Davis, *Magical Urbanism: Latinos Reinvent the US*, London: Verso, 2000
Debra DeLaet, *U.S. Immigration Policy in an Age of Rights*, Westport CT: Praeger, 2000
Judith Adler Hellman, Mexican Lives, NY: New Press, 1994 (Chapter 7: "The Border")
Helen Hayes, *U.S. Immigration Policy and the Undocumented: Ambivalent Laws, Furtive Lives*, Wesport CT: Praeger, 2001
David Jacobson, *Rights Across Borders: Immigration and the Decline of Citizenship*, Baltimore: Johns Hopkins U. Press, 1997
David Kyle and Rey Koslowski, eds., *Global Human Smuggling: Comparative Perspectives*, Baltimore; Johns Hopkins U. Press, 2001 (See especially Peter Andreas, "The Transformation of Migrant Smuggling Across the U.S.-Mexican Border"; David Spener, "Smuggling Migrants Through South Texas: Challenges Posed by Operation Rio Grande"; Mark Miller, "The Sanctionizing of Unauthorized Migration and Alien Employment")
Joseph Nevins, *Operation Gatekeeper: The Rise of the "Illegal Alien" and the Making of the U.S.-Mexico Boundary*, NY: Routledge, 2001
David M. Reimers, *Unwelcome Strangers: American Identity and the Turn Against Immigration*, NY: Columbia U. Press, 1998
Sebastian Rotella, *Twilight on the Line: Underworlds and Politics at the U.S.-Mexico Border*, NY: WW Norton, 1998
Ramón Eduardo Ruiz, *On the Rim of Mexico: Encounters of the Rich and Poor*, Boulder CO: Westview, 1998
John Torpey, *The Invention of the Passport: Surveillance, Citizenship and the State*, Cambridge: Cambridge U. Press, 2000
David Weissbrodt, *Immigration Law and Procedure in a Nutshell*, 4th Ed., St. Paul MN: West, 1998

(Footnotes)

* Stephen Keating, Director of the Privacy Foundation (http://www.privacyfoundation.org), suggested using the BCC as a case study to shed light on post-Sept. 11 proposals for a national ID card.

(Endnotes)

1 See "AAMVA DL / ID Standard 2000," http://www.aamva.org/standards/stdAAMVADLIdStandard2000.asp; see also *Washington Post*, Jan. 14, 2002 (http://www.washingtonpost.com/ac2/wp-dyn/A41032-2002Jan13?language=printer).
2 See http://www.lasercard.com/app/secure.htm and http://www.lasercard.com/app/app2.htm.
3 See Joseph W. Eaton, *Card-Carrying Americans: Privacy, Security, and the National ID Card Debate*, Totowa NJ: Rowman & Littlefield, 1986.
4 See, e.g., the Denver Post (Oct. 21, 2001; http://www.denverpost.com/Stories/0,1002,6439%257E190297,00.html) on a Mexican immigration official who co-ran the smuggling of hundreds from Syria, Iraq, and Jordan via Mexico into the US.
5 "The Threat of Terrorism is from Illegal Aliens," *Phyllis Schlafly Report*, Oct. 2001, http://

www.eagleforum.org/psr/2001/oct01/psroct01.shtml (interestingly, Schlafly opposes a national ID card; she also wants the Timothy McVeigh case reopened to look for John Doe No. 2 – perhaps one with a foreign connection).

6 "He also forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name" (Revelation 13:16). See my entry on "Identification cards" in the forthcoming *Encyclopedia of American Conspiracy Theories*, ed. Peter Knight (ABC-Clio, 2004), and Paul Boyer, *When Time Shall Be No More: Prophecy Belief in Modern American Culture* (Cambridge MA: Harvard U. Press, 1992), chapter 8 ("Antichrist, 666, and the Mark of the Beast").

7 http://travel.state.gov/HIA2000.html

8 *Statistical Yearbook of the INS*, 1998, http://www.ins.gov/graphics/aboutins/statistics/1998yb.pdf

9 See http://www.fairus.org/html/08270110.htm

10 IIRIRA: "Section 104. Improvements in Border Crossing Identification Card. New border crossing cards will include biometric identifiers (such as fingerprints or handprints) that are machine-readable. The cards will

begin to be issued in April 1998 and the machine-readable checking will occur on or after October 1999."

11 *Brownsville Herald*, Dec. 12, 2001, http://www.brownsvilleherald.com/sections/archive/topstoryjmp/12-20-01/News3.htm

12 See US Immigration and Naturalization Service (INS), "A Guide to Selected U.S. Travel/Identity Documents for Law Enforcement Officers," Aug. 1, 1998, http://www.fels.org/insforms/insdocs.htm

13 See http://www.ssa.gov/history/reports/briefhistory.html

14 Frank D. Bean et al., "Illegal Mexican Migration and the United States/Mexico Border: The Effects of Operation Hold the Line on El Paso/Juarez," US Commission on Immigration Reform, July 1994, http://www.utexas.edu/lbj/uscir/respapers/imm_jul94.pdf, p. 117

15 See http://www.house.gov/hunter/brdrchron3.htm

16 See http://www.house.gov/judiciary/ib072299.htm; http://www.house.gov/judiciary/stan0722.pdf

17 US State Dept., "Border Crossing Card (BCC) and Border Biometrics Program," Oct. 2001, http://travel.state.gov/bcc.html

18 See http://www.mexico-info.com/consulate/documentation.htm#passports

19 Simson Garfinkel, "Identity Card Delusions," Technology Review, April 2002, http://technologyreview.com/articles/garfinkel0402.asp: "States that digitize driver's-license photographs can use face recognition systems to find out if the same person has multiple identity cards issued in different names. (Last year the Mexican Federal Election Institute adopted this technology to help stamp out duplicate voter registrations.)" See also http://www.bioprivacy.org/Mexico.htm, http://www.wola.org/mexbulletin2.html, http://www.cnn.com/2000/WORLD/americas/06/30/mexico.elections/

20 See http://mozcom.com/~nso8/LateRegn.htm; see also Crewdson, *The Tarnished Door*, p. 41.

21 http://www.doj.gov/oig/i9609.htm

22 Michael R. Bromwich, Inspector General, US DOJ, before the US Senate Caucus on International Narcotics Control, May 14, 1997, http://www.usdoj.gov/oig/tesswbr1.htm. See also Peter Andreas, *Border Games: Policing the U.S.-Mexico Divide*, p. 99; http://www.ndsn.org/SEPT96/CUSTOMS.html;

http://www.usdoj.gov/oig/sa971/sa971p2.htm.

23 http://www.sec.gov/Archives/edgar/data/30140/0000891618-97-004321.txt

24 http://www.ins.gov/graphics/publicaffairs/newsrels/BCCRel.htm
25 http://www.usdoj.gov/oig/au9706/a9706tc.htm; emphasis added.
26 http://oig.state.gov/dept_chal.htm
27 Frank D. Bean et al., "Illegal Mexican Migration…" (see note 14), p. 116
28 See House Immigration Subcommittee Oversight Hearing on Electronic Technology Border Control, Oct. 11, 2001 (summarized at http://www.fairus.org/html/08270110.htm), and Senate Judiciary Committee-Subcommitte on Technology, Terrorism and Government Information Subcommittee, Oct. 12, 2001 (summarized at http://www.fairus.org/html/08271110.htm)
29 See DOJ/OIG, "The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of Its IDENT Automated Fingerprint Identification System," March 20, 2000, http://www.usdoj.gov/oig/resenrpt/resentoc.htm
30 See DOJ report on "Integration of Fingerprint Systems," Dec. 7, 2001, http://www.usdoj.gov/oig/inspection/I-2002-003/finger.htm
31 See http://www.wired.com/news/print/0,1294,47201,00.html; http://www.msnbc.com/news/647826.asp;
http://www.ocregister.com/breakingnews/attack/09282001/dmv00928cci4.shtml
32 See Crewdson, *Tarnished Door*, p. 43
33 See Richard Smith's excellent work on facial recognition: http://www.computerbytesman.com/facescan/presentation/index.htm; see also Jay Stanley and Barry Steinhardt, "Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida" (ACLU special report), Jan. 3, 2002, http://www.aclu.org/issues/privacy/drawing_blank.pdf; http://www.aclu.org/features/f110101a.html
34 See http://www.oracle.com/pls/ebn/popup.on_demand?p_referred=related_show&p_shows_id=919253& p_win_size=L150
35 http://www.konzept-pr.de/pressemitteilungen.cfm?identer=697&kunde=Keyware
36 See Andreas, *Border Games*, p. 91; see also http://www.fpusa.com/dmpits.htm; *National Institute of Justice*
Journal, Oct. 1998 (http://www.ncjrs.org/pdffiles/jr000237.pdf), pp. 21-25; http://www.fpusa.com/dmpits.zip
37 http://www.usdoj.gov/opa/pr/2000/March/108jmd.htm; see also http://www.apbonline.com/crimesolvers/serialkiller/2000/03/20/resendiz0320_01.html
38 http://www.google.com/search?q=cache:www.senate.gov/~judiciary/te101701si-norton.htm+&hl=en
39 See http://www.usdoj.gov/oig/i9609.htm
40 On employee monitoring, see Schulman, "Computer and Internet Surveillance in the Workplace," http://www.sonic.net/~undoc/survtech.htm
41 http://www.csmonitor.com/durable/1999/10/26/p11s1.htm;
42 http://www.currentlegal.com/LegalNews/uspl1998/106-215.html
43 http://migration.ucdavis.edu/mn/archive_mn/apr_1999-06mn.html; see also http://www.ins.usdoj.gov/graphics/aboutins/congress/testimonies/1999/990318.pdf
44 http://www.house.gov/judiciary/6144.htm
45 See http://www.international.duke.edu/FAQ/int_address_report.html
46 David Weissbrodt, *Immigration Law and Procedure in a Nutshell*, 4th E., pp. 468-7
47 Crewdson, *Tarnished Door*, p. 125
48 *See Dita Vogel, "Identifying Unauthorized Foreign Workers in the German Labor Market," in Jane Caplan and John Torpey, eds., *Documenting Individual Identity: The Development of State Practices in the Modern World*

49 INS, "25-Mile Zone — Regulatory History," Oct. 8, 1999, http://www.ins.usdoj.gov/graphics/publicaffairs/backgrounds/BGround.htm (emphasis added)

50 See Mike Davis, *Magical Urbanism*, ch. 7; see also http://www.arc.org/C_Lines/CLArchive/story2_3_08.html

51 See Weissbrodt, *Immigration Law and Procedure*, pp. 195-7; Carliner et al., *The Rights of Aliens and Refugees* (ACLU), pp. 118-125; David A. Harris, *Profiles in Injustice: Why Racial Profiling Cannot Work*, NY: New Press, 2002, ch. 6; some of the key Supreme Court cases are *Almeida-Sanchez v. US* (1973), *US v. Ortiz* (1975), *US v. Brignoni-Ponce* (1975), and *US v. Martinez-Fuerte* (1976). Two 9th Circuit Court of Appeals cases, *US v. Montero-Camargo* and *US v. Sanchez-Guillen* (1999) peripherally involved BCCs. *Murillo v. Musegades* (1992) is a key case (settled) involving constant Border Patrol stops and searches of students at Bowie High School near El Paso; some parents, fearing accidental deportations of their children, would have their children bring their birth certificates with them to school every morning (see Amnesty International's report on the US/Mexican border, 1998, http://www.web.amnesty.org/ai.nsf/index/AMR510031998).

52 http://www.ilw.com/lawyers/immigdaily/cases/2001,0123-Barajas.shtm

53 Ellison presentation on national ID to Oracle employees: see note 33

54 Judith Adler Hellman, *Mexican Lives*, pp. 169-70

55 http://www.ins.usdoj.gov/graphics/lawenfor/interiorenf/investigations.htm

56 Mark J. Miller, "The Sanctioning of Unauthorized Migration and Alien Employment," in Kyle and Koslowski, eds., *Global Human Smuggling*, p. 325; emphasis added

57 See http://www.usda.gov/oce/oce/labor-affairs/newhires.htm; http://www.acf.dhhs.gov/programs/cse/newhire/nh/state_cb.htm; http://www.acf.dhhs.gov/programs/cse/newhire/nh/answers.doc

58 Miller, "Sanctioning of Unauthorized Migration," p. 325; see also "Illegal Aliens: Fraudulent Documents Undermining the Effectiveness of the Employment Verification System," July 1999, http://www.house.gov/judiciary/stan0722.pdf

59 Peter Andreas, "The Transformation of Migrant Smuggling across the U.S.-Mexican Border," in Kyle and Koslowski, *Global Human Smuggling*, p. 112

60 Peter Andreas, *Border Games*, p. 86

61 See http://www.workforce.com/section/00/feature/23/13/85/

62 See e.g. Gustavo Lopez Castro, "Coyotes and Alien Smuggling," www.utexas.edu/lbj/uscir/binpapers/v3a-6lopez.pdf

63 David Spener, "The Logic and Contradictions of Intensified Border Enforcement in Texas," in Andreas and Snyder, eds., *Wall Around the West*, pp. 119, 134 n. 17.

64 GAO, "INS' Southwest Border Strategy: Resource and Impact Issues Remain After Seven Years," August 2001, http://www.bordercounties.com/documents/goa_boarder_strategy.pdf

65 See http://dailynews.yahoo.com/h/azstar/20011226/lo/many_mexicans_stay_in_u_s_for_yule_1.html

66 Weissbrodt, *Immigration Law and Procedure*, p. 22

67 Rafaela G. Castro, *Chicano Folklore*, Oxford: Oxford U. Press, 2001, p. 158

68 See Kitty Calavita, *Inside the State: The Bracero Program, Immigration, and the INS*, NY: Routledge, 1992

69 See, e.g., Bruce Wiegand, *Off the Books: A Theory and Critique of the Underground Economy*, Dix Hills NY: General Hall, 1992; Thomas Gabor, *Everybody Does It!: Crime by the Public*, Toronto: U. of Toronto Press, 1994

70 See Jon Agar, "Modern Horrors: British Identity and Identity Cards," in Caplan and Torpey, eds., Documenting Individual Identity, pp. 101-120.