Electronic Employment Eligibility Verification: Franz Kafka's Solution To Illegal Immigration

by Jim Harper

Executive Summary

In last summer's debate over immigration reform, Congress treated a national electronic employment eligibility verification (EEV) system as a matter of near consensus. Intended to strengthen internal enforcement of the immigration laws, electronic EEV is an Internet-based employee vetting system that the federal government would require every employer to use.

Broad immigration reform failed before Congress thoroughly considered national EEV, but the lines of debate have been drawn. Advocates in Congress will try to attach a nationwide worker registration system to any immigration bill Congress considers, and the Bush administration recently announced steps to promote such a system. A mandatory national EEV system would have substantial costs yet still fail to prevent illegal immigration. It would deny a sizable percentage of law-abiding American citizens the ability to work legally. Deemed ineligible by a database, millions each year would go pleading to the Department of Homeland Security and the Social Security Administration for the right to work. By increasing the value of committing identity fraud, EEV would cause that crime's rates to rise.

Creating an accurate EEV system would require a national identification (ID) system, costing about $20 billion to create and hundreds of millions more per year to operate. Even if it were free, the country should reject a national ID system. It would cause law-abiding American citizens to lose more of their privacy as government records about them grew and were converted to untold new purposes. "Mission creep" all but guarantees that the federal government would use an EEV system to extend federal regulatory control over Americans' lives even further.

Introduction

More than a decade ago, a Cato Institute study opened with an urgent alert:

Republicans in the House and Senate are moving quickly forward with Orwellian legislation that would create a national computerized registration system for all American workers. The new federal computer worker registry, which is intended to reduce illegal immigration, is the crucial first step toward the implementation of a national identification card system for all 120 million American workers.[1]

In their paper, "A National ID System: Big Brother's Solution to Illegal Immigration," John J. Miller from the Center for Equal Opportunity and Stephen Moore of the Cato Institute called this system "an ill-conceived idea that would grant the government vast new police-state powers, require citizens to surrender basic freedoms and privacy rights,

and fail to halt illegal immigration." The leaders of virtually every libertarian, conservative, and civil liberties organization in America, they reported, had denounced the computer registry as "misguided and dangerous."[2]

Miller and Moore's study evidently educated policymakers and helped stave off such a system. Nevertheless, a pilot program begun then now threatens to resurrect the national computerized registration system they warned of, with all the big-government ills that surround it. A dozen years later, it is time to sound the alarm again.

In last summer's congressional debate on immigration reform, a worker registration and national identification (national ID) system was treated almost as a matter of consensus agreement. It remains a viable—even prominent— policy option in the immigration area, and legislation requiring national worker registration and a national ID system could advance with any immigration-related legislation moving through Congress. The Bush administration announced a number of steps in mid-August 2007 to promote registration and tracking of American workers.

About 10 years before Miller and Moore sounded the alarm in their Cato study, the Immigration Reform and Control Act of 19863 introduced the concept of "internal enforcement" into U.S. immigration law. IRCA conditioned Americans' ability to work on proving their legal presence and status in the country. This requirement was supposed to suppress illegal immigration by reducing the magnet of relatively high-paying work that brought such immigrants into the country.

But internal enforcement did not work. With employment in the United States still very attractive and legal opportunities for immigration restricted, people continued to come to the United States illegally.

Policymakers conveniently chalked up the failure of internal enforcement to weakness in implementation rather than to theory or design. They quickly set to strengthening internal enforcement rather than scrapping it. The creation of an electronic employment eligibility system called "Basic Pilot" in 1996 was one such measure. As Miller and Moore had pointed out, making it work would require a national ID card and massive databases of information about all American workers. Nevertheless, Basic Pilot went ahead, and it may soon move further forward.

Along with its Orwellian features, today we know that administering a system of electronic EEV would conjure Franz Kafka as well. A sizable percentage of workers—foreign- and native-born alike—would be denied the ability to work legally by a faceless federal database system. Deemed ineligible by the database, millions of American workers each year would have to present themselves at the Department of Homeland Security and the Social Security Administration, clutching their identity papers and pleading for the right to work.

Such a system would make working in the United States more difficult, of course, but it would not eliminate the United States' attraction to immigrants. Some potential illegal

immigrants would change their plans, but others would respond quite differently. Some workers and employers would collude to avoid this immigration enforcement system. Work "under the table" would increase and, along with it, other forms of illegality.

The value of committing identity fraud would rise, and more illegal immigrants would commit this crime or deepen the minor frauds they are now involved in. Criminals and criminal rings would use the Social Security number (SSN) data from stolen laptops and hacked databases much more often in identity fraud as a robust black market for Americans' personal information emerged.

The use of these data to fabricate mock identities would compound the problem for victims in a diabolical way. Seeking to prove their right to simple employment, American workers would have to appeal to bureaucrats who assume they are identity thieves.

Miller and Moore were correct: creating an accurate federal EEV system would require a national ID system. Such a system would have extraordinary costs. About $20 billion would be the tally for implementing a national ID system, some of that cost hidden in taxes, some of it paid directly by each national-IDcarrying worker. Operating the verification program would cost at least $300 million to $400 million per year.

The cost in lost privacy to all Americans would be high. Both employers and the government would have to collect and store personal information about American workers that is not necessary for employment—only for administration of employment laws and regulations. Kept in digital form for long periods, this personal information could be readily converted to untold new purposes.

Even if this system were workable and costeffective, we should not want it. "Mission creep" all but guarantees that the federal government would use a worker registration and surveillance system to capture greater regulatory control over Americans' lives. Ultimately, all kinds of transactions that are now personal and private, or matters of state or local law, would become subjects of federal government authority.

Partisan control of Congress and the presidency has reversed since Miller and Moore attacked the Republican plan to register all American workers in 1995, but national-IDbased worker surveillance seems alive and well under a Democratic Congress. More clear than ever are the sound reasons why electronic employment eligibility verification (EEV) and "internal enforcement" should be rejected.

Dysfunctional Immigration Law Begets EEV

The nation's immigration policy is at a crossroads. According to Labor Department projections, the U.S. economy, which is already near full employment,[4] 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 sales. Yet from 1996 to 2004, the number of adult Americans without a high school education—the demographic that typically fills those jobs—fell by 4.6 million.[5]

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

Just as water follows the laws of gravity, workers continually move to the United States. Unlike water, however, which simple barriers can stop, 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. Thus, migration into the United States has persisted over the last several decades.

Today, however, the political consensus holds that the country has too many immigrants and that something must be done about it.[6] A part of that consensus is that internal enforcement of immigration law should be strengthened, including by electronic employment eligibility verification. EEV requires employers to run background checks with the government on new or existing employees to see whether they are eligible to work under the immigration laws.

A full-fledged EEV system has many practical and technical problems, to say nothing of the question of whether it is appropriate for a free country. But the human forces that a policy would channel or counteract are the most important influences on how the supporting technical system must be designed. Those forces determine where the challenges the system will come from and what the human and monetary costs will be if it is to work for its intended purpose. Immigration law—today deeply at odds with Americans' interests—is the source of the problem and the starting point for analysis.

America's Original Open Borders Close

At the time of the founding and during the early part of U.S. history, the country's immigration policy was one of open borders. Naturalization rules fluctuated, and the law authorized the president to expel dangerous foreign nationals, but immigrants were welcome.

Indeed, in 1864, because of a labor shortage caused by the Civil War, Congress passed legislation to encourage immigration. It allowed enforcement in U.S. courts of the agreements immigrants had made in their home countries to repay their travel costs from wages earned in America. The law also established a federal government office in New York City to help immigrants reach their interior U.S. destinations.[7]

In 1875 Congress passed the first law to exclude people, aimed at convicts and prostitutes. The practice of exclusion was promptly adapted to racial and ethnic prejudice by 1882's Chinese Exclusion Acts, and, in the 1920s, a national-origin quota system greatly restricted immigration from countries outside northern and western Europe. National-origin quotas persisted until 1965 when the Immigration and Nationality Act

Amendments initiated a sevencategory system for family reunification and employment-based categories.

By the 1980s, the United States was seeing a strong flow of immigrants from Mexico and Central America. This paralleled earlier flows from Germany, Ireland, Italy, and elsewhere, but these immigrants could enter through uncontrolled parts of a land border without documentation. In 1986 Congress determined that illegal immigration rates were too high, but in passing the Immigration Reform and Control Act,[8] Congress failed to recognize either the power of the economic forces underlying such immigration or its benefits.

While legalizing the illegal aliens in the country, Congress declined to expand legal channels for immigration. Instead, it changed the long-standing natural rule that working in the United States depended simply on willingness and ability. Americans' right to earn an honest living by trading their labor would now have to wait for proof of compliance with federal immigration laws.

"Internal Enforcement" and "Basic Pilot"

IRCA made unlawful the knowing hire of workers who are not eligible to work in the United States under the immigration laws.[9] By requiring employers to check employees' documentation, the law conscripted employers into immigration law enforcement. All employers today are required to verify employees' work eligibility by collecting completed I-9 forms and by checking employees' documentation.[10]

The logic behind this idea was simple: making it illegal to hire an illegal immigrant could reduce the strength of this country's economic "magnet." But the policy of "internal enforcement" built on this simple logic failed. Just as a magnet's attraction passes through paper, the attraction of the United States to immigrants surpasses this paperwork.

The I-9 process and employer sanctions undoubtedly had some effect on illegal immigration and working, but not very much. Between 1986 and 1996, illegal immigration rates appear to have remained steady.[11] Document fraud undermined the I-9 system, and the law prompted some employers to discriminate wrongly against citizens and legal immigrants because of their Hispanic surnames, poor English-language skills, or appearance.

Ten years later, with illegal immigration continuing apace, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996[12] sought to "improve on" the failing policy of internal enforcement. It required the Immigration and Naturalization Service to commence three pilot programs to test electronic verification of employees' work eligibility. These were the Citizen Attestation Verification Pilot Program, the Machine-Readable Document Pilot Program, and the Basic Pilot Program. These three programs were intended to test whether verification procedures could make the existing Form I-9 process better by (1) reducing document fraud and false claims of U.S. citizenship, (2) discouraging discrimination against employees, (3) avoiding violations of civil liberties

and privacy, and (4) minimizing the burden on employers to verify employees' work eligibility.13

The Citizen Attestation Verification Pilot Program allowed workers to attest to their citizenship status. The status of new hires attesting to being work-authorized noncitizens was electronically checked against information in INS databases. Unsurprisingly, ineligible workers simply attested to being citizens. Employers did not ferret out this kind of fraud. Many did discriminate against work-authorized noncitizens, however, 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.

DHS initiated the Machine-Readable Document Pilot Program in Iowa because that state issued driver's licenses and ID cards carrying the information required for the I-9 in machine-readable form. Nevertheless, 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 SSNs on driver's licenses, which was done in the interest of protecting Iowans' privacy and data security. DHS terminated the Machine-Readable Document Pilot Program in 2003 as well.

Basic Pilot—first renamed the "employment eligibility verification" program, or EEV, and then renamed again, "E-Verify"—is the remaining effort to verify work eligibility electronically. As of May 2007, about 9,000 of the 17,000 employers registered for the system were active users.[14] Currently, about 52,000 of the country's 5.9 million employers have registered for it—about .88 percent.[15] Congress extended the Basic Pilot program in January 2002[16] and again in December 2003.[17] It is currently set to expire in late 2008.

How Electronic Employment Verification Works

After collecting I-9 forms, participating employers enter the information supplied by workers into a government website. The system compares these data with information held by the Social Security Administration and with DHS databases. If the name and SSN pairs match to citizen data at the SSA, a worker is approved. The system compares information from noncitizens with DHS data to determine whether the employee is eligible to work.

E-Verify electronically notifies employers whether their employees' work authorization is confirmed. Submissions that the automated check cannot confirm are referred to U.S. Citizenship and Immigration Service staff in the Department of Homeland Security, who take further steps to verify eligibility or who find the worker ineligible.

When E-Verify 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 eight working days by contacting the SSA or DHS.

When a worker does not contest his or her tentative nonconfirmation within the allotted time, the E-Verify program issues a final nonconfirmation for the worker. The employer is required to either immediately terminate the worker or notify DHS that it continues to employ the worker—confessing to a law violation.

The Administration Pushes EEV

The administration recently began to expand the federal government's use of E-Verify and instituted measures to increase private employers' verification of workers' immigration status. On August 10, 2007, Homeland Security secretary Michael Chertoff and Commerce secretary Carlos Gutierrez announced a number of steps to tighten and expand employment eligibility verification.[18] Among other things, they proclaimed the commencement of a rulemaking to require all federal contractors and vendors to use E-Verify. Full compliance would expand participation in the program by some 200,000 companies, a more than 20-fold increase to about 3.5 percent of all U.S. employers. Numerous bills have been introduced in Congress to promote EEV in various ways,[19] and the administration will attempt to convince states to do the same thing.[20]

Secretaries Chertoff and Gutierrez also announced DHS's issuance of a "no-match" regulation increasing employers' liability if their workers' names and SSNs do not correspond to SSA records.[21] Plans to "update" the civil fines for hiring illegal immigrants would raise penalties by 25 percent and expand criminal investigations of the country's employers.

Secretaries Chertoff and Gutierrez further declared that the administration would seek to expand the data sources E-Verify can check, including visa and passport information. They will seek access to state motor vehicle department records and photographs to "lay the groundwork for further expansion" of the electronic employment eligibility verification system.[22]

Finally, they announced that the administration would publish a regulation to reduce the number of documents that employers could accept for I-9 forms or E-Verify. The regulation could reduce the number all the way down to a single, nationally uniform ID.

The major immigration reform bill debated in Congress last summer would have required new hires to have a REAL ID Act– compliant card for employment eligibility purposes within three years.[23] REAL ID is the troubled 2005 national ID law that many states have declined to implement. Debate on the immigration bill collapsed when the Senate appeared willing to strip REAL ID from the bill[24] and an amendment calling for $300 million in spending on REAL ID failed.[25] Seeking to revive this moribund national ID law, however, the administration may try to do by regulation what Congress would not do in legislation.

Along with promoting EEV and worker registration by any means, the administration has worked to wear down resistance in various ways. Administration officials have lobbied state officials to go along with the national ID law.[1] And in late September 2007, the

U.S. government sued the state of Illinois, seeking to nullify an impediment that state had placed in the way of the administration's EEV plans.[27]

In an entry on the DHS's new "Leadership Journal" blog, Secretary Chertoff announced the lawsuit, asking: "Could it be that the Illinois state legislature wants to prevent businesses from using the best available tools to determine whether new employees are illegal aliens? I certainly hope not, but that's precisely what a new state law is poised to do."[28]

In fact, the Illinois Right to Privacy in the Workplace Act bars Illinois employers from enrolling in E-Verify or any similar system until the SSA and DHS can make final determinations on 99 percent of their tentative nonconfirmation notices within three days. In other words, if the system will prevent Illinois workers from working, the state wants nothing to do with it.

Difficulty of administration is one of several formidable problems with trying to build an EEV system for federal immigration law enforcement. Creating a nationwide system for checking identity and eligibility is *much* more easily said than done.

Franz Kafka's Solution to Illegal Immigration

A nationwide EEV system would send a substantial number of workers—native-born and legal immigrant alike—into labyrinthine bureaucratic processes, preventing them from working until the federal government deemed their papers to be in order. It would be more like something out of a Franz Kafka novel than a sound U.S. federal policy. EEV would delay or deny the employment of American workers in numerous ways.

Screening Workers Screens Out Workers

Think of electronic employment verification as a screen through which all workers would have to pass before they could earn a living. The problem is to get eligible workers through the screen quickly and to keep ineligible workers from passing through. It is hard to do both at the same time. The federal government currently has only fragments of the infrastructure for accomplishing this goal, and the processes for doing so are rife with flaws.

For example, simple errors in transcription and data entry by employees and employers will create a baseline wrongful tentative nonconfirmation rate. According to a recent survey of employers participating in Basic Pilot, 52 percent had received at least one tentative nonconfirmation for a new employee caused by data entry mistakes.[29]

Then we must consider the error rate in federal government databases. In December 2006, the SSA's Office of the Inspector General estimated that the agency's "Numident" file—the data against which Basic Pilot checks worker information—has an error rate of 4.1 percent. Every error resulted in Basic Pilot's providing incorrect results.[30] At that rate, 1 in every 25 new hires would receive a tentative nonconfirmation. At 55 million

new hires each year,[31] this rate produces about 11,000 tentative nonconfirmations per workday in the United States—a little more than 25 people per congressional district, each day of the working week, all year long.

Knocking Rungs off the Ladder

No illusions should be harbored about the impediments to working that this system would create if expanded to a national scale. Even the "simple" process of clearing up basic data errors would carry with it formidable problems.

Consider this hypothetical scenario that illustrates the trouble an ordinary worker might have with the EEV program: Peggy Smith is a single mother of two, born and raised in the Midwest town where a new Big Store recently opened. On Tuesday afternoon, retail chain the Big Store calls Peggy to tell her it has accepted her application to work as a sales clerk trainee.

The new job is a coup for Peggy because she has struggled diligently to get her high school equivalency degree while making ends meet since her husband was killed in a car crash. She will start work the following Monday with a two-week (paid!) training course that is given at the store once a quarter.

On Thursday afternoon, she comes in to the human resources office, her two middleschool- age children in tow, with the documentation necessary for her Form I-9. Human resources enters the data into the EEV system just before the close of business Thursday, finding that Peggy is a tentative nonconfirmation. Human resources calls her to tell her about the problem Friday morning, but she cannot make it back to the store to collect the written instructions on how to appeal her nonconfirmation before the weekend.

On Monday, arriving early for training, Peggy is presented with instructions for appealing her nonconfirmation. The instructions tell her to visit a Social Security Administration office that is 30 minutes away. The SSA office is open Monday through Friday from 8:30 a.m. to 5:00 p.m. Her usual shift and the training sessions are from 8:00 a.m. to 4:30 p.m., and she must pick up her kids from their after-school activities most days of the week.

The EEV program's requirements do not permit employers to delay training or an actual start date based upon a tentative nonconfirmation. [32] Even if Big Store could delay her start date, Peggy does not want to forgo a quarter's work by missing the training that each new clerk trainee gets. Hoping that the problem will go away, Peggy attends the Big Store training sessions each day. Because she has not appeared at a government office to contest her nonconfirmation within eight days, the EEV system issues a final nonconfirmation to the Big Store, and Peggy is fired.

Welcome to the Jungle

Even if Peggy were somehow confident enough with her employment situation to get time away from training, and even if this recent recipient of her GED were familiar enough with the procedure for contesting a tentative nonconfirmation (while juggling childcare), the unwelcoming and inefficient processes she would encounter at the federal government's offices should not be lightly dismissed. Disputes of tentative nonconfirmations would not happen in lushly carpeted offices with marble columns, hot coffee, and friendly, attentive staff. The experience of American workers when they sought permission to work would be much more like their trips to the nation's departments of motor vehicles, post offices, and dentists— long lines, unfriendly service, and painful procedures.

Some evidence indicates what American workers would experience when they went to clear up their tentative nonconfirmations. At the beginning of 2007, a new travel restriction was imposed on all persons traveling by air between the United States and Western Hemisphere countries. Americans visiting these nearby neighbors are now required to present a passport to reenter the United States, formerly not required if other proof of a right to reenter was available. This requirement was an opening step in the implementation of a program called the Western Hemisphere Travel Initiative, which— for little security benefit— will eventually require all Americans visiting local neighboring countries to carry a passport. [33]

The new rule drove a crush of Americans to passport offices seeking travel documents and caused delays in processing of up to a month and a half, even though the State Department had augmented its staff.[34] Travelers across the country had their plans thrown into doubt, and they angrily besieged State Department offices. The bill for the increased demand for passports has been estimated at $1 billion for just three years.[35]

The passport issuance process is a loose parallel to the probable system for contesting tentative nonconfirmations. Although the number of tentative nonconfirmations may not be as high, the EEV system would be expected to handle about a million transactions each week, with more than 2 million of those getting further review as tentative nonconfirmations each year.

It gets worse. For a significant number of American workers, challenging tentative nonconfirmations would not be just a matter of presenting their documents and cleaning up the data in government systems. Counterattacks on the system would complicate things. Many law-abiding American citizens would enter SSA and DHS offices as criminal suspects and potential candidates for deportation.

Counterattacks and Complications

Immigrants and employers dedicate their ingenuity to getting what they want and need. Although a national EEV system would reduce the growth in illegal immigration by some measure, it would also prompt illegal immigrants and some employers to undertake a variety of countermeasures.

For example, more people would work "under the table." Workers and employers would collude—even more often than they do now[36]—to avoid the already substantial regulatory hassles and costs of working on the books. With the increased liability for employers who did comply with the Form I-9 process (the updated penalties noted earlier), following the letter of the law would be riskier, and violating the law by going underground would be relatively more attractive.

Avoidance of EEV would be one result of strengthened internal enforcement. But a variety of counterattacks on the EEV system would be part of the response as well. They would create extraordinary new costs and complexities that would burden U.S. workers while weakening EEV's deterrence to illegal employment and immigration.

Counterattack, Response, and Counter- Counterattack

One counterattack on the EEV system that illegal immigrants would adopt is a mere shift in strategy. Today, many submit false documentation of plausible names and SSNs for the Form I-9 process. This technique would not pass EEV, of course: the name and SSN must match in the SSA's records.

In response, illegal immigrants would adjust their frauds so that they use name and SSN pairs that match. It is slightly more difficult to do but easily worthwhile to procure "legal" work.

To respond to this attack, the EEV system would monitor the use of name and SSN pairs. When a name and SSN were used too often in succession, or in different parts of the country, the system would "flag" the name and SSN pair. Its users would be suspected of fraud, and they would be tentatively nonconfirmed.

However, this response would have costs. One, of course, is that it requires a federal database that records every new hire in the country— yet another of many incremental increases in the tracking of law-abiding Americans. None of them are terribly objectionable by themselves, but the totality is quite concerning.

A more immediate cost is that law-abiding citizens would regularly stand accused of identity fraud. The SSA and DHS would not know which user of a name-SSN pair was the genuine person and which was using a false identity. EEV would tentatively nonconfirm all users of that name-SSN pair. The "true" individuals attached to fraudulently used identities would learn of identity fraud in their names when they were refused work by EEV and plunged into a bureaucratic morass.

Today, identity fraud creates financial difficulties for innocent victims when they find that their financial reputations have been sullied. EEV would also make them unemployable.

Illegal immigrants would counterattack in response to the tracking of name-SSN pairs by using *original* name-SSN pairs with each new hire. EEV would cause illegal aliens to

seek out name-SSN pairs that have not been used recently in employment. It would create a bigger criminal market for American citizens' personal information.

Since 2005, the Privacy Rights Clearinghouse has been collecting information about data breaches that could expose individuals to identity theft.[37] Not all of the breaches it includes in its study concern both name and SSN—some have financial account numbers, driver's license numbers, and other key identifiers— but by late 2007, more than 200 million records had been breached.

Currently, data breaches rarely result in identity fraud. A June 2007 Government Accountability Office report found evidence of identity fraud resulting from relatively few breaches.[38] Today, victims' family members and friends, household employees, and financial services personnel with access to sensitive personal information are often the perpetrators of identity fraud. By creating new demand for name and SSN pairs, EEV would increase the value of breached identity data and the rate of identity fraud. The casual criminals who now produce fake IDs for illegal immigrants would organize information networks to meet the demand for "fresh" names and SSNs.

These networks might steal legitimate companies' logins and human resources data, enrolling shell companies in EEV to ping the database for usable sets of identifiers. Using the photo-screening tool (discussed below), they might collect thousands of photos from which each illegal immigrant could select the citizen he or she most resembles to impersonate with forged documents.

Yet another attack on the EEV system would be to corrupt the federal employees who handle tentative nonconfirmations. As so often happens in departments of motor vehicles (DMVs) across the country,39 criminals would find federal workers willing to use their access—or fellow workers' logins—to "confirm" people operating under false identities. Doing so may well exclude from work the people whose identities are being used.

Consider also how employers would protect themselves. With illegal immigrants today coming predominantly from Spanishspeaking countries south of the U.S. border, identity fraud and corruption attacks on the EEV system would focus largely on Hispanic surnames and given names. Recognizing that Hispanic employees—even native-born citizens— are more often caught up in identity fraud and tentative nonconfirmation hassles, employers would select against Hispanics in their hiring decisions. New hires from other ethnic groups would be less likely to bring employers such trouble—to say nothing of the updated penalties previously discussed. The wrongful discrimination that the Basic Pilot program was supposed to suppress would increase under EEV because of counterattacks on the system.

Shockingly, the current E-Verify program has no process for appealing final nonconfirmations. The DHS Web page with information "for employees" provides no advice to workers who believe they have been wrongly refused the right to work by DHS.40 A nationwide EEV system would wrongly give thousands of eligible American

workers final nonconfirmations each year, with no apparent appeal process, blatantly depriving them of due process and, of course, their livelihoods.

Not all the ills that EEV would cause American citizens are easy to predict. Along with those discussed here, others would appear in any full-scale implementation. The consequences of scaling up a small program like Basic Pilot/E-Verify should not be underestimated. It has many flaws at its current size, but taking the program national would be a change in kind, not in degree. It would create new and different problems.

The employers in Basic Pilot/E-Verify now are relatively well equipped and motivated compared to the variety of employers that an expanded EEV system would encounter. Most small businesses have no personnel dedicated to compliance. Many businesspeople are rarely connected or not connected to the Internet, because of remoteness, cost, or lack of business necessity. The compliance and accuracy rates experienced in an expanded program would be lower than what exists now, and discrimination rates would be higher.

Known or unknown today, the infirmities in EEV and the counterattacks on a full-scale system would weaken it as a tool for reducing illegal immigration. They would promote wrongful discrimination. Moreover, they would plunge a significant number of nativeborn American citizens into Kafkaesque federal bureaucratic procedures, denying them work and money to feed their families until a federal government database says they are allowed to do so.

EEV, National ID, and Worker Surveillance

People angered by illegal immigration are undoubtedly frustrated that internal enforcement works so poorly and that our systems provide so little security against people entering the country illegally. This is simply because big, uniform identity systems do not work well. As Phillip J. Windley, the former chief information officer of Utah, observes in his book *Digital Identity*:

Visions that a centralized approach will promote security, cost savings, or management simplicity are a mirage. Centralized digital identity systems do not scale. Identity relationships are inherently web-like in structure, while centralized technologies like directories are hierarchical.[41]

In other words, identity works well in oneon- one transactions, in groups, and in voluntary organizations. People and businesses naturally collect the identifiers and other information they need for meetings, contracts, dates, employment, friendship, and so on. But people do not have a single identity that can be captured and applied to all their relation- ships.[42] As Windley points out, relationships define the many different identities people have.[43] Identities do not define relationships— at least not in a modern, free country.

Bringing Americans into a uniform government identity system—for controlling illegal immigration or any other purpose—would make people's relationship with government one of the foremost in their lives. It would be an attempt to force a relationship on them

that many do not want. But a successful EEV system— indeed, successful internal enforcement of federal immigration law—requires this kind of overweening, unworkable, and unacceptable identity system.

Several bills introduced in recent Congresses have proposed establishing federal EEV systems but have denied creating a national ID card, saying things like, "Nothing in this Act shall be construed to authorize, directly or indirectly, the issuance or use of national identification cards or the establishment of a national identification card." Establishing a national EEV system without a national ID card is nearly impossible, and the national-ID denials in these bills have been false.[44] All proposals and plans to improve the Form I-9 process—whether or not by going electronic—show that internal enforcement of federal immigration law requires a national ID.

I-9s and Identity

In personal interactions, people use identification constantly. When they have met before, people are very adept at recognizing each other again using their sight, hearing, and other senses. This facility enables people to pick up where they left off when they see each other a second, third, and fourth time. The success and familiarity people have with in-person identification may give policymakers excessive confidence in identification's power in other contexts.

Currently, U.S. employers must collect and examine identity and eligibility information from all employees at the time of hire. They can do so 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 Social Security card. The employer must attest, under penalty of perjury, that it has examined the documents and found they appear to be genuine and that the employee appears eligible to work in the United States.

The conversion of every small businessperson and human resources director into an immigration agent surely hides the cost of the enforcement regime, but it does not necessarily work well to combat illegal employment. For example, employers often fail to accurately identify their workers, hiring unauthorized workers despite faithfully carrying out their duties under the law.

The opening of the employment relationship is not like ongoing personal relationships. Particularly in low-skill jobs, the new employee proffers his or her identity for the first time as the relationship begins. The employer has little reason, and takes little time, to examine the applicant's identity bona fides.

At this early point in the relationship, however, the law 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 works so well in families. Employers identify their new employees using ID cards.

Identification by Card

The process of identifying someone by card is important and valuable, allowing people to be treated as "known," to a degree, from the first encounter. But the identification-by-card process is also fraught with weaknesses that can undermine the process when it does not benefit both parties. Figure 1 illustrates the three steps by which a card transfers identity information from the ID subject (the cardholder) to the ID verifier (or relying party).

First, the subject applies to a card issuer (such as a DMV) for a card, typically supplying nearly all the personal information the card will contain. Next, the card issuer creates a card, supplying information to any later verifier. Finally, the verifier compares the card to the person presenting it. Having veri- fied that the card is about the subject, the verifier accepts the information on the card.

Each of these three steps is a point of weakness and an opportunity for false information to creep in. In the first step, the subject may supply the card issuer with false information (including false documents), or the subject may corrupt employees within the card issuer, causing them to issue a genuine, but inaccurate, card. A fraudulently or corruptly acquired genuine card will almost certainly deceive any later employer.

At issue in the second step is the security of the card against forgery or tampering. Although 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 and altering them. Employers, who would be acting against

their interests to discover such things, cannot be expected to discover forgery or tampering of any decent quality.

A photo-screening tool pilot program recently initiated by DHS is intended to detect certain forgeries.[45] When a noncitizen new hire presents a DHS-issued permanent resident card or employment authorization document, employers in this program are required to compare the photograph on the card to a copy of the photograph appearing on the employer's computer screen via the EEV system. If the photographs do not match, the employee is issued a tentative nonconfirmation.

This crosscheck does not solve the hard problem—people entering the ID system through fraud or corruption—but it does provide security against one type of forgery attack on the EEV system. DHS desires to collect passport photos from the State Department and driver's license photos from DMVs around the country to expand this program from DHSissued documents to all Americans' passports and driver's licenses. This expansion, of course, involves creating a national photo-ID database.

The photo verification tool may cause employers to spend a little more time considering the appearance of the new hire, but just as likely, employers will believe that comparing the images on the card and computer is all they need to do. That procedure does nothing to establish whether the person presenting the card is the person it was issued to. What matters is that the picture on the card is a picture of the person presenting it.

This is the third step in the identificationby- card process, comparing the identifiers on a card to the subject. Here, as in the second step, employers will not be terribly eager to discover deception, such as someone presenting the card of a person similar in appearance. A number of factors explain why the verifier check is weak in the employment context. People are better at recognizing faces of their own race and familiar races than faces that look different. Strong social pressures exist— from the fear of rudeness to the appearance of racism—not to second-guess the picture on the card a person has presented. The third step in the identification-by-card process is another weakness.

The Ideal Fix? Cradle-to-Grave Biometric Tracking

Each of the steps can be shored up, of course, and some of them would be strengthened in small ways by elements of EEV. But the things necessary to make a system like this really impervious to forgery and fraud would convert it from an identity system into a cradle-to-grave biometric tracking system. Almost no way exists to do national EEV that is not a step down that road.

Let us take the identification-by-card process and assess what is necessary to make it hold up against the frauds, forgeries, and other weaknesses that undermine EEV:

Verification of identifiers, the verifier check that ties the card to the bearer, can be strengthened and improved. Rather than relying on the fallible human perception used in

verifying photo-ID cards, an "improved" EEV system would use modern biometric measuring of each American, such as by fingerprint readers or iris scanners. Were every American biometrically registered, the biometric information embedded in their cards— retrieved from the card, retrieved from the human, and compared by machine— could provide much stronger assurance to verifiers that cards are about the people presenting them.

The security of cards against forgery and tampering (the concern raised in the second ID-by-card step) can be improved vastly with a variety of techniques, especially by using encryption. Printing or embedding information in a card using cryptographic techniques can establish with a high degree of certainty that the information was placed there by a particular agency and that it has not been altered since it was placed there. This technique can, however, conceal from the ID subjects themselves what is on the cards they must carry and display. The photo-screening tool pilot program is a very crude, noncryptographic version of this kind of security, showing that the photo on a card has not been replaced or altered.

The veracity of the information that makes it onto a card may be the most challenging element to improve. After all, the information on identity cards is a collection of biographical data—name, date of birth, address, height, weight, and such—that is not easily verifiable. Names change or hyphenate, for example, as people marry, divorce, and remarry.

The way to ensure that accurate data are found on a card is to abandon the current practice of allowing applicants for identity cards to submit information about themselves. Rather, identity information and records of important life events could be cataloged from birth (or a person's first entry into the country) using powerful machinereadable biometrics, all the way up to DNA, as "index card" identifiers. The photo-screening tool is a step in this direction: it begins to make the dossier as important as the card.

Applicants for cards could submit some of the information, but the core identity information on each card would have to be tied to a central biometric identity repository— probably run by the government. Reliable biographical information would have to be collected and stored by this repository. This system would deny potential fraudsters the ability to submit false information to ID issuers, and it would suppress their frauds.

This excursion into an "ideal" employment eligibility system shows where internal enforcement of immigration law almost invariably leads: to a national, cradle-to-grave, biometric tracking system—a national ID and surveillance system. IRCA could be administered without these things, but the chances of that being done are very, very slim.

A Narrow, Nonidentifying Alternative

A credential such as eligibility for employment under IRCA can be proved without creating a nationwide biometric tracking scheme. In fact, templates already exist. But it is unlikely to see adoption.

The Transportation Security Administration's Registered Traveler program currently accepts privately issued documents like the Clear card[46] from Verified Identity Pass, Inc., to prove a person's membership in RT. The Clear system is designed so that it does not create records of travelers' use of the system, even as it provides biometric proof of their membership in RT using iris and fingerprint scanning.

A similar system could verify employment eligibility without surveillance and tracking. The government agency or other credential provider would have to examine applicants' proof of citizenship (and noncitizens' proof of eligibility) and, *without making copies of these documents or of the person's biometrics*, issue a biometric card or token that indicates to verifiers only work eligibility and any time limits on that eligibility. When a person was hired, a biometric tie to records securely stored on the card or token would indicate his or her eligibility for employment.

As simple as such a system would be, strong government resistance makes it very unlikely that it will see the light of day. The TSA currently requires that Clear card users present government-issued ID at airports, for example, even though the Clear system presents biometric proof of RT membership based on a government-issued ID that the Clear user previously presented. (Verified Identity Pass CEO Steven Brill has charitably characterized the TSA's defenses of this double- ID rule as "plainly absurd.")[47]

Governments have strong interests in tracking people, for both legitimate and not-so-legitimate reasons. Many government programs accord rights and benefits based on biographical information that must be recorded, maintained, and periodically checked. For the vast majority of people, however, employment eligibility under IRCA is not such a program. Most workers in the United States who are citizens will be eligible to work under IRCA for their entire lives. Maintaining data about them after a biometric work-eligibility card has issued would not serve any administrative purpose.

Nevertheless, the government would not accept a tracking-free system for two reasons. First, a system like EEV "requires" identification and tracking to shift the risk of error in the card-issuance process from the government to the citizen. A wrongly issued workeligibility card that does not also publicly identify the bearer could not be cancelled or recalled if it were issued because of mistake, fraud, or corruption. All cards would have to be replaced if the government had failed to administer its system well.

Second, tracking preserves government power. A work-eligibility and tracking system such as EEV makes the individual's employment eligibility subject to revision at a later time, if the government wants to change the rules or adapt the system to new purposes, for example. A nonidentifying work-authorization card or token denies government the power to change its policies without the expense and effort of reissuing all cards or tokens.

Governments are averse to accepting the risk of error, and they rarely exhibit the discipline needed to avoid tracking of people who interact with their programs.[48] Unless the federal government can accept the risk of error and is willing to commit to lasting employment eligibility rules, it will require any internal enforcement program to use databases and tracking rather than just issuing cards that prove eligibility to work and nothing more. It will push Americans toward a national ID and worker surveillance system.

Some people claim that they would prefer a national ID and this kind of surveillance to attack the scourge of illegal immigration. But the costs of such a system—in American citizens' dollars, in privacy, and in lost American values—would be substantial, even as it failed to curtail illegal immigration.

An EEV Tax, Privacy Undone, and Mission Creep Unleashed

Were the national ID system necessary for effective EEV put in place, employers could do somewhat reliable verification of employment eligibility, but the system would impose many costs on the country and society. The dollar costs of a nationwide EEV system would be high. EEV would have far greater privacy consequences than the current system—consequences that would fall on American citizens, not on illegal immigrants. And, once in place, an EEV system would be used for everything from health care to gun control. Expanded EEV 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—indeed, by a federal database system.

Costs in Taxpayer Dollars

In December 2005, the Congressional Budget Office estimated the costs of the electronic employment verification system in HR 4437, an immigration reform bill in the 109th Congress.[49] Those costs were substantial.

Under the Basic Pilot expansion in that bill, CBO found that 50 million 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, DHS and the SSA would have had to spend approximately another $100 million per year on new personnel. The federal government, states, localities, and private businesses would all have 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.

The national ID system required to do EEV at all well would be even more expensive. The REAL ID Act—our moribund national ID law—is a first step toward the

comprehensive national ID system that would be needed to do EEV successfully. In proposed regulations for the REAL ID law, DHS estimated $17 billion in costs to implement REAL ID.[50]

About $11 billion of those implementations costs would fall directly on state governments. Because states already have functioning DMVs, this increment is the low end of the spectrum. Were the SSA or some other federal entity to create an identity infrastructure from scratch, the costs would be tens of billions more.

The public would bear the other $6 billion of REAL ID implementation costs in navigating the new bureaucracy and red tape needed just to get a driver's license. Individuals would have to dig up birth certificates or get copies from public records offices (some of which may not exist any more, such as in New Orleans). Native-born American citizens who may never have traveled overseas would need to search for proof of "legal presence" in the country. Americans would stand in very long lines at DMV offices. A DHS analysis detailed the 10-year time-costs of REAL ID to citizens, estimating 161.9 million hours preparing applications, 26.5 million hours obtaining birth certificates, 15.8 million hours obtaining Social Security cards, and 64.7 million hours on DMV visits.[51]1

The smallest movement in the direction of a national ID has revealed the kinds of problems that would arise from attempting to herd Americans into the identity system needed for EEV and internal enforcement. Alabama is a state that tried to get ahead of the REAL ID Act's mandates in 2006. Attempting simply to match up the names in SSA databases with motor vehicle bureau records, Alabama sent letters to individuals whose records were mismatched, asking them to correct the "erroneous" information on their driver's licenses. Thousands of panicked Alabama residents jammed Department of Public Safety offices thinking they would lose their licenses.[52] Such problems would multiply dramatically should the national identity infrastructure needed for EEV ever be created.

American Citizens' Privacy

The American-citizen taxpayer would incur not only 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 and the security of personal data.

When an employer collects 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 digital data breaches that so regularly come to light.

When an organization enters I-9 information into a Web form and sends it to the SSA and DHS, that information is very easy for those entities to access, copy, share, and use. It is likely combined with "meta-data"—information about when the data were collected, from whom, and so on.

The EEV process would give these agencies access to a wealth of new data about every American's working situation. Because it uses the SSN, EEV data would easily be correlated with tax records at the Internal Revenue Service, education loan records in the Department of Education, health records at the Department of Health and Human Services, and so on. Americans living with EEV should not expect that they could get work if they were in arrears on any debt to the U.S. government, for example.

Unless a clear, strong, and verifiable data destruction policy were in place, any EEV system, however benign in its inception, would be a surveillance system that tracked all American workers. The system would 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.

Beyond EEV's direct costs, the identity system required to do EEV successfully entails further privacy costs and threats. The privacy and data security consequences arising from the necessary national ID, for example, are immense, increasingly well understood, and probably insurmountable.

The REAL ID Act requires states to maintain databases of foundational identity documents, creating an incredibly attractive target for criminal organizations, hackers, and other wrongdoers. They would have more motivation than ever to collect identity information should a nationwide EEV system control access to employment.

The breach of a state's entire database—or the whole country's—containing copies of birth certificates and various other documents and information could topple the identity system we use in the United States today. This is the risk posed by the recent colossal data breach in Britain, in which essential data about 25 million U.K. citizens were copied to discs, placed in the post, and lost.[53] The best data security is achieved by avoiding the creation of large databases of sensitive and valuable information in the first place. EEV would put Americans' sensitive personal information at risk.

The security of back-end systems is far from the only problem. Creation of a nationally uniform identity system as required for EEV would bring a major change in how American society would use identity. It is not just another in a series of small steps. The national ID required by EEV would promote tracking of, and data collection about, all citizens.

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. Uniform ID cards would have the same influence on the uses of ID cards.

Most driver's licenses today have machinereadable components like magnetic stripes and bar codes. Their types, locations, and designs— and the information they carry—differ from state to state. For this reason, they are not used very often. But if all identification

cards and licenses were the same, as under REAL ID, or if a national EEV card were used, economies of scale would exist in producing card readers, software, and databases to capture and use this information. Americans would inevitably be asked more and more often to produce an ID card and to share the data from that card when they engaged in various governmental and commercial transactions.

Others would capitalize in turn on the information harvested using national ID cards and collected in state databases. Massed personal information—publicly and privately held—would be an irresistible attraction to DHS and many other governmental entities, which would dip into deep wells of data about American citizens for an endless variety of purposes.

Many people believe they have nothing to hide and feel willing to have their employment tracked if it will stop illegal immigration. Unfortunately, it will not. Moreover, most people who make the nothing-to-hide claim balk when they are actually confronted with stark choices about privacy.

People have things to hide. Maintaining a private life is normal and natural. Indeed, many people object on principle to compilations of information about themselves, no matter who is doing it and no matter what the purpose. This is consistent with life in a free country, where law-abiding citizens can protect their privacy for any reason or no reason.

Any electronic employment verification system will be a target for hackers, a data breach waiting to happen, a threat to the identity system we rely on today, and a surveillance system for both corporate and government use. Even if many of these flaws in a national EEV system could be mitigated, it is not a system that Americans should want. A successful EEV system would see mission creep from its first day.

Mission Creep

If an EEV system reliably identified people and determined their legal status under federal law, federal authorities would waste no time in adapting it to new uses. In the immigration area alone, proposals have been made to regulate housing in the same way as employment. In Hazelton, Pennsylvania, for example, the demagogic mayor sought and passed a law in 2006 making it illegal for landlords to "harbor" illegal aliens.[54] In another 10 years, the failure of EEV to weaken the economic magnet of the United States might convince federal lawmakers that they must take this same step.

The right to necessities other than housing could be conditioned on legal status. Given the failure of employment restriction to deter illegal immigration, financial services could be denied to all those who cannot prove their lawful presence through an adapted EEV system. Federal legislation proposed in the 110th Congress would regulate the documentation that non-U.S. persons may use to open financial accounts in the name of terrorism and immigration control.[55] Legislation has also been proposed to encourage public colleges and universities to verify the immigration status of students.[56]

Enforcement of immigration law is just one of many uses EEV would be put to once established. Many things could be brought within the purview of federal authorities if a national system for tracking and controlling individuals were in place.

Health care is an area that would be ripe for electronic tracking. Whether to enforce immigration law, implement a health insurance mandate, create a national health records database, or carry out any other health policy vogue, the national tracking system created for EEV could be adapted to federal government priorities in the health arena. A DHS official recently suggested that a national ID be required for purchasing cold medicine.[57] An EEV system could take that policy a step further and deny medicines and other purchases to Americans without proper documentation.

The federal government might apply a national EEV system to gun control. When an EEV system exists, having purchasers of guns prove they are citizens or legally entitled U.S. residents would not be asking too much. Counting individuals' gun purchases would be easy with this database system, and it could record the number of guns and quantity of ammunition bought by any one person. Indeed, statistical analysis could show where an excess of weaponry was sold in any one area. Authorities might use the system to search for purchasers of too many guns, believing they are feeding the black market or perhaps caching weapons in a homegrown terrorism plot. Never mind that the same analysis would turn up law-abiding gun collectors and avid sportsmen.

Speaking of terrorism, the biometric card required for EEV would be readily adapted to the identity-based security programs that have grown up at airports since the September 11, 2001, attacks. Experienced travelers, having had time in line to think about it, know well that showing ID is very weak security against committed threats—people willing to kill themselves bombing an airliner are willing to identify themselves beforehand. But identification checks at airports make uninformed people feel safer, and having people show a nationally uniform biometric card would augment that exercise in security theater. It might also allow expansion of identity checking to malls, subway stations, office buildings, and other publicly accessible infrastructure. [58]

A national EEV system would be an avenue along which regulatory power over American citizens would flow to the federal government. It would draw vastly more information about Americans' lives into federal government databases, and it would expose their sensitive data to more security threats. The information-age crime of identity fraud would blossom under EEV because the value of breaking the uniform government identity system it requires would grow higher. Building the EEV system would cost billions and billions of taxpayer dollars, while saddling American workers and employers with regulatory burdens and criminal liability.

As an administrative tool, an EEV system would have to be nearly perfect to avoid having enormous negative effects on American workers and employers. EEV would wrongly screen out lawful American workers. Probable counterattacks on the EEV system mean that it will plunge law-abiding American citizens into Kafkaesque bureaucracy, preventing them from working until they can negotiate their way through

unwelcoming federal government offices. Unfathomably, today EVerify has no appeals process. Any national EEV program would be an intrusive, expensive incursion on the American workplace and the rights of American workers.

Conclusion

Bad policies are like cancer. They metastasize and occupy other parts of the body politic. Our country's immigration law has held an unnatural cap on new American workers' coming to the United States for decades now, and attempts to make a success of that bad policy have produced circumlocutions like "internal enforcement" and "electronic employment eligibility verification." These are additional cancerous nodes that threaten American workers with Kafkaesque bureaucracy, denied employment, a national ID system, and broad surveillance.

The "problem" most illegal immigrants present is their eagerness to enter our labor markets, provide goods and services for Americans' consumption, and grow the U.S. economic pie. Millions of otherwise honest, hard-working, and law-abiding people have come to the United States without documentation. Many want very badly to follow the same path our forefathers did, and they would be a credit to this country if we made it legal for them to come. In a deep irony, Congress may soon expand EEV, increasing government spending and bureaucracy so that our maladjusted immigration law can continue to stifle U.S. economic growth.

Proponents of internal enforcement and electronic employment verification surely stand on a sound principle—the rule-of-law ideal that people should enter the country legally. But current immigration law is a greater threat to the rule of law than any of the people crossing the border to come here and work. Our immigration policies have fostered the illegality so common in the employment area.

Heavier internal enforcement would not reduce the illegality—it would promote it. Faced with the alternative of living in poverty and failing to remit wealth to their families, illegal immigrants would deepen the modest identity frauds they are involved in today. Their actions would draw American citizens, unfortunately, into a federal bureaucratic identity vortex.

For minimal gains in illegal immigration control, national EEV would sacrifice moreimportant founding principles: the liberty and personal freedom of American citizens; constitutionally mandated limits on federal power; low taxes, minimal regulation, and competition; and privacy.

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

Up to this point in our nation's history, employers and workers have decided who should work for whom. Even under the IRCA regime as it stands now, employers select whom they will hire, perhaps accepting some potential liability if they hire someone who 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 to school their children. With nationwide electronic employment verification, however, the United States would move to a regime where the last word on employment decisions would not be with the worker and employer but with bureaucrats in the federal government. This result would extend federal government power into an area where it has no business being.

Notes

[1] John J. Miller and Stephen Moore, "A National ID System: Big Brother's Solution to Illegal Immigration," Cato Institute Policy Analysis no. 237, September 7, 1995, http://www.cato.org/pubs/pas/pa237.html.

[2] Ibid.

[3] Public Law 99-603, codified at U.S. Code 8 § 1324a et seq.

[4] "Fed's Poole Says U.S. Economy Near Full Employment, Trade Not Destroying Jobs," Forbes. com, September 6, 2007, http://www.forbes.com/markets/feeds/afx/2007/09/06/afx4089152.html.

[5] Daniel T. Griswold, "Immigration Reform Must Include a Temporary Worker Program," Orange County Register, March 7, 2007, http://www.freetrade.org/node/600.

[6] The consensus is mistaken. See Daniel Griswold, "A Boon Rather Than a Burden," Politic.org, August 27, 2007, http://www.freetrade.org/node/741.

[7] Act to Encourage Immigration, 38th Cong., 1st sess. (July 4, 1864), U.S. Statutes at Large 13 (1864): 385–87.

[8] Public Law 99-603, codified at U.S. Code 8 § 1324a et seq.

[9] Ibid., § 101(a)(1), codified at U.S. Code 8 § 1324a(a)(1).

[10] Ibid., §101(a)(1)(B), 101(b), codified at U.S. Code 8 § 1324a(a)(1)(B), 1324a(b).

[11] Because it is clandestine, illegal immigration is difficult to measure, but the Center for Immigration Studies estimated in 1997 that about 420,000 illegal aliens joined the long-term population each year during the previous 10-year period (offset by deaths,

emigration, and adjustment to legal status that resulted in an increase of 275,000 annually). Steven A. Camarota, "5 Million Illegal Immigrants: An Analysis of New INS Numbers," Center for Immigration Studies, Immigration Review 28 (Spring 1997), http://www.cis.org/articles/1997/IR28/5million.html.

[12] Public Law 104-208, U.S. Statutes at Large 110 (1996): p. 309.

[13] See generally, Richard M. Stana, director, Homeland Security and Justice Issues, U.S. Government Accountability Office, Testimony before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Verification System, GAO-07-924T, 110th Cong., 1st sess., June 7, 2007, http://www.gao.gov/new.items/d07924t.pdf.

[14] Ibid.

[15] U.S. Citizenship and Immigration Services, Department of Homeland Security, "Press Release: EVerify Program Surpasses 52,000 Employers," February 12, 2008, http://www.uscis.gov/files/pressrelease/everify12022008.pdf.

[16] Basic Pilot Extension Act of 2001, Public Law 107-128, U.S. Statutes at Large 115 (2002): p. 2407.

[17] Basic Pilot Program Extension and Expansion Act of 2003, Public Law 108-156, U.S. Statutes at Large 117 (2003): p. 1944.

[18] See White House, "Fact Sheet: Improving Border Security and Immigration within Existing Law," August 10, 2007, http://www.whitehouse.gov/news/releases/2007/08/20070810.html.

[19] See HR 2508, 110th Cong., 1st sess. (requiring all federal contractors to use Basic Pilot); Border Control and Contractor Accountability Act of 2007, HR 3496, 110th Cong., 1st sess. (requiring all DHS contractors to use Basic Pilot); Employment Eligibility Verification and Anti-Identity Theft Act, HR 138, 110th Cong., 1st sess. (requiring employers to join Basic Pilot after receiving SSA "no-match" letter); Airport Security Enhancement Act of 2007, HR 4177, 110th Cong., 1st sess. (requiring Basic Pilot/ EEV for airport employees); Department of Homeland Security Appropriations Act, 2008, HR 2638, 110th Cong., 1st sess. (requiring EEV for DHS and for state programs receiving DHS grants); Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Act, 2008, HR 3161, 110th Cong., 1st sess. (requiring Basic Pilot for recipients of agriculture subsidies); Border Enforcement, Employment Verification, and Illegal Immigration Control Act, HR 4065, 110th Cong., 1st sess. (requiring EEV for government workers and "critical" employers within 2 years); Transportation, Housing and Urban Development, and Related Agencies Appropriations Act, 2008, HR 3074, 110th Cong., 1st sess. (requiring Basic Pilot for Department of Housing and Urban Development contractors); Departments of Labor,

Health and Human Services, and Education, and Related Agencies Appropriations Act, 2008, HR 3043, 110th Cong., 1st sess. (requiring Basic Pilot for Department of Labor, Department of Health and Human Services, and Department of Education contractors); Commerce, Justice, Science, and Related Agencies Appropriations Act, 2008, HR 3093, 110th Cong., 1st sess. (requiring Basic Pilot for Department of Justice, Department of Commerce, and other agency contractors).

[20] A law requiring the use of E-Verify took effect in Arizona January 1, 2008. Fair and Legal Employment Act, HB 2779, 48th Ariz. Legislature, 1st Reg. Session.

[21] Department of Homeland Security, "Safe- Harbor Procedures for Employers Who Receive a No-Match Letter," Federal Register 72 (August 15, 2007): 45,611.

[22] See White House, "Fact Sheet: Improving Border Security and Immigration within Existing Law," August 10, 2007, http://www.whitehouse.gov/news/releases/2007/08/20070810.html.

[23] Secure Borders, Economic Opportunity and Immigration Reform Act of 2007, May 18, 2007, bill draft at Title III, http://kennedy.senate.gov/imo/media/doc/Senator%20Kennedy's%20Immigration%20Bill.pdf.

[24] See Nate Anderson, "Did REAL ID Help Derail the Immigration Bill?" Ars Technica, June 29, 2007, http://arstechnica.com/news.ars/post/20070629-did-real-id-help-derail-immigration-bill.html.

[25] Anne Broache, "Senate Rejects Extra $300 Million for REAL ID," CNetNews.com, July 27, 2007, http://www.news.com/Senate-rejects-extra-300-million-for-Real-ID/2100-7348_3-6199220.html.

[26] See Anne Broache, "Is Real ID Plan on Its Deathbed?" CNet News Blog, November 2, 2007, http://www.news.com/8301-10784_3-9809992-7.html.

[27] Illinois Public Law 095-0138, § 12(a), codified at 820 Illinois Compiled Statutes 55/12.

[28] Michael Chertoff, "A Tool We Need," Leadership Journal blog, September 24, 2007, http://www.dhs.gov/journal/leadership/2007/09/tool-weneed.html.

[29] Westat, "Interim Findings of the Web-Based Basic Pilot Evaluation," Report submitted to U.S. Department of Homeland Security, Washington, DC, December 2006, p. III-15, http://www.uscis.gov/files/nativedocuments/WestatInterimReport.pdf.

[30] Office of the Inspector General, Social Security Administration, "Accuracy of the Social Security Administration's Numident File," Congressional Response Report A-08-06-26100, December 2006, http://www.socialsecurity.gov/oig/ADOBEPDF/audittxt/A-08-06-26100.htm.

[31] See Congressional Budget Office, Cost Estimate: H.R. 4437, Border Protection, Antiterrorism, and Illegal Immigration Control Act of 2005, December 13, 2005, pp. 3–4 (citing Bureau of Labor Statistics figures), http://www.cbo.gov/ftpdocs/69xx/doc6954/hr4437.pdf.

[32] U.S. Citizen and Immigration Services, "I Am an Employer . . . How Do I . . . Use E-Verify?" September 2007, p. 2, http://www.uscis.gov/files/nativedocuments/E4_english.pdf.

[33] See Department of State, Western Hemisphere Travel Initiative Web page, http://travel.state.gov/travel/cbpmc/cbpmc_2223.html.

[34] Matthew Lee, "Passport Requests Flood State Department," Associated Press, March 16, 2007, http://news.yahoo.com/s/ap_travel/20070316/ap_tr_ge/travel_brief_us_passports;_ylt=AuGCNy3Tw0Z6491HO86wucjMWM0F.

[35] "Increased Demand in Passports Predicted," Associated Press, August 17, 2007, http://www.cbsnews.com/stories/2007/08/17/travel/main3179514.shtml.

[36] In mid-2006, former Treasury Department official Bruce Bartlett said that the underground economy is about 10 percent of gross domestic product, or $1.3 trillion. Bruce Bartlett, "The Illegal Immigrant Taxpayer," Wall Street Journal, May 19, 2006, http://online.wsj.com/article/SB114800257492157398.html?mod=todays_us_opinion.

[37] See Privacy Rights Clearinghouse, "A Chronology of Data Breaches," http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[38] U.S. Government Accountability Office, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO 07-737, Washington, DC, June 2007, http://www.gao.gov/new.items/d07737.pdf.

[39] See Center for Democracy and Technology, "Unlicensed Fraud: How Bribery and Lax Security at State Motor Vehicle Offices Nationwide Lead to Identity Theft and Illegal Driver's Licenses," January 2004, http://www.cdt.org/privacy/20040200dmv.pdf.

[40] Department of Homeland Security, U.S. Citizenship and Immigration Services, "For Employees," http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=d6f988e60a405110VgnVCM1000004718190aRCRD&vgnextchannel=d6f988e60a405110VgnVCM1000004718190aRCRD.

[41] Phillip J. Windley, Digital Identity (Sebastopol, CA: O'Reilly, 2005), p. 119.

[42] Jim Harper, Identity Crisis: How Identification Is Overused and Misunderstood (Washington: Cato Institute, 2006), p. 15. ("Your 'identities' . . . are collections of information that other people and institutions have about you, collections that they use to distinguish you from other people in their minds or records.")

[43] Windley, Digital Identity, pp. 12–13.

[44] See, for example, Illegal Immigration Enforcement and Social Security Protection Act of 2007, HR 98, 110th Cong., 1st sess.; Employment Eligibility Verification and Anti-Identity Theft Act, HR 138, 110th Cong., 1st sess.; Border Security and Immigration Reform Act of 2007, HR 2413, 110th Cong., 1st sess.; Secure Borders FIRST (For Integrity, Reform, Safety, and Anti-Terrorism) Act of 2007, HR 2954, 110th Cong., 1st sess.; STRIVE Act of 2007, HR 1645, 110th Cong., 1st sess.; and Comprehensive Immigration Reform Act of 2007, S 1348, 110th Cong., 1st sess.

[45] U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, "News Release: USCIS Launches Photo Screening Tool for E-Verify Program," September 25, 2007, http://www.uscis.gov/files/pressrelease/EVerifyRelease25Sep07.pdf.

[46] See http://www.flyclear.com.

[47] Steven Brill, chairman and chief executive officer, Clear/Verified Identity Pass, Inc., testimony before the House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, Hearing on "Managing Risk and Increasing Efficiency: An Examination of the Implementation of the Registered Traveler Program," July 31, 2007, http://homeland.house.gov/SiteDocuments/20070731145944-83679.pdf.

[48] The city of San Francisco's medical marijuana program is a rare example of a government administrative system that is designed not to be suitable for surveillance. See Harper, Identity Crisis, pp. 225–30.

[49] Congressional Budget Office, "Cost Estimate: HR 4437," http://www.cbo.gov/ftpdocs/69xx/doc6954/hr4437.pdf.

[50] Department of Homeland Security, "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Proposed Rule," Federal Register 72, no. 46 (March 9, 2007): 10,819, http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm.

[51] Department of Homeland Security, "Regulatory Evaluation, Notice of Proposed Rulemaking, REAL ID," Code of Federal Regulations, title 6, part 37, RIN: 1601-AA37, Docket Number DHS-2006-0030 (February 28, 2007), p. 3.

[52] "Alabama Puts Brakes on License Notification," Decatur Daily News, October7, 2005, http://legacy.decaturdaily.com/decaturdaily/news/051007/license.shtml.

[53] Philip Webster, "25 Million Exposed to Risk of ID Fraud," Times (London), November 21, 2007, http://www.timesonline.co.uk/tol/news/uk/article2910705.ece.

[54] Hazelton, Pennsylvania, Ordinance 2006-18: Illegal Immigration Relief Act Ordinance § 5.

[55] S 2393, 110th Cong., 1st sess. (November 16, 2007).

[56] HR 4459, 110th Cong, 1st sess. (December 12, 2007).

[57] Anne Broache, "DHS: Real ID Could Help Shut Down Meth Labs," CNet NewsBlog, January 16, 2008, http://www.news.com/8301-10784_3-9851813-7.html.

[58] Alas, this expansion would not protect the country from terrorism. Assuming terrorists aim to sap the economy and vitality of the United States, they could do very well by serially attacking non-ID-controlled targets, even with backpack bombings. If the United States were induced to further "secure" infrastructure through ID checks, inconveniencing each of the 240 million licensed drivers in the United States to show ID by just one minute per week would cost society over $4 billion per year in lost time alone (assumed value: $20/ hour)—a net present cost of $57 billion (assuming 7 percent interest).

About The Author

Jim Harper is director of information policy studies at the Cato Institute and author of the book *Identity Crisis: How Identification Is Overused and Misunderstood.*