Testimony of Jim Harper
Director of Information Policy Studies
The Cato Institute
to the House Committee on the Judiciary
Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law

Hearing on Proposals to Improve the Electronic Employment Verification and Worksite Enforcement System

April 26, 2007

Executive Summary

There are formidable problems with creating a workable and acceptable electronic employment verification system for federal immigration law enforcement. Creating a nationwide system for checking identity and eligibility is *much* more easily said than done.

Given the flaws in the current system, it is unsurprising that there should be a push to improve it. However, improvements that prevent eligible citizens from working should not be adopted. It is more important that American citizens and eligible people should be able to work than it is to exclude illegal aliens from working.

There is probably no way to change the current system so that it prevents more ineligible people from working without also preventing more citizens and eligible people from working. This suggests that the policy of internal enforcement itself is the source of the problem.

Beyond its influence on work, expanding electronic verification would impose many costs on the country and society. The dollar costs of a nationwide electronic verification system would be high. Electronic verification would have far greater privacy consequences than the current I-9 system — and these consequences would fall on American citizens, not on illegal immigrants. Expanded electronic verification would invert our federal system and explode limited government.

The policy that will dissipate the need for electronic verification by fostering legality is aligning immigration law with the economic interests of the American people. Legal immigration levels should be increased.

Testimony of Jim Harper
Director of Information Policy Studies
The Cato Institute
to the House Committee on the Judiciary
Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law

Hearing on Proposals to Improve the Electronic Employment Verification and Worksite Enforcement System

April 26, 2007

Chairman Lofgren, Ranking Member King, and Members of the Committee:

It is a pleasure to speak with you today. I am director of information policy studies at the Cato Institute, a non-profit research foundation dedicated to preserving the traditional American principles of limited government, individual liberty, free markets, and peace. In that role, I study the unique problems in adapting law and policy to the information age. I also serve as a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, which advises the DHS Privacy Office and the Secretary of Homeland Security on privacy issues.

My most recent book is entitled *Identity Crisis: How Identification Is Overused and Misunderstood*. I am also editor of Privacilla.org, a Web-based think tank devoted exclusively to privacy, and I maintain an online resource about federal legislation and spending called WashingtonWatch.com, which recently introduced a legislative wiki that will increase government transparency — especially once you in Congress realize that you can use it to communicate directly with the interested public. I speak only for myself today and not for any organization with which I am affiliated or for any colleague.

Congratulations and thank you for conducting extensive hearings on so many dimensions of the immigration reform issue. When bills pass Congress without hearings, the results can be expensive and threatening to liberty. The REAL ID Act is one example. While that law has done much for me in terms of frequent flyer miles and book sales, I prefer Congress to legislate with care.

There are formidable problems with creating a workable and acceptable electronic employment verification system for federal immigration law enforcement. By stating the

problem in terms of identification and credentialing, perhaps I can help surface some of those problems and help you determine what the best approach is to immigration reform, whether there should be an electronic employment verification system, and what the concerns are with such a system.

My analysis leads me to conclude that there are fundamental problems with the policy of "internal enforcement" which electronic employment verification supports. The flaws in internal enforcement should be fatal to that concept. The solution that will foster legality is aligning immigration law with the economic interests of the American people.

Immigration Policy, Briefly

One cannot talk about a technology-focused government program without examining policy considerations. The human forces that a policy would channel or counteract are the most important influence on how the supporting system must be designed, where the challenges to it will come from, and the human and monetary costs of making the system work for its intended purpose.

Our nation's immigration policy is at a crossroads. According to my colleague Dan Griswold and Labor Department projections, our economy will continue to create 400,000 or more low-skilled jobs annually in the service sector — tasks like food preparation, cleaning, construction, landscaping, and retail. Yet during the period from 1996 to 2004, the number of adult Americans without a high school education — the demographic that typically fills these jobs — fell by 4.6 million.[1]

These demographic facts create very powerful economic forces. There is demand in the United States for both low- and high-skilled workers. Workers in many nearby countries desire and, in many cases, very badly need work of the kind offered in the United States. The economic gradient is steep.

Like water following the laws of gravity, there has been continuing movement of workers to the United States. Unlike water, which can be stopped with simple barriers, people on both sides of the border dedicate their ingenuity to getting what they want and need. The self-interest of employers and workers is a powerful (and almost always beneficial) force that is hard to quell or conquer.

The last major effort to address immigration did not admit the power of these economic forces, however. In the Immigration Reform and Control Act, Congress chose not to expand legal immigration, but instead interposed a legal eligibility requirement on the employment relationship. IRCA made it unlawful for employers to knowingly hire

[1] Daniel T. Griswold, *Immigration Reform Must Include a Temporary Worker Program*, Orange County Register (Mar. 7, 2007) <http://www.freetrade.org/node/600>.

workers who are not eligible to work in the United States. All employers are required to verify employees' work eligibility via the I-9 form, and employers who knowingly hire ineligible workers are subject to penalties.

There is logic to this idea: In theory, making it illegal to hire those not legally in the United States could reduce the strength of this country's economic "magnet." The I-9 process and employer sanctions undoubtedly have had some effect on curtailing illegal immigration and working, but not very much. The policy cannot be called a success — obviously — Congress is revisiting it.

Employment eligibility verification has not changed or defeated the underlying economics. It would not be a good idea to do so — Americans benefit from the influx of labor, and the workers who come here benefit from working here.

Because the I-9 process and employer sanctions seek to defeat their economic interests, the system has two principle opponents: employers and workers. It relies on them for implementation, though, which is why success has been so elusive and will continue to be. It is important to examine whether a "strengthened," electronic system such as an expanded Basic Pilot can improve on the status quo, and whether the costs of implementing such a system are justified by the benefits.

Eligibility Checks as a Credentialing System

It is useful to look at employer sanctions under the Immigration Reform and Control Act system through the lens of identity and credentialing. This helps reveal all the steps in the process, their weaknesses, what it would take to fix them, and what that would cost. If nothing else, it shows that a nationwide system for checking identity and eligibility is *much* more easily said than done.

Simply put, IRCA made working legally in the United States contingent on presenting a certain credential: proof of legal eligibility. There is a difference, of course, between being eligible to work and proving that eligibility. The gap between actual eligibility and proof of it is routinely exploited by the system's opponents — again, employers and workers — as they pursue their interests.

<u>False Positives and False Negatives in Screening for Ineligibility</u>
It is difficult to prove work eligibility under IRCA on a mass scale. Because the credential is a personal one (i.e., attaching to the individual, non-transferable), there are two steps to this process: 1) identification of the individual and 2) determination of that individual's eligibility.

Flaws in the processes for proving identity and eligibility (actually, testing for ineligibility) mean that some people who are entitled to work may be denied work ("false

positives"), and some who are not legally entitled to work will be able to work ("false negatives").

False positives and false negatives are almost always in tension with each other. Seeking lower false positives usually requires the acceptance of higher false negatives, and vice versa. For example, a system that excluded every single ineligible worker without exception (*zero* false negatives) would exclude from working many eligible workers (high false positives).

Because of our system of values and rights, the IRCA regime must have very low false positives — and no false positives attributable to government action. It is wrong to deprive those who are legally eligible to work of a livelihood, and a wrongful deprivation of work based on government action would be a denial of Due Process. This requires the acceptance of some false negatives (i.e., the employment of some ineligible people).

Though the current system appears deeply flawed, it may be relatively well tuned to the requirement that there be the barest minimum of false positives. A system with high false negatives — essentially, a sloppy internal enforcement system — may be the most appropriate accommodation of the difficult-to-implement policy of internal enforcement.

Changing to an electronic system like an expanded Basic Pilot must happen without raising false positives, which, again, would be incompatible with our system of individual rights and dignity, as well as with Due Process in many cases. Let us briefly examine the current processes before turning to how an expanded Basic Pilot would change them and whether the those changes are justified given the costs.

<u>Employment Eligibility Verification: the I-9</u>

Currently, employers must collect and examine identity and eligibility information from all employees at the time of hire. This can be done through a single document, such as a passport or certificate of U.S. citizenship, or through two separate documents, one each for identity and eligibility, such as a driver's license and a social security card. The employer must attest, under penalty of perjury, that it has examined the documents, found that they appear to be genuine, and that the employee appears eligible to work in the United States.

This conversion of every small business person and human resources director in the country to an immigration agent assuredly hides the cost of the enforcement regime, but it does not necessarily work very well at combating illegal working, for a combination of reasons.

First, like many broad identity and credentialing systems, the I-9 process is highly subject to avoidance. As noted above, employers and workers have strong economic incentives to get together on mutually agreeable terms. The IRCA policy is an interposition on that

process. Employers and workers can and do collude to avoid the system entirely. They conduct business "under the table," avoiding IRCA and various taxes and regulatory restrictions, as well.

Assuming they operate within the system, however, employers and workers still create many false positives and negatives, wrongly excluding some people from work, and allowing some to work contrary to IRCA.

Checking Identity and Eligibility

In our personal interactions, people use identification constantly. We are very adept at recognizing others with our eyes, ears, and other senses. This enables us to pick up right where we left off when we see people a second, third, and fourth time. Our success and familiarity with in-person, familiar identification seems to give us excessive confidence in identification's power in other contexts.

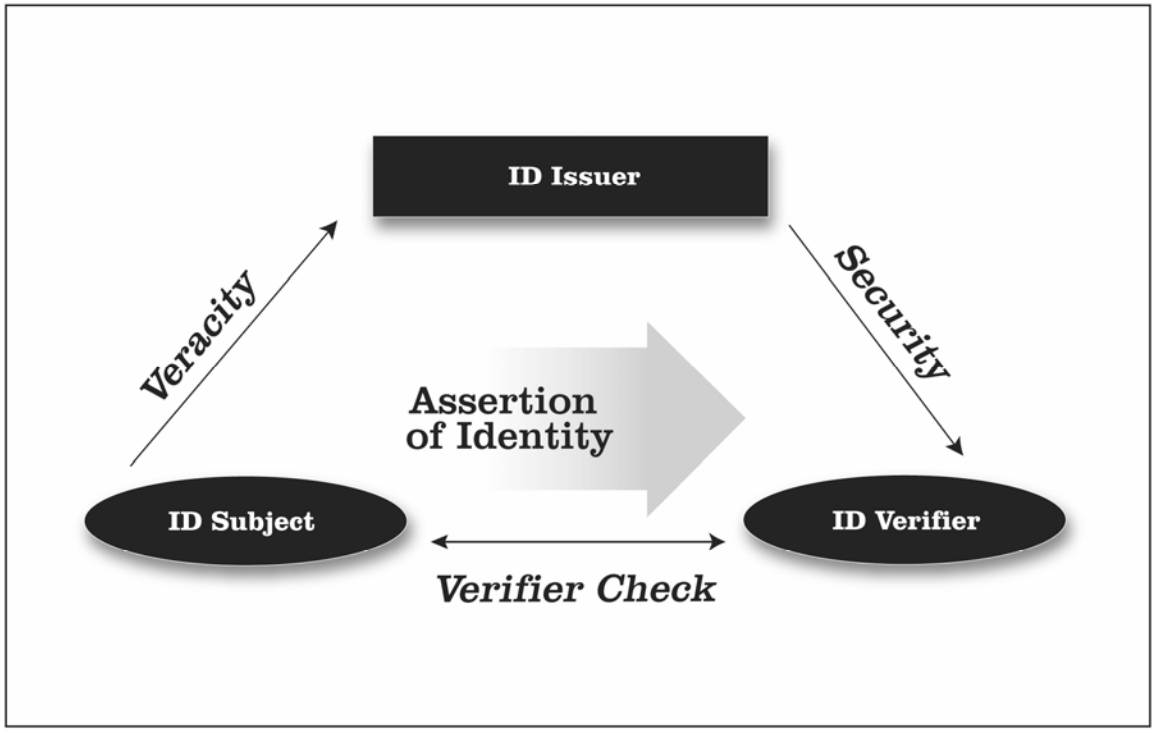
The employment relationship is not like our relationships with friends and neighbors. It typically commences among strangers. Particularly in low-skill jobs, the new employee proffers his or her identity for the first time at the beginning of the relationship. The employer takes little time to examine the applicant's identity *bona fides*.

At this early point in the relationship, though, the government requires the employer to examine and report on the new employee's identity information. It is not a natural, personal interaction of the kind that gives us so much confidence in identification. It is identification by card.

In my book, *Identity Crisis: How Identification is Overused and Misunderstood*, I describe the process of identifying someone by card. This is an important and valuable process, which allows people to be treated as "known," at least to a degree, from the first encounter. But the identification-by-card process is also fraught with weaknesses. The figure on the next page describes the three steps in the process by which a card transfers identity information from the subject (cardholder) to the verifier (relying party).

First, the subject applies to a card issuer for a card, typically supplying all the information on the card. Next, the card issuer creates a card, supplying information to any later verifier. Finally, the verifier compares the card to the subject and, having verified that the card is about the subject, accepts the information on the card.

Each of these three steps is a point of weakness, an opportunity for false negatives to creep in. In the first step, the subject may apply to the card issuer with false information (including false documents), or the subject may corrupt employees within the card issuer, causing them to issue an inaccurate but genuine card. This will almost certainly deceive the employer, who, except under extraordinary circumstances, cannot be expected to second-guess information printed on a genuine, un-tampered-with card.



At issue in the second step is the security of the card against forgery or tampering. Though many government-issued ID documents are quite resistant to forgery and tampering, the broadened use of these documents (including for immigration control) has increased the value of forging such documents and devising ways to tamper with them. Employers, who would be acting against their own interests to discover such things, cannot be expected to discover forgery or tampering of any decent quality.

The third step, comparing the identifiers on a card to the subject, is an area where employers are not specially disabled — everyone has the same ability to compare a picture to the face in front of them — but here, again, employers will not be terribly eager to discover deception, such as someone showing the card of a different person similar in appearance.

If the worker has opted to present separate identity and eligibility documents, the process for employer verification of eligibility follows much the same path — and it carries the same risks to the system.

The worker may have acquired the eligibility document by fraud or corruption, such as by wrongly acquiring a certified copy of a birth certificate matching the name on the identity document. The security of this kind of document tends to be low, which

compromises the second step in the process. Social security cards, for example, are relatively commonly forged. Because these documents do not typically have any biometric identifiers, there is no way for the employer to check it against the worker. A mere name-match to the identity document is taken as proof that the eligibility document is tied to the identity document which was previously tied to the worker.

Considering the many tenuous steps involved in the process, it is little wonder that deputizing employers as immigration agents has not been an end to the U.S. economic "magnet." There are high false negatives in the system today.

This process is also a source of false positives, though. It prevents people who are legally entitled to do so from working.

The requirement to present documents itself is a barrier to employment, for example, particularly for homeless, indigent, and mentally ill people. Due to personal failing or not, they may lack education and basic coping skills, they may have experienced violence, theft of their belongings, and drug and alcohol addiction. But when the time comes to clean up, pull themselves up by their bootstraps, and take that entry-level janitorial job, federal law requires them to present documents they often do not have.

If the documents are unavailable, they must be applied for within three business days, and produced within 90 days, or the new employee will be fired. People on the margins are undoubtedly discouraged and dissuaded from working by these barriers — low as they may seem to the elites that populate the committee rooms and witness tables in Congress.

Discrimination is another source of false positives. The I-9 Form itself has prominent anti-discrimination information, undoubtedly because of employers' IRCA-inspired hesitance to employ potentially ineligible workers. Employers who want to hire workers without hassles, and who want to steer clear of liability under IRCA, will naturally gravitate away from job candidates whose eligibility to work appears marginal. Workers with Hispanic surnames, or who lack proficiency in English, are probably turned away by risk-averse employers long before the question of documentation arises.

"Improving" Eligibility Screening with Electronic Checks

Given the flaws in the current system, it is unsurprising that there should be a push to improve it. However, improvements that would raise false positives should not be adopted. It is more important that American citizens should be able to work than it is to exclude illegal aliens from working. There is probably no improvement that lowers false negatives without raising false positives. This suggests that the policy of internal enforcement itself is the source of the problem. At least two attempts to improve it have already failed.

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 required INS to commence three pilot programs to test electronic verification of employees' eligibility to work: the Citizen Attestation Verification Pilot Program, the Machine-Readable Document Pilot Program, and the Basic Pilot Program. According to the Government Accountability Office, the three pilot programs were to test whether pilot verification procedures could improve the existing Form I-9 process by reducing (1) document fraud and false claims of U.S. citizenship (i.e., false negatives), (2) discrimination against employees (false positives), (3) violations of civil liberties and privacy, and (4) the burden on employers to verify employees' work eligibility.[2]

The Citizen Attestation Verification Pilot Program allowed workers to attest to their citizenship status. The status of newly hired employees attesting to being work-authorized noncitizens was electronically checked against information in INS databases. Unsurprisingly, ineligible workers attested to being citizens. Employers, who lacked an interest in ferreting out this kind of fraud, did not ferret out this kind of fraud. But they did discriminate against work-authorized noncitizens, likely because of the paperwork and liability risks such workers presented. The Department of Homeland Security terminated the Citizen Attestation Verification Pilot Program in 2003.

The Machine-Readable Document Pilot Program was initiated in Iowa because that state issued driver's licenses and identification cards carrying the information required for the I-9 in machine-readable form. The program had technical difficulties in reading the driver's licenses and IDs, and it was undermined by the state's transition away from using Social Security numbers on driver's licenses in the interest of Iowans privacy and data security. DHS terminated the Machine-Readable Document Pilot Program in 2003 as well.

Basic Pilot is the remaining effort to verify work eligibility electronically. After completing the I-9 Forms, employers enter the information supplied by the worker into a government Web site. The data is then compared with information held by the Social Security Administration and with DHS databases to determine whether the employee is eligible to work.

Basic Pilot electronically notifies employers whether their employees' work authorization is confirmed. Submissions that the automated check cannot determine are referred to U.S. Citizenship and Immigration Service staff, who take further steps to verify eligibility, or who determine the ineligibility of the worker.

---

[2] *See generally*, Government Accounting Office, Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts, GAO-05-813 (Aug. 2005) <http://www.gao.gov/new.items/d05813.pdf>.

When Basic Pilot cannot confirm a worker's eligibility, it issues the employer a "tentative nonconfirmation." The employer must notify the affected worker of the finding, and the worker has the right to contest his or her tentative nonconfirmation within 8 working days by contacting SSA or USCIS. When a worker does not contest his or her tentative nonconfirmation within the allotted time, the Basic Pilot program issues a final nonconfirmation for the worker and the employer is required to either immediately terminate the worker or notify DHS of the continued employment of the worker.

False Negatives Lowered, But at a Cost

Basic Pilot undoubtedly does have some controlling influence on the rate of false negatives — ineligible workers being able to work. The submission of the worker's proffered name and Social Security number to the Social Security Administration allows for a simple background check: comparing whether the name/SSN combination submitted matches a combination in the SSA's files.

By databasing submissions, SSA can position itself to detect multiple uses of the same name/SSN combination, such as when the same "identity" is hired in multiple states during the same week. These types of checks increase the challenge for ineligible workers and probably reduce illegal working to some degree.

Given the economic incentives in favor of work, however, workers (and employers) will take a variety of counter-measures. More employment will occur under the table, for example. Ineligible workers, or criminal organizations working on their behalf, may corrupt employees in Social Security offices and the Department of Homeland Security to obtain confirmations of eligible status. This kind of corruption routinely occurs in Departments of Motor Vehicles across the country because of the value in having a real (though inaccurate) driver's license or state-issued ID card.

The primary counter-measure ineligible workers will take is to seek documents with genuine, but rarely used, name/SSN combinations. The source of those identifier combinations, of course, will be work-eligible Americans. Expanding Basic Pilot will increase illicit trade in Americans' Social Security numbers and other identifiers. Expanding Basic Pilot will increase identity fraud.

False Positives Raised

While lowering false negatives and illegal working some, expanding Basic Pilot will also raise false positives. More work-eligible Americans will be denied employment.

The sources of false positives are many, and they will compound to frustrate American workers and employers alike. For example, simple errors in data entry by employers will create a baseline mistaken "tentative nonconfirmation" rate, sending workers into the unwelcome embrace of federal bureaucratic offices and processes.

Last December, the Social Security Administration's Office of Inspector General estimated that the SSA's "Numident" file — the data against which Basic Pilot checks worker information — has an error rate of 4.1% . All of the cases it analyzed resulted in Basic Pilot providing incorrect results.[3] At this rate, one in every 25 new hires would receive a "tentative nonconfirmation" and have to engage with the bureaucracy — most likely during hours they are supposed to be at those new jobs. False positives would be high and costly under an expanded Basic Pilot.

The "logic checks" that SSA might run are not as simple to deal with as one might assume. Looking for the same "identity" hired multiple times in short succession, for example, would suggest that some workers are submitting fraudulent information, but it would not reveal which ones. A work-eligible person would be just as suspect as the non-work-eligible people using his or her information.

The work-eligible person would probably be "tentatively nonconfirmed" like the rest, and have to prove that, among all the people using this identity, he or she is the true person. This will not be easy for people with low levels of education, limited proficiency in English, and other detriments. They may be pushed out of the legitimate working world, their identity fraud victimization made worse by what they perceive only as confounding bureaucratic procedures.

Let there be no illusion that people seeking redress for a "tentative nonconfirmation" from the Social Security Administration or the Department of Homeland Security will enjoy a pleasant, speedy process. Offices where people seek redress for data errors would be as friendly, courteous, responsive, and efficient as the Departments of Motor Vehicles offices that Americans so dread. People will wait in line for hours to access bureaucrats that are not terribly interested in getting them approved for employment.

The consequences of scaling up a program like this should not be underestimated. Basic Pilot has many flaws at its current size, but growing the program will create new and different problems. Going from less than 20,000 employers to the entire nation is a change in kind, not degree. The employers in the program now are relatively well-equipped and motivated compared to the variety of employers an expanded Basic Pilot would encounter.

Most small businesses have no personnel dedicated to compliance. Many businesspeople are rarely connected or not connected to the Internet, either because of remoteness, cost, or lack of business necessity. The compliance, accuracy, and non-discrimination rates experienced in an expanded Basic Pilot would likely be lower than what is currently seen.

---

[3] Office of the Inspector General, Social Security Administration, *Accuracy of the Social Security Administration's Numident File*, A-08-06-26100 (Dec. 2006) <http://www.socialsecurity.gov/oig/ADOBEPDF/audittxt/A-08-06-26100.htm>.

The Costs of Expanded Electronic Verification

Beyond its influence on working, expanding electronic verification would impose many costs on the country and society. The dollar costs of a nationwide electronic verification system would be high. Electronic verification would have far greater privacy consequences than the current system — and these consequences would fall on American citizens, not on illegal immigrants. Expanded electronic verification would invert our federal system and explode limited government. Final employment decisions would no longer be made by employers and workers, but by a federal government bureaucracy — or maybe two of them.

Taxpayer Dollars

In December 2005, the Congressional Budget Office estimated the costs of the electronic employment verification system in H.R. 4437, an immigration reform bill in the 109th Congress.[4] Those costs were substantial.

Under the Basic Pilot expansion in that bill, CBO found that 50 to 55 million new hires would have to be verified each year. A total of 145 million currently employed workers would have to have been screened using the expanded system by 2012. CBO's estimate was conservative; it excluded agricultural workers.

Given the massiveness of the undertaking, CBO estimated $100 million in short-run costs for upgrading software, hardware, databases, and other technology. To handle queries about "tentative nonconfirmations," the Department of Homeland Security and Social Security Administration would have had to spend about $100 million per year on new personnel. The federal government, states, localities, and private businesses would all have had to spend more for screening their workers. Accordingly, CBO found that the mandates in the bill would exceed the thresholds set by the Unfunded Mandates Reform Act of 1995.

Ironically (returning to substantive policy briefly again), all of this government spending and expanded bureaucracy would go toward preventing productive exchanges between employers and workers. Taxes and spending would rise to help stifle U.S. economic growth. Astounding.

---

[4] Congressional Budget Office, Cost Estimate: H.R. 4437, Border Protection, Antiterrorism, and Illegal Immigration Control Act of 2005 (Dec. 13, 2005) <http://www.cbo.gov/ftpdocs/69xx/doc6954/hr4437.pdf>.

American Citizens' Privacy

The American citizen taxpayer would not only incur pocketbook costs and increased bureaucracy, but lost privacy as well. An electronic system is not just a faster paper system. It has dramatically different effects on privacy.

When an employer fills out a form like the I-9 and puts it in a file, the information on the I-9 remains practically obscure. It is not very easy to access, copy, or use. This protects privacy, and it protects against the data breaches we have heard so much about recently. It is relatively inefficient — but secure in terms of the worker's privacy.

When an organization enters I-9 information into a Web form and sends it to the Social Security Administration and Department of Homeland Security, that information becomes very easy for those entities to access, copy, or use. It is likely combined with "meta-data" — information about when the information was collected, from whom, and so on. The process gives these agencies access to a wealth of data about every American's working situation. And because it is tied to the Social Security number it can easily be correlated with tax records at the IRS, education loan records in the Department of Education, health records at the Department of Health and Human Services, and so on.

Unless a clear, strong, and verifiable data destruction policy is in place, any electronic employment verification system will be a surveillance system, however benign in its inception, that observes all American workers. The system will add to the data stores throughout the federal government that continually amass information about the lives, livelihoods, activities, and interests of everyone — especially law-abiding citizens.

Many people believe that they have nothing to hide, and feel willing to have their employment tracked if it will stop illegal immigration. Unfortunately, it will not. And most people who make the "nothing to hide" claim balk when they are actually confronted with stark choices about privacy. No one has ever mailed me their tax forms so I can publish them on the Web.

People have things to hide. That is normal and natural. Indeed, many people object to information about themselves being compiled on principle, no matter who is doing it or what their purpose. That is an acceptable way of thinking in this country, where we allow law-abiding citizens to protect privacy for any reason or no reason.

Employment Eligibility Data and Identity Fraud

Disclosure to the government is not the only privacy-related concern with an electronic employment verification system. Data security is an issue as well. We have seen massive data breaches from government agencies in the recent past, and from private entities too. Many occur by mistake. In some cases, a particular set of data is the target of a hacker or criminal.

Earlier in my testimony, I noted that a counter-measure ineligible workers will use in the face of an electronic employment verification system is to acquire new name and Social Security number pairs. The very best source of this information will be the system itself — the Social Security Administration and DHS databases, the offices where "tentative nonconfirmations" are processed, the people that process them, and the communications links that connect all these elements.

Any electronic employment verification system will be a target for hackers, a data breach waiting to happen, and a threat to the identity system we rely on today. The best security against data breach is not collecting information in the first place. Electronic employment verification would put Americans' sensitive personal information at risk.

Add-ons to Electronic Employment Verification: A National ID System

As I discussed above, an expanded electronic employment verification system would not just stop ineligible workers from working and employers from hiring them. It would change behavior, causing work to be done under the table and increasing identity fraud aimed at defeating the 'strengthened' system.

The establishment of such a system would also change the behavior of governments. An electronic employment system would expand over time and join with other programs. These behaviors are just as important to consider.

Were an electronic employment verification system in place, it could easily be extended to other uses. Failing to reduce the "magnet" of work, electronic employment verification could be converted to housing control. Why not require landlords and home-sellers to seek federal approval of leases and sales so as not to give shelter to illegal aliens? Electronic employment verification could create better federal control of financial services, and health care, to name two more.

It need not be limited to immigration control, of course. Electronic verification could be used to find wanted murderers, and it would move quickly down the chain to enforcement of unpaid parking tickets and "use taxes." Electronic employment verification charts a course for expanded federal surveillance and control of all Americans' lives.

It is well recognized that Basic Pilot does little to detect or suppress orthodox identity fraud, in which criminals or illegal aliens present false credentials. Employers — deputized as immigration officials and acting against their interests — can be expected to remain quite unhelpful at ferreting out this fraud.

Seeking to close this 'loophole,' many immigration reform proposals already include the creation of some form of national identification scheme. With the REAL ID Act near collapse — states are refusing to implement this unfunded surveillance mandate — the

dominant proposal seems to be the idea of having a secure, biometric Social Security card. This has the same characteristics and flaws as any other national ID system. These problems deserve review.

Costs to Taxpayers

The REAL ID Act has forced some analysis of having a national ID in the U.S., and there is now cost information to work with. The Department of Homeland Security recently estimated in its Notice of Proposed Rulemaking on the Act that implementing this national ID system would cost $17 billion dollars.[5] This is a huge expenditure, which actually fails cost/benefit analysis.[6]

REAL ID, of course, contemplates implementation by state Departments of Motor Vehicles, which are somewhat equipped for the logistical problems involved in personal information collection (including biometrics) and card issuance. The Social Security Administration has essentially no similar capacity — issuing a card is the easy part. SSA would have to construct many more satellite offices, gain the capability to collect and store biometrics and other information, and build many other capabilities from scratch, at enormous further cost.

Surveillance

There are serious additional privacy concerns with the creation of a nationally uniform identity system. Economists know well that standards create efficiencies and economies of scale. When all the railroad tracks in the United States were converted to the same gauge, for example, rail became a more efficient method of transportation. The same train car could travel on tracks anywhere in the country, so more goods and people traveled by rail. A nationally uniform "secure, biometric" Social Security card would have the same influence on the uses of ID cards.

If all Americans had the same identification card, there would be economies of scale in producing card readers, software, and databases to capture and use the information from the cards. Americans would inevitably be asked more and more often to produce identification cards, and share the data from them, when they engaged in various governmental and commercial transactions.

Various institutions would capitalize on the information collected in the federal database behind the card and harvested using these Social Security cards. Speaking to the

---

[5] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Proposed Rule 72 Fed. Reg. at 10,845 (Mar. 9, 2007).

[6] Testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute, to the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia at a hearing entitled "Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards" at 6-9 (Mar. 26, 2007) <http://hsgac.senate.gov/_files/TestimonyHarper.pdf>

Department of Homeland Security's Data Privacy and Integrity Advisory Committee recently, Anne Collins, the Registrar of Motor Vehicles for the Commonwealth of Massachusetts said, "If you build it they will come." Speaking of REAL ID, she was pointing out that massed personal information would be an irresistible attraction to the Department of Homeland Security and many other governmental entities, who would dip into data about us for an endless variety of purposes.

The DHS NPRM on REAL ID cites some other uses that governments would make of REAL ID, including controlling unlawful employment, gun ownership, drinking, and smoking. Uniform ID systems are a powerful tool. Just like REAL ID, a secure, biometric Social Security card would be used for many purposes beyond what are contemplated today, including tracking of law-abiding citizens.

Transfer of Power

The old saw is true: Information is power. Uniform government ID systems have important consequences in terms of the individual's relationship to government. A major concern with national IDs is the power that identification systems give to governments.

We are all well aware of the beneficent motives of most government employees, but good feelings are not good security. Governments and government officials do stray from the path of lawfulness, peace, and liberty. If the government knows where you are, if it knows where your assets are, if it knows how you communicate and with whom, it is in a much better position to affect your life in ways you may not like.

Governments of the future, making use of national ID systems — and particularly electronic tracking — would not have to go through the difficulties they traditionally have when they want to affect the rights and liberties of an individual. Large databases about people change the incentive structure that law enforcement and national security agencies face.

To be simplistic, traditionally, law enforcement agencies have investigated crimes. They have learned of something bad happening or something bad about to happen, and they have gone after that. More and more, with data available about everybody, they will be in a position to investigate people, instead of crimes.

It is easy to overstate but impossible to deny that uniform national ID systems are a threat to our freedoms. Places like Nazi Germany, the Soviet Union, and apartheid South Africa all had very robust identification systems. Identification systems did not cause the tyranny or rank discrimination that overtook those countries, but identification systems were very good administrative systems that these oppressive regimes used.

Avoiding a national identification system is a bulwark against tyranny. If our identity systems are difficult to navigate, that provides us security against broken democracy. I

am very proud of our government and our system, but we should take care to protect ourselves by avoiding a national identification system.

Insecurity

As discussed above, identity fraud would be exacerbated by expanding Basic Pilot. A uniform national ID system would contribute further to this problem.

One reason why identity fraud is so easily engaged in today is that a Social Security number is pretty much the only key that one needs to access people's financial lives. Because the system is so simple and economically efficient, it is also efficient for criminals. They navigate our identity system easily and use the SSN, plus one or two other identifiers, to break into people's financial lives.

All of us are used to securing our physical assets with six, eight, or ten different keys that we keep on our key chains. It is a terrible security idea, ignoring the lesson we carry around in our pockets, to design a system that uses one key to control access to our intangible lives: our finances, communications, health care, and so on.

Many technologists, and of course governments, think that a single key is a great idea. It is true that a single-key system such as a "secure, biometric" Social Security card would work very well for institutions, but it would not secure the lives and privacy of individuals. Our identification systems should be diversified, not unified. Bringing all Americans within a national ID system is a massive undertaking that the rightfully independent and unruly American people will rightly resist.

The expansion of Basic Pilot would reduce illegal working some, at costs to American citizens in terms of suppressed legal working, higher taxes and more bureaucracy, and threats to privacy and data security. It would leave open a rather significant 'loophole,' though, doing almost nothing to connect truly verifiable identity information to the eligibility decision. The solution to this — and the ineluctable direction of an electronic employment verification policy — is to create a national ID system. This is anathema to American values.

Ultimately, the problem is with the policy of internal enforcement itself. For relatively small immigration control benefits, the costs of verifying eligibility are very high. The parties to the employment eligibility system are required to act against their interests, meaning they will always slow-walk compliance. The policy invites attacks on our already too fragile identity system. And the privacy and dollar costs fall on law-abiding citizens, not wrongdoers.

Instead of moving to electronic eligibility verification, the policy of internal enforcement should be eliminated, root and branch. The need for it can be dissipated, and legality

fostered, by aligning immigration policy with the economic interests of the American people. Legal immigration levels should be increased.

Ending Limited Government to Save It

Economics isn't everything. There are principles at stake here that should not be forgotten. Proponents of internal enforcement, electronic employment verification, and national ID systems believe strongly that people who come here in violation of the law should not enjoy this country's benefits. Were that the one founding principle of our nation, they would be right in all that they support.

But many other principles are at stake: the individual liberty and personal freedom of American citizens; the constitutionally mandated limits on federal power; low taxes, minimal regulation, and competition; privacy.

I will close by observing a small, but very symbolic change that electronic employment verification would make: Up to this point in our nation's history, decisions about who should work for whom have been made by employers and workers. Even under the IRCA regime as it stands now, employers make the selection of who they will hire, perhaps accepting some potential liability if they hire someone that is "ineligible." Letting workers and employers get together on their own terms makes eminent sense, just like people deciding for themselves what food they should eat and how their kids should be schooled.

But with nationwide electronic employment verification, we would move to a regime where the last word on employment decisions would not be with the worker and employer, but with the federal government. This is an extension of federal government power into an area where it has no business being. The founders of our nation and the Framers of our Constitution would spin in their graves to see what Congress is considering.

Proponents of internal enforcement and electronic employment verification surely have a sound principle that they stand on. But they have grown willing to sacrifice more important, founding principles for the less important goal of controlling illegal immigration — and ineffectively at that.