WRITTEN STATEMENT OF
THE AMERICAN CIVIL LIBERTIES UNION

For a Hearing on

"How E-Verify Works and How It Benefits American Employers and Workers"

Submitted to the House Judiciary Committee

February 27, 2013

ACLU Washington Legislative Office
Laura W. Murphy, Director
Christopher Calabrese, Legislative Counsel

The American Civil Liberties Union (ACLU) submits this statement to the House Judiciary Committee on the occasion of its hearing addressing "How E-Verify Works and How it Benefits American Employers and Workers."[1] This statement aims to provide the Committee with an appraisal of the privacy and civil liberties implications of a mandatory employment verification system ("mandatory E-Verify").[2]

Several immigration reform proposals have called for mandatory E-Verify in some form.[3] For example, the Senate Gang of Eight proposal describes a "tough, fair, effective and mandatory employment verification system."[4] Unfortunately, E-Verify is a flawed electronic employment-eligibility screening system that imposes unacceptable burdens on America's workers, businesses and society at large. **For example a mandatory E-Verify system with a mere 1% error rate would affect approximately 1.5 million American workers.** Nationwide, E-Verify would create a virtual national ID and would lay the groundwork for a possible biometric national ID system, thereby imposing significant privacy and civil liberties costs on all Americans, including lawful workers, businesses, and taxpayers.

I. Privacy Concerns

A. National ID

E-Verify is an internet-based system that contains identifying information on almost every American. It includes names, photos from passports and DHS documents, some drivers' license information, social security numbers, phone numbers, email addresses, workers' employer, industry, and immigration information like country of birth.[5] The internet-enabled process operates by allowing employers to check the system to see if a newly hired employee is work authorized. Right now, it is largely voluntary except where it is required for federal contractors and by some states.

This vast collection of personal information is already well on its way to becoming a national identity system. When E-Verify began, it was used essentially for document

---

[1] The ACLU is a nationwide, non-partisan organization of more than a half-million members, countless additional activists and supporters, and 53 affiliates nationwide dedicated to enforcing the fundamental rights of the Constitution and laws of the United States. The ACLU's Washington Legislative Office (WLO) conducts legislative and administrative advocacy to advance the organization's goal of protecting the privacy rights of every American and protecting the rights of immigrants', including supporting a roadmap to citizenship for aspiring Americans.

[2] For a statement regarding the ACLU's broader position on immigration reform, please see: http://www.aclu.org/immigrants-rights/aclu-statement-senate-judiciary-committee-hearing-comprehensive-immigration-reform

[3] *See* "FACT SHEET: Fixing our Broken Immigration System so Everyone Plays by the Rules," The White House, January 29, 2013, available at http://www.whitehouse.gov/the-press-office/2013/01/29/fact-sheet-fixing-our-broken-immigration-system-so-everyone-plays-rules. The document notes the mandatory electronic employment verification program will ensure "the privacy and confidentiality of all workers' personal information" and will "include(s) important procedural protections."

[4] Brad Plumer, READ: Senators release bipartisan plan for immigration reform, Washington Post, January 28, 2013. Available at: http://www.washingtonpost.com/blogs/wonkblog/wp/2013/01/28/read-senators-release-their-plan-for-immigration-reform/.

[5] *Privacy Impact Assessment for the E-Verify Program*, USCIS Verification Division, May 4, 2010.

verification. Workers would present Social Security cards and other information and the system would assure that number or other record was legitimate and belonged to an individual who was work authorized. With the addition of more information to the system, especially photographs, the nature of E-Verify has changed. It is rapidly becoming a system for identifying workers – by entering identifying information and receiving a photograph. Recently some lawmakers have called for this system to be further supplemented by a physical card which would contain identifiers such as fingerprints or other biometrics which could be used to verify identity as part of the E-Verify process.[6]

These two proposals – biometric national ID and mandatory E-Verify – could easily become a wide-ranging government permission slip necessary to access basic rights and services. Social Security numbers, originally intended to be used for distribution of benefits, were never meant to be used for identification. Now it is almost impossible to function in America without one. If it becomes mandatory, E-Verify could expand in much the same way. An internet connection and access to the system could lead to unwarranted harassment and denial of access to TSA checkpoints, voting booths, and gun permits, or other harmful uses not yet envisioned. Further, as described below, E-Verify is plagued by errors and bureaucratic hurdles to work. If Congress expands the system to become a national ID system, these problems would quickly become not only employment issues, but also problems with travel and other fundamental freedoms.

Such a national identity system could also enable other types of data surveillance. If combined with other databases, including data on travel, financial information or communications, E-Verify would be a gold mine for intelligence agencies, law enforcement, licensing boards, and anyone who wanted to spy on American workers. Because of its scope, it could form the basis for surveillance profiles of every American.

While the bipartisan Senate plan calls for "procedural safeguards to protect American workers, prevent identity theft, and provide due process protections," no safeguards can change the fact that creating a biometric national ID would irreparably damage the fabric of American life.[7] Our society is built on the presumption of privacy: as long as we obey the law, we are all free to go where we want and do what we want – embrace any type of political, social or economic behavior we choose—without the government (or the private sector) looking over our shoulders or monitoring our behavior. This presumption of personal freedom is one of the keys to America's success as a nation. It encourages us to be creative, motivates us to pursue our entrepreneurial interests, and validates our democratic instincts to challenge any authority that may be unjust. A national ID system would turn those assumptions upside down by making every person's ability to participate in a fundamental aspect of American life – the right to work – contingent upon government approval.

B. Identity Theft

[6] Danny Yadron, *Senators in Immigration Talks Mull Federal IDs for All Workers*, Wall Street Journal, Feb. 21, 2013.
[7] Plumer at 1.

The system is vulnerable to another privacy harm: 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 607 million records have been hacked, lost or disclosed improperly including those related to E-Verify.[8] As just one example, in October and December 2009, Minnesota officials learned that the company hired to process the state's E-Verify forms had accidentally allowed unauthorized individuals to gain access to the personal information of over 37,000 individuals due to authentication practices and web application vulnerabilities in their system.[9]

Currently, the Department of Homeland Security (DHS) is not doing all that it can to protect the E-Verify system. A software industry best practice is to have a third party security professional audit systems in order to look for information security flaws in the software code or the configuration of servers. These so-called "red teams" are used by the military, the National Security Agency, the Department of Energy, as well as by private industry.[10] However currently it appears that DHS has only taken piecemeal steps taken to improve the security of the E-Verify system, none of which suggest the presence of a comprehensive information security program.[11]

Regardless of whether or not Congress makes the use of E-Verify by employers mandatory, it is absolutely vital that E-Verify receive a thorough audit by independent security experts, that all flaws are fixed, and that DHS commit to re-auditing the system each year. The E-Verify system contains sensitive personally identifying information on millions of Americans, is connected to the internet, and it should be assumed that it will be a target for hackers.

II. Existing Problems with the System

A. Error Prone Databases

Implementing E-Verify nationwide would require reliance on massive and inaccurate databases, and the room for error is enormous. Currently, E-Verify has been implemented in only a fraction of the country's workplaces. **If applied to the entire workforce and with a**

---

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

[9] John Fay, *FTC Settlement Highlights the Importance of Protecting Sensitive I-9 Data in an Electronic World*, Guardian I-9 And E-Verify Blog, May 4, 2011.

[10] *See* Robin Mejia, Red Team Versus Blue Team: How to Run an Effective Simulation, CSO Online, March 28, 2008, available at http://www.csoonline.com/article/221695/red-team-versus-blue-team-how-to-run-an-effective-simulation. See also Google, Google's Approach to IT Security, 2012, available at https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf (Google "Engages outside security experts to conduct periodic security assessments of Google's infrastructure and applications").

[11] Westat Corporation, Findings of The E-Verify Program Evaluation, 2009, at page 36 ("USCIS staff report that they have undertaken a number of efforts to improve E-Verify … including exploring ways to make E-Verify more secure.") and page 108 ("Other future changes expected are … Improvements in the registration process to make it more secure"). See also Claire Stapleton, Privacy Branch Chief, USCIS, Privacy Impact Assessment for the E-Verify Program, May 4, 2010 ("E-Verify has implemented a broad range of technical, operational, and physical security measures to protect the system and its information. These security measures include access controls for both internal and external users…E-Verify has an automated mechanism to ensure that users change their passwords at a specified interval. User accounts are locked after several failed attempts to log on... Password data is encrypted within the system. E-Verify is located within a multi-layered firewall architecture…").

conservative 1 percent error rate (as a recent Migration Policy Institute paper estimates[12]), 1.5 million work-authorized employees could be terminated if they are unable to fix their records. If applied only to new hires, 517,000 workers could lose their jobs.[13]

Correcting a record or contesting a determination is a difficult and in some cases impossible task. Sometimes workers don't have the time or never learn they have the right to contest their determinations. Studies from cities and states where E-Verify is in place have shown this, with disastrous consequences. A survey of 376 immigrant workers in Arizona (where use of E-Verify is required) found that 33.5% were fired immediately after receiving a tentative denial in the system and were never given a chance to correct potential errors. Furthermore, not one of those workers was notified by the employer that he or she had the right to appeal the E-Verify finding, despite such a requirement in the memorandum of understanding (MOU) that all employers sign with DHS before using the program.[14]

Some workers are never able to resolve an error. For example, Jessica St. Pierre, a U.S. citizen telecommunications worker in Florida, was initially hired for a position. However she was unable to start work due to an E-Verify error. Despite her pleas to government officials, she was unemployed for several months and eventually had to take a lower paying job.[15] The error was eventually traced to the employer incorrectly entering her name.

These error rates are caused by a variety of factors. Women or men who changed their names at marriage, divorce, or re-marriage may have inconsistent files or may have never informed either the Social Security Administration or DHS of name changes. Simple key stroke or misspelling errors also contribute to the volume of erroneous data. Individuals with naming conventions that differ from those in the Western world may have had their names anglicized, transcribed improperly, or inverted. The GAO predicted that if E-Verify were made mandatory for new hires nationwide, approximately 164,000 citizens per year would receive a tentative non-confirmation (TNC – a system output saying the individual does not have a match in the system) just for name-change related issues.[16] It would be even more damaging if applied not just to new hires, but to existing workers as well.

The high number of error rates occurring among certain cultural groups can lead to an appearance of discrimination in the employment process. Five out of 25 employers acknowledged to GAO that TNCs were more likely to occur with Hispanic employees having hyphenated or multiple surnames.[17] Additionally the TNC rate for employees who were eventually authorized to work was approximately 20 times higher for foreign-born employees than for U.S.-born employees from April through June of 2008.[18] These striking disparities

---

[12] Doris Meissner and Marc Rosenblum, *The Next Generation of E-Verify: Getting Employment Verification Right* (Migration Policy Institute, July 2009), http://www.migrationpolicy.org/pubs/Verification_paper-071709.pdf.
[13] *Id.*
[14] Caroline Isaacs, Sanctioning Arizona: The Hidden Impacts of Arizona's Employer Sanctions Law (American Friends Service Committee, 2009), www.afsc.org/tucson/ht/a/GetDocumentAction/i/74700.
[15] Written Statement of Jessica St. Pierre, *"E-Verify Preserving Jobs for American Workers" House Committee on the Judiciary Subcommittee on Immigration Policy and Enforcement Hearing*, February 10, 2011.
[16] GAO, *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, p.19.
[17] *Id*. p. 20.
[18] *Id*. p. 40

could easily lead employees to believe they were being judged on more than just their credentials. Moreover, employers may shy away from hiring non-native-born individuals or those with foreign names because of a fear they would be harder to clear through the system.

B. Process for Discovering Errors in the System

Workers injured by data errors need a way to resolve those errors quickly and permanently so they do not become presumptively unemployable. Workers face two distinct challenges. The first is to learn that errors in their records exist and the second is the lack of fundamental due process protections for resolving those errors.

In order to alert workers to errors in their record we recommend two approaches. The first is to allow workers to check their own records and the second is to provide direct notice to workers whenever they are the subject of an E-Verify search.

Self-Check

We commend U.S. Citizenship and Immigration Service for beginning this process by creating a self-check system that allows workers to check on their E-Verify data. It is a fundamental privacy principle that individuals should have access to their own information in order to assure its completeness and correctness.

We have some specific concerns about how the self-check program will be implemented. First of all, self-check is a tool for allowing workers to correct their records. It must not be used as a pre-screening tool. If employers imposed a self-check requirement – effectively serving as an E-Verify pre-screening tool – they would shift the cost from the employer to the employee. In keeping with the statistics cited above, such costs would fall disproportionately on immigrants, minorities, and women. This would undermine the anti-discrimination provisions built into the system to ensure that authorized workers are able to contest TNCs and document their eligibility to work.

Second, the system must protect the privacy of both employers and employees. Considering high rates of identity fraud associated with the E-Verify system, it is no surprise that individuals are very concerned about the retention of their personal information in a database to which more and more people are gaining access. There must be clearly defined limits in regard to potential sharing of personal information.

Third, there must be an option for self-check access to people without credit histories. If self-check relies on background check information, then it will be unavailable to populations of foreign nationals who have only recently arrived in the U.S. and have not yet developed a credit history. This would include some of those with the most complicated immigration situations such as refugees, asylum seekers, and people with temporary protected status.[19]

Worker Notice

[19] The American Immigration Lawyers Association, *E-Verify Self Check Program*, November 29, 2010

Currently the only mechanism allowing individuals to learn when their records have been checked in the E-Verify system is through notification by an employer. The practical result of this policy is that the person best positioned to identify and report misuse of E-Verify checks – the worker – never learns about them. The problem is particularly acute in cases of identity theft. In many cases, workers could provide a wealth of valuable information about misuse of the system if they were notified when verification checks occurred, given a place to report misuse of their information, and provided with a minimum amount of education. On the last point, it would be helpful to provide as part of this notice information such as, "Have you started a new job in the last few days? If not, your personal information may have been improperly accessed in a government database."

For example, if a worker learns of multiple improper checks, it may indicate his or her personal information has been sold for use by undocumented workers seeking employment. Alternately, a single improper check may be evidence that a worker's personal information has been stolen from another source (such through a data breach) and thieves are using a hacked E-Verify account to validate the accuracy of the information before using it for purposes such as credit card fraud. Finally, a notification that comes when a worker has only applied for a job may be evidence of improper prescreening.

System notification and reporting could be implemented easily. The Social Security Administration already has address information for beneficiaries (it performs an annual mailing of benefit information) and notice could include a link that allows individuals to directly report back on problems. The conditions when verification typically occurs are fairly straightforward (the beginning of employment), so an individual could reasonably understand when a verification is improper and report it. Such a notice would also provide a timely reminder to a worker's right to appeal and educate the worker about the E-Verify system.

C. Due Process Protections

Once workers learn of errors in E-Verify, they need a robust system for contesting those mistakes. Absent such a system, mandatory E-Verify could render a worker unemployable because they cannot get work clearance from the system. Meaningful due process under E-Verify should:

- Create an administrative review process for erroneous final non-confirmations (FNCs) with worker protections, including a stay of the FNC while the worker pursues the appeal;

- Create an appeal process for the administrative review, including a stay of the FNC while the worker pursues the appeal;

- Create a judicial review process for the administrative appeal with remedies for wrongly terminated workers, including damages and reinstatement;

- Establish a 24-hour hotline, with interpretation available in multiple languages, which will receive inquiries from workers and employers concerning determinations made by E-Verify; and

- Prohibit employers from misusing E-Verify and create penalties for misuse.

Currently, there is no formal redress for workers who receive an erroneous FNC resulting in a bar from employment. In some cases USCIS or the Office of Special Council for Immigration-Related Unfair Employment Practices (OSC), has intervened to correct erroneous FNCs, but this cannot be a meaningful substitute for a formal process. While there is currently a DHS employee hotline, it is only available 8:00 a.m. to 5:00 p.m. and has representatives who speak English and Spanish. Because many low wage workers often work long hours at multiple jobs and speak languages other than English or Spanish, the hotline must be more accessible.

Ultimately without a formal process, E-Verify errors place an enormous financial burden on workers, particularly those who are low-income. Without redress, and with job loss, low wage workers face challenges including eviction and loss of health care benefits. It is unacceptable that work-authorized citizens and immigrants lose their jobs and suffer economic hardship due to errors in the verification system, and when that does happen they should be compensated.

III. Conclusion

For all of the above reasons, the ACLU believes that E-Verify is a fatally flawed system. It should not be mandated nor should it be part of any comprehensive immigration reform update.