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 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

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 po

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

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]

creation of a new employment blacklist –a “No-