WASHINGTON
LEGISLATIVE OFFICE

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

Testimony of Christopher Calabrese
Counsel, Technology & Liberty Project, Washington Legislative Office

American Civil Liberties Union

Opposing a National ID System and Mandatory Employment Verification as Part of Any Comprehensive Immigration Reform Proposal

U.S. Senate Committee on the Judiciary
Subcommittee on Immigration, Refugees and Border Security

"Ensuring A Legal Workforce: What Changes Should Be Made To Our Current Employment Verification System?"

July 21, 2009
226 Dirksen Senate Office Building

Chairman Schumer, Ranking Member Cornyn and Subcommittee Members, on behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, and its more than half a million members, countless addition supporters and activists, and 53 affiliates across the country, we are pleased to submit this testimony. The ACLU writes to oppose any legislative proposal that would impose a mandatory electronic employment eligibility verification pre-screening system or biometric based national identity system on America's workforce.

Under any name, mandatory imposition of the original Basic Pilot Employment Verification System (also known as E-Verify) or another mandatory employment eligibility prescreening system would impose unacceptable burdens on America's workers, businesses and society at large without resolving America's undocumented immigration dilemma. The costs associated with a mandatory program cannot be denied and cannot be overstated; any benefits are speculative, at best. Additionally in recent weeks, the ACLU has heard described the need for a biometric based identity system. The ACLU would be remiss if it did not make immediately clear our opposition to this idea. As promoted, we believe it would create a national identification system with all the accompanying privacy, civil liberties and cost issues associated with such a system.

This testimony is divided into two parts. The first describes the myriad problems of a biometric national ID system including efficacy, cost, administrative burden and privacy and the second is a description of the well-known existing problems with the voluntary E-Verify program.

Biometric National Identification System

In addition to the problems described below with the Employment Eligibility Verification System (EEVS or, alternatively, E-Verify), any system that uses a biometric model (either as part of an ID card or stored database) for verifying identity is going to run into additional privacy problems as well as a number of other complex practical and security problems. These problems will keep it from acting as an effective verification system.

The ACLU believes that a biometric national identification system should be rejected for the following reasons:

- **i. it runs contrary to American cultural values;**
- **ii. it will be hugely expensive and create a new federal bureaucracy;**
- **iii. it will not prevent unauthorized employment; and**
- **iv. it will trample Americans' privacy and civil liberties.**

i. A Biometric National ID System Runs Contrary to Americans' Cultural Values

As an initial matter it is critical to understand the vast scope of a biometric system. **Any biometric system would require the fingerprinting (or collection of some other biometric) of the entire working population of the US.** Americans will have to be treated like criminals

and suspects in order to work. This process will be far from painless. It will involve long lines, gathering identity documents, and considerable confusion and mistake. Any biometric system that goes beyond photographing individuals will face enormous cultural stigma. Not only will this create substantial backlash against the government but also against immigrants (and those who appear to be foreign) who many will perceive as having created this problem.

This proposal is certain to be controversial and poses a significant threat to the passage of any legislation to which it is attached, including Comprehensive Immigration Reform.

ii. A Biometric National ID System Will be Hugely Expensive and Create a New Federal Bureaucracy

The key to a biometric system is the verification of the individual. In other words, an individual must visit a government agency and must present documents such as a birth certificate or other photo ID that prove his or her identity. The agency must then fingerprint the person (or link to some other biometric) and place the print in a database. The agency might also place the biometric on an identification card. Such a process would create a quintessential national ID system because it would be nationwide, would identify everyone in the country, and would be necessary to obtain a benefit (in this case the right to work).

The closest current analogy to this system is a trip to the Department of Motor Vehicles to obtain a drivers' license. The federalizing of that system (without the addition of a new biometric) via the Real ID Act will cost more than $23 billion if carried out to completion, though 24 states have rejected the plan, putting its completion in grave doubt. The cost to build such a system from scratch would be even more staggering. It would involve new government offices across the country, tens of thousands of new federal employees and the construction of huge new information technology systems. It is far beyond the capacity of any existing federal agency.

Such a system would spawn a huge new government bureaucracy. Every worker would have to wait in long lines, secure the documents necessary to prove identity, and deal with the inevitable government mistakes. Imagine the red tape necessary to provide documentation for 150 million US workers. All of the problems of the existing E-Verify system would be magnified as workers faced another bureaucratic hurdle before they could begin their jobs.

Employers would not escape from problems with the system, either. They would have to purchase expensive biometric readers, provide Internet connections, train HR workers, and endure delays in their workforce. Especially in these times of severe economic pressure, such expenses will threaten many businesses operating on the edge of profitability, both large and small.

These problems are not hypothetical. After spending billions the United Kingdom effectively abandoned its efforts to create a biometric national ID card, making it voluntary. Dogged by public opposition, concerns about data privacy, and extensive technical problems, the

program has been an embarrassment for the British government. Conservative Party politicians (currently ahead in the polls) plan to scrap the program altogether if they assume power.[1]

iii. A Biometric National ID System Will Not Prevent Unauthorized Employment

Despite a popular assumption to the contrary, a biometric national ID system would largely fail to solve the problem of undocumented immigration. Security systems must be judged not by their successes, but rather by their failures. After enduring a host of bureaucratic hassles and costs most Americans would likely be able to enroll in the biometric system. But that does not make the system a success – those workers were already working lawfully. The system only succeeds if it keeps the undocumented workers in this country from securing employment and a biometric national ID system is unlikely to do that.

The first and most obvious failure is that this system does nothing about employers who opt out of the system altogether (work "off the books"). Already, by some reports, more than 12 million undocumented immigrants are working in the United States. Many of these workers are part of the black market, cash wage economy. Unscrupulous employers who rely on below-market labor costs will continue to flout the imposition of a mandatory employment eligibility pre-screening system and biometric national ID. These unscrupulous employers will game the system by running only a small percentage of employees through the system or by ignoring the system altogether. In the absence of enforcement by agencies that lack resources to do so, employers will learn there is little risk to gaming the system and breaking the law.

Law abiding employers, however, will be forced to deal with the hassle and inconvenience of signing up for E-Verify and a biometric system. Then they'll be forced to watch and wait when they are blocked from putting lawful employees to work on the planned date due to system inaccuracies or other malfunctions. The inevitable result will be more, not fewer, employers deciding to pay cash wages to undocumented workers. Similarly, cash wage jobs will become attractive to workers who have seemingly intractable data errors. Instead of reducing the number of employed undocumented workers, this system will create a new subclass of employee – the lawful yet undocumented worker.

Additional failures will come when the worker is initially processed through the system. Crooked insiders will always exist and be willing to sell authentic documents with fraudulent information.[2] Undocumented immigrants will be able to contact these crooked insiders though the same criminals whom they hired to sneak them into the United States. Securing identification will simply be added to the cost of the border crossing.

Worse, since 2004, more than 260 million records containing the personal information of Americans have been wrongly disclosed.[3] Many individuals' personal information, including social security numbers, are already in the hands of thieves. There is nothing to prevent a

---

[1] Michael Holden, *Plans dropped for compulsory ID cards*, REUTERS, June 30, 2009

[2] Center for Democracy and Technology, "Unlicensed Fraud." January 2004 (www.cdt.org/privacy/**2004**0200dmv.pdf).

[3] [3] Privacy Rights Clearinghouse Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm

criminal from obtaining fraudulent access to E-Verify (pretending to be a legitimate employer), verifying that a worker is not already registered in the system and sending an undocumented worker to get a valid biometric using someone else's information.

Additional problems inherent in any biometric will materialize both when an individual is enrolled, and at the worksite. For example, according to independent experts there are a number of problems that prevent proper collection and reading of fingerprints, including:

- Cold finger
- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Location of finger on platen (poorly placed core)
- Cuts to fingerprint; and
- Manual activity that would mar or affect fingerprints (construction, gardening).[4]

When these failures occur it will be difficult and time consuming to re-verify the employee. Running the print through the system again may not be effective, especially if the print has been worn or marred. Returning to the biometric office for confirmation of the print is not likely to be a viable solution because it creates another potential for fraud; the person who goes to the biometric office may not be the person who is actually applying for the job. These are complex security problems without easy solutions.

Perhaps worst of all, there would be mounting pressure to "fix" many of these problems with more databases filled with identifying information such as birth certificates or DNA in an attempt to identify individuals earlier and more completely. This would mean more cost, more bureaucracy and less privacy.

From a practical point of view a biometric system is the worst of both worlds. It puts enormous burdens on those already obeying the law while leaving enough loopholes so that lawbreakers will slip through.

iv. **A Biometric National ID System Will Trammel Privacy and Civil Liberties**

The creation of a biometric national ID would irreparably damage the fabric of American life. Our society is built on privacy, the assumption that as long as we obey the law, everyone is free to go where we want and do what we want – embrace any type of political, social or economic behavior we choose. We can pursue our personal choices all without the government (or the private sector) looking over our shoulders monitoring our behavior. This degree of personal freedom is one of the keys to America's success as a nation. It allows us to be creative, enables us to pursue our entrepreneurial interests, and validates our democratic instincts to challenge any authority that may be unjust.

[4] International Biometrics Group, http://www.biometricgroup.com/reports/public/reports/biometric_failure.html

A biometric national ID system would turn those assumptions upside down. A person's ability to participate in a fundamental aspect of American life – the right to work – would become contingent upon government approval. Moreover, such a system will almost certainly be expanded. In the most recent attempt to create a national ID though a state driver's license system called Real ID, at the outset the law only controlled access to federal facilities and air travel. Congressional proposals quickly circulated to expand its use to such sweeping purposes as voting, obtaining Medicaid and other benefits, and traveling on interstate buses and trains.[5] Under a national ID system, every American needs a permission slip simply to take part in the civic and economic life of the country.

Historically, national ID systems have been a primary tool of social control. It is with good reason that the catchphrase "your papers please" is strongly associated with dictatorships and other repressive regimes. Registration regimes were an integral part of controlling unauthorized movement in the former Soviet Union and enforcing South Africa's old apartheid system. They also helped both Nazi Germany and groups in Rwanda commit genocide by identifying and locating particular ethnic groups.[6] There were certainly factors that contributed to making these governments so abhorrent, but they all shared a system of national identification. Why would we willingly create such a system that could so easily become a tool for abuse in the hands of the wrong governmental leadership?

The danger of a national ID system is greatly exacerbated by the huge strides that information technology ("IT") has made in recent decades. A biometric national ID system would violate privacy by helping to consolidate data. There is an enormous and ever-increasing amount of data being collected about Americans today. Grocery stores, for example, use "loyalty cards" to keep detailed records of purchases, while Amazon keeps records of the books Americans read, airlines keep track of where they fly, and so on. This can be an invasion of privacy, but Americans' privacy has actually been protected because all this information remains scattered across many different databases. Once the government, landlords, employers, or other powerful forces gain the ability to draw together all this information, privacy will really be destroyed. And that is exactly what a biometric national ID system would facilitate.

If a biometric national ID system is linked with an identity card the problems will grow even greater. A card would facilitate tracking. When a police officer or security guard scans an ID card with his or her pocket bar-code reader, for example, it will likely create a permanent record of that check, including the time and location. How long before office buildings, doctors' offices, gas stations, highway tolls, subways and buses incorporate the ID card into their security or payment systems for greater efficiency? The end result would be one where the government monitors citizens' movements inside their own country and records those movements through these "internal passports."

The sordid history of national ID systems combined with the possibilities of modern IT paint a chilling picture. These problems cannot be solved by regulation or by tinkering around

[5] See, e.g. H.R. 1645, the Security Through Regularized Immigration and a Vibrant Economy Act of 2007 (110th Congress).
[6] Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 Fla. L. Rev. 697, 709.

with different types of biometrics. Instead, the entire unworkable system must be rejected so that it does not intolerably impinge on American's rights and freedoms.

Electronic Employment Verification

The ACLU opposes a mandatory Electronic Employment Verification System for five reasons:

(i) it poses unacceptable threats to American workers' privacy rights by increasing the risk of data surveillance and identity theft;

(ii) data errors in Social Security Administration ("SSA") and Department of Homeland Security ("DHS") files will wrongly delay or block the start of employment for lawful American workers;

(iii) it lacks sufficient due process procedures to protect workers injured by such data errors;

(iv) both SSA and DHS are unable to implement such a system and SSA's ability to continue to fulfill its primary obligations to the nation's retirees and disabled individuals would deteriorate; and

(v) it will lead to rampant employer misuse in both accidental and calculated ways.

I. Mandating Electronic Employment Eligibility Verification Poses Unacceptable Threats to American Workers' Privacy Rights

A nationwide mandatory EEVS would be one of the largest and most widely accessible databases ever created in the U.S. Its size and openness would be an irresistible target for identity theft and almost inevitably lead to major data breaches. Additionally, because the system would cover everyone (and be stored in a searchable format), it could lead to even greater surveillance of Americans by the intelligence community, law enforcement and private parties.

The E-Verify system currently contains an enormous amount of personal information including names, photos (in some cases), social security numbers, phone numbers, email addresses, workers' employer and industry, and immigration information like country of birth. It contains links to other databases such as the Customs and Border Patrol TECS database (a vast repository of Americans' travel history) and the Citizen and Immigration Service BSS database (all immigration fingerprint information from US VISIT and other sources).[7]

The data in E-Verify, especially if combined with other databases, would be a gold mine for intelligence agencies, law enforcement, licensing boards, and anyone who wanted to spy on

[7] 73 Fed. Reg. 75449.

American workers. Because of its scope, it would likely form the backbone for surveillance profiles of every American. It could be easily combined with other data such as travel, financial, or communication information. 'Undesirable' behaviors – from unpopular speech to gun ownership to paying for items with cash – could be tracked and investigated by the government. Some of these databases linked to E-Verify are already mined for data. For example, the TECS database uses the Automated Targeting System (ATS) to search for suspicious travel patterns. Such data mining would be even further enhanced by the inclusion of E-Verify information.

Without proper restrictions, American workers would be involuntarily signing up for never ending digital surveillance every time they apply for a job. In order to protect Americans' privacy, we recommend that Congress must limit the retention period for queries to the E-Verify system to three to six months, unless it is retained as part of an ongoing compliance investigation or as part of an effort to cure a non-confirmation. This is a reasonable retention limitation for information necessary to verify employment. By comparison, information in the National Directory of New Hires, which is used on an ongoing basis to allow states to enforce child support obligations, is deleted after either 12 or 24 months.[8] The current retention period for E-Verify (set by regulation) is an astonishing 10 years; in other words, deadbeat dads have better privacy than American workers.

We also recommend that the use of information in any employment verification system be strictly curtailed. It should only be used to verify employment or to monitor for employment-related fraud. There should be no other federal, state, or private purpose. Data should also be bound by strict privacy rules, such as those that protect census data which sharply limit both the disclosure and use of that information.[9]

Additionally, the system must guard against data breaches and attacks by identity thieves. Since the first data breach notification law went into effect in California at the beginning of 2004, more than 260 million records have been hacked, lost or disclosed improperly.[10] In 2007, it was reported that the FBI investigated a technology firm with a $1.7 billion DHS contact after it failed to detect "cyber break-ins".[11] The loss of this information contributes to identity theft and a constant erosion of Americans' privacy and sense of security. A compulsory employment verification system will contain the records of more than 150 million American workers – a vast expansion on the existing system. It will be accessible by millions of employers, federal employees, and others. There is absolutely no question that an employment verification system will be breached. The question is simply how bad the breach will be and how much harm it will cause.

II. Data Errors Will Injure Lawful Workers by Delaying Start Dates or Denying Employment Altogether

[8] The data retention limitation for the National Directory of New Hires is governed by 42 U.S.C. §653 (i).
[9] Protections for census data can be found at 13 U.S.C. §9.
[10] Privacy Rights Clearinghouse Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[11] Ellen Nakashima and Brian Krebs, *Contractor Blamed in DHS Data Breaches*, WASHINGTON POST, Sept. 24, 2007.

Recent government reports acknowledge that huge numbers of SSA and DHS files contain erroneous data that would cause "tentative non-confirmation" of otherwise work-eligible employees and, in some cases, denial of their right to work altogether. The United States Customs and Immigration Service (USCIS) states that 3.1% of workers receive a tentative non-confirmation from the E-Verify system and only .3% are able to resolve the issue.[12] In many of these cases workers are eligible to work lawfully but simply don't have the time or don't know they have the right to contest their determinations and seek different employment. Finding another job is not an option for many unemployed Americans in this economy, and under a mandatory E-Verify system finding another job will be impossible.

SSA also reports that approximately 17.8 million of its files contain erroneous data, 12.7 million of which concern U.S. citizens. The SSA's Office of Inspector General reports that the Social Security database has a 4.1 percent error rate. Even cutting this data error rate by 90% would leave approximately 1.78 million workers – more than 1.2 million of whom will be U.S. citizens – at the mercy of a system that provides no adequate due process for challenging and correcting erroneous data.

The causes of these data errors are well-known. First, legacy files produced on paper before the onset of the information age contained numerous inconsistencies or may have been lost or never updated. Second, women or men who changed their names at marriage, divorce or re-marriage may have inconsistent files or may never have informed either SSA or DHS of name changes. Third, simple key stroke errors contribute to the volume of erroneous data. Fourth, individuals with naming conventions that differ from those in the Western world may have had their names anglicized, transcribed improperly or inverted. Fifth, individuals with common names may have had their files wrongly conflated or merged with others sharing the same or similar name.

All of these problems make implementation of such a mandatory pre-screening system difficult, if not impossible. Congress should not mandate such a system unless and until these databases and the files they contain are substantially improved. A first step, however, to aid both SSA and DHS in carrying out their distinct but primary missions -- other than employment eligibility prescreening -- would be for Congress to mandate that both agencies systematically audit and review their files' data quality to eliminate errors. Only after such a systematic effort to improve data is completed should Congress even consider mandating use of these files to pre-screen worker eligibility.

III. Pending Legislative Proposals Lack Meaningful Due Process Protections for Lawful Workers Injured by Data Errors

Workers injured by data errors will need a means of quickly and permanently resolving data errors so they do not become presumptively unemployable. Congress must prevent the

[12] USCIS website (checked July 16, 2009)
http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=f82d8557a487a110VgnVCM1000004718190aRCRD&vgnextchannel=a16988e60a405110VgnVCM1000004718190aRCRD

creation of a new employment blacklist –a "No-Work List" that will consist of would-be employees who are blocked from working because of data errors and government red tape.

To resolve data errors, Congress must prevent the enactment of a mandatory pre-screening system unless it has meaningful due process provisions. Such procedures should mirror the fair information practices that undergird the Privacy Act of 1974 and control how the government should handle data it collects about the public.[13] Therefore, Congress should not pass any legislation unless it mandates that:

(i) the systems and databases used to collect and disseminate information about those attempting to work be publicly disclosed so that workers and employers are aware of them;

(ii) information collected by either government agencies or employers shall be gathered for one purpose only and shall not be used for other purposes without individuals' voluntary and fully informed consent;

(iii) workers can access information held about them in a timely fashion without having to petition the government;

(iv) workers can correct, amend, improve or clarify information held about them by either the government or employers;

(v) information about employees be accurate, up to date and kept only as long as relevant; and

(vi) retained information is protected against unauthorized losses such as data breaches or identity theft.

Given the inordinately high database error rates, it is incumbent upon Congress to prevent the imposition of a mandatory system that fails to provide workers with a fair and just set of administrative and judicial procedures to resolve data errors promptly and efficiently. True due process would require the creation of a system to expedite workers' inquiries at both SSA and DHS, in addition to the existing opportunity – too often not communicated to employees wrongly non-confirmed – to submit additional information to the agencies.[14] In demanding due process for workers in such a system, any worker who challenges erroneous government data deserves a presumption of work eligibility.

True due process requires congressional establishment of open, accessible, efficient, and quick administrative procedures so as to enable any aggrieved worker to get back to work and so as not to deprive an employer of its chosen employee. First, Congress must enable and require that SSA and DHS hire and train sufficient staff to handle the millions of additional inquiries they will receive as workers try to resolve data errors. These new government employees will be needed for the substantial increase in the manual verification workload, each verification often

[13] 5 U.S.C. §§ 552, et seq.
[14] Id.

taking more than two weeks to complete. Thus, the ACLU urges the creation and full-staffing of 24-hour help lines at SSA and DHS. Second, when data provided by a worker conflicts with government files, the aggrieved worker must be provided a right to a quick, efficient, and fair administrative review. Third, costs should be borne by the government for each such administrative appeal so as to minimize injury to the worker. Fourth, the administrative law judge, or other arbiter, should be able to order the government to correct and supplement the government records at issue. Fifth, government employees should be empowered and compelled to correct data errors expeditiously. Sixth, the administrative law judge must be empowered to order the government to reimburse the worker's costs and to reimburse for lost wages plus interest. We would urge a strict liability standard so as to encourage the government to improve its data quality.

If the administrative process fails to resolve data discrepancies, then due process requires the right to a judicial process. Because of the costs of bringing suit, including filing fees, retaining counsel, obtaining documents, finding and presenting witnesses, and hiring experts, the government must bear the burden of any judicial process. What undocumented worker would contest a tentative non-confirmation before a federal judge – toward what end? Congress should place the legal burden on the government's shoulders to demonstrate a worker's ineligibility rather than forcing the worker to prove his or her eligibility.

Some have suggested, without foundation, that the Federal Tort Claims Act (FTCA) would offer an appropriate remedy for aggrieved workers. The FTCA falls short and does not provide an adequate procedure for the hundreds of thousands who would be impacted unfairly by the imposition of a mandatory procedure. The U.S. Court of Claims reported an extensive backlog of cases and requires a worker to exhaust a six-month long waiting period before filing suit. **During the pendency of the FTCA administrative procedure and lawsuit, the worker would be barred from working.**

Because the FTCA is inadequate, Congress must mandate an alternative expedited federal administrative and court procedure, and judges should be empowered to order the government to correct any erroneous files and to reimburse a worker for costs and fees for bringing suit, including attorney's fees. Furthermore, federal judges should be required to order agencies to reimburse a worker for any lost wages and lost opportunity costs, plus interest. The legal standard should be one of strict liability, so that any government error leads to redress that makes the injured worker whole. Any lesser legal standard, such as negligence or recklessness, will fail to (i) assist the aggrieved worker and his or her family; and (ii) encourage the agencies to improve data quality so as to reduce the harm from such a system going forward.

IV. Government Agencies are Unprepared to Implement a Mandatory Employment Eligibility Prescreening System

As recent government reports evaluating E-Verify have made clear, both SSA and DHS are woefully unprepared to implement a mandatory employment eligibility pre-screening system. In order to implement such a system, both agencies would need to hire hundreds of new, full-time employees and train staff at every SSA field office. DHS has an enormous backlog of unanswered Freedom of Information Act (FOIA) requests from lawful immigrants seeking their

immigration files. Those files, many of which are decades old, are the original source of numerous data errors. If DHS cannot respond to pending information requests in a timely fashion now, how much worse will the problem be when lawful immigrants, including naturalized citizens, lawful permanent residents, and visa holders need the documents immediately to start their next jobs? Consequently, DHS must hire hundreds more employees to respond to these FOIAs.

Businesses seeking to comply with any newly imposed system will also put additional strain on these government agencies. Problems can be anticipated in attempting to respond to employers' requests and in establishing connectivity for businesses located in remote regions or that do not have ready access to phones or the internet. These agency deficiencies will surely wreak havoc on independent contractors and the spot labor market for short-term employment.

If history is our guide, agency officials will be unable to scale up the existing software platform for E-Verify to respond to the enormous task of verifying the entire national workforce and all the nation's employers. It makes little sense to adopt a system that is pre-destined to cause chaos within these agencies, not to mention the lives of the thousands of Americans wrongfully impacted.

V. Employers Will Misuse a Mandatory Employment Eligibility Prescreening System

Employers have misused and will continue to misuse any mandatory employment eligibility verification system. Such misuse has resulted in discrimination and anti-worker behavior in the past and there is no reason to suggest that pattern will change with a new verification system in place. From the inception of E-Verify, the U.S. Government Accountability Office and DHS studies have documented various types of misuse. Some employers have even self-reported that they screen out workers with "foreign" surnames or fail to explain tentative non-confirmations to employees. Other employers have self-reported that they have punished employees with tentative non-confirmations by withholding wages and assignments during the period until any discrepancy is resolved.

If Congress imposes a mandatory system, it will need to create effective enforcement mechanisms that prevent the system from being a tool for discrimination in hiring. Such discriminatory actions will be difficult to prevent and even more difficult to correct. Congress should ask: how will the government educate employers and prevent misuse of E-Verify or any similar system?

VI. Conclusion: Congress Must Not Enact a Mandatory Employment Eligibility Pre-Screening System or Biometric National ID System

The ACLU urges the Subcommittee on Immigration, Refugees, and Border Security to reject imposition of a mandatory electronic employment eligibility pre-screening system and biometric national ID system. Such systems would cause great harm to employers across the country and to lawful workers and their families while doing little to dissuade undocumented workers. The likelihood for harm is great and the prospect for gain is purely illusory.