

June 29, 2011

United States Senate
Washington, DC 20510

Re: **Oppose E-Verify and any Mandatory Provision Expanding the System**

Dear Senator:

We write today to express in the strongest possible terms our opposition to H.R. 2164, the “Legal Workforce Act”. H.R. 2164 would mandate the use of the bureaucratic E-Verify system and for the first time in history require every American to be checked against an error prone government database. If a worker’s information is incorrect in E-Verify, he or she can’t work until the problem is resolved. In addition to the harmful effects this process would have on workers and the economy, we believe the risks to individual privacy are too great and the likely benefits are too small to justify inserting the federal government into every hiring decision made by every employer across the country.

A nationwide mandatory E-Verify system would be one of the largest and most widely accessible databases of private information ever created in the U.S. Its size and openness would present an irresistible target for identity thieves. Additionally, because the system would cover everyone eligible to work in the United States, it could quickly expand to a host of other uses for the intelligence community, law enforcement, and corporate America.

The current E-Verify system, implemented in a small fraction of the country’s workplaces, 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 links to a variety of other databases such as the Customs and Border Patrol (CBP) TECS database (a vast repository of Americans’ travel history) and the Bureau of Citizenship and Immigration Services (CIS) BSS database (all immigration fingerprint information from US VISIT and other sources).¹ CIS has recently announced the inclusion of drivers’ license information from at least one state.²

Because E-Verify contains photos and will very soon contain drivers’ license information it could quickly evolve into a national identity system. E-Verify is internet-based and hence available almost anywhere. If the system is expanded, it could easily be used to verify drivers’ licenses at airports or federal facilities and combined with travel, financial, or watch list information. The errors and problems with E-Verify would then transform from employment issues to problems with travel and other fundamental freedoms.

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

¹ 73 Fed. Reg. 75449.

² Notice of Privacy Act System of Records, 76 Fed. Reg. 26738 (May 9, 2011), available at <http://www.gpo.gov/fdsys/pkg/FR-2011-05-09/html/2011-11291.htm>

2004, more than 510 million records have been hacked, lost or improperly disclosed including E-verify databases.³ In October 2009, and again in December 2009, Minnesota state officials learned that the company hired to process their E-verify forms had accidentally allowed unauthorized individuals to gain access to the personal information of over 37,000 individuals due to poor authentication practices and web application vulnerabilities in their system.⁴ If the Department of Homeland Security and states are unable to provide proper data security, we cannot possibly expect small business across America to do so.

H.R. 2164 also contains a pilot biometric ID card program. This program would allow any employer to fingerprint all employees and would create private sector “enrollment providers”. These providers would combine biometrics, information from employers, commercial databases, and information from DHS and Social Security Administration – all for the purpose of identity verification. Such a card would exacerbate the existing problems with E-Verify by adding additional sensitive information and allowing it to be kept in private hands.

For all of these reasons, we oppose H.R. 2164 and any expansion of the E-Verify system and we urge you not to move the bill from committee.

Sincerely,

American Civil Liberties Union

American Library Association

American Policy Center

Bill of Rights Defense Committee

Center for Digital Democracy

Competitive Enterprise Institute

Consumer Action

Consumer Watchdog

Cyber Privacy Project

Defending Dissent Foundation

Electronic Frontier Foundation

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

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

The 5-11 Campaign

Identity Project

Liberty Coalition

The Multiracial Activist

The National Center for Transgender Equality

National Workrights Institute

PrivacyActivism

Privacy Rights Clearinghouse

Privacy Times

The Rutherford Institute

United Sikhs

Former Congressman Bob Barr

Law Professor Chip Pitts, Stanford Law School & Oxford University