



Eastern Region Office
PO Box 60173
Philadelphia, PA 19102
215-592-1513 T
215-592-1343 F

Central Region Office
PO Box 11761
Harrisburg, PA 17108
717-238-2258 T
717-236-6895 F

Western Region Office
PO Box 23058
Pittsburgh, PA 15222
412-681-7736 T
412-681-8707 F

MEMORANDUM

TO: The Pennsylvania Senate

FROM: Elizabeth Randol, Legislative Director, ACLU of Pennsylvania

DATE: June 25, 2019

RE: OPPOSITION TO HB 1170 P.N. 2129 (Mackenzie)

[House Bill 1170](#) seeks to prevent unauthorized workers from gaining employment by requiring that all construction workers seek permission from the government when starting a job. In order to detect the small percentage of job seekers who are unauthorized workers, a mandatory E-Verify system creates a whole new level of intrusive government oversight of daily life—a bureaucratic “prove yourself to work” system that hurts ordinary people.

Expanding mandatory E-Verify in Pennsylvania would impose unnecessary and unacceptable burdens on America’s workers and businesses. It would contribute to a massive government database of workers’ information that threatens privacy and could be used to facilitate additional forms of data surveillance. In addition, given the E-Verify error rate, mandatory use could result in authorized workers being denied the ability to work without a meaningful avenue to seek redress.

On behalf of over 100,000 members and supporters of the ACLU of Pennsylvania, I respectfully urge you to vote ‘no’ on House Bill 1170 for the following reasons:

E-Verify poses a significant risk to the privacy and security of American workers

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, 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).¹ 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 hack or surveil American workers. In fact, just this June, [CPB’s database was hacked](#) as part of a malicious cyberattack, compromising the database that includes facial recognition and license plate photos.² Because of its scope, it could build surveillance profiles of every American and could be easily combined with travel, financial, or communication data. Some of these databases linked to E-Verify are already mined for data.³ ‘Undesirable’ behaviors – from unpopular speech to gun ownership to paying for items with cash – could be tracked and investigated by the government.

¹ 73 Fed. Reg. 75449.

² Harwell, Drew. “U.S. Customs and Border Protection says photos of travelers were taken in a data breach.” The Washington Post, 10 June 2019.

³ U.S. Dept. Of Homeland Security, Privacy Impact Assessment Update From The USCIS Person Centric Query Service Supporting Immigration Status Verifiers Of The USCIS National Security And Records Verification Directorate/Verification Division (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_pcq_nsrv_update.pdf.

E-Verify invites misuse and its inaccuracies disproportionately harm vulnerable communities

From the inception of the program, the GAO and DHS have repeatedly documented various types of misuse of E-Verify by employers. A [study](#) commissioned by the U.S. government confirmed that many employers were engaging in various activities that are prohibited under E-Verify in order to protect workers' rights. For example:

- 17.1% of the employers admitted to restricting work assignments until authorization was confirmed
- 15.4% reported delaying training until employment authorization was confirmed
- 2.4% reported reducing pay during the verification process⁴

Despite efforts to improve its unacceptably high error rate, E-Verify remains [plagued by inaccuracies](#).⁵ [Errors](#) due to typos, name changes due to marriage, and even simply placing additional spaces after someone's name⁶ are mistakes that affect thousands of workers and employers each year. E-Verify in its current form has [barred thousands of legal workers from working](#). Moreover, a [study](#) by the Government Accountability Office (GAO) found that error rates in the system were higher for foreign-born employees versus U.S. born employees.⁷ Taken together, these abuses and deficiencies would disproportionately affect poor workers, [immigrant workers](#), [women](#), and communities of color.

E-Verify lacks sufficient due process protections for workers with a Tentative Non-Confirmation (TNC)

If the government wants to block a person from working, the burden should be on it to demonstrate that the person is ineligible. But E-Verify places the *burden on workers* - who *rely on employers* to notify them of a TNC - to navigate a complex, tedious bureaucracy to prove their eligibility to work. Untangling the source of an E-Verify error is no easy feat. Individuals are often [not informed](#) what specific records are the source of the E-Verify determination, even though that notification is required under the terms of E-Verify.⁸ Workers [face challenges](#) in determining how to access their own information or seek corrections.⁹ Those who receive a TNC (nonconfirmation) are thrown into a situation where they must affirmatively reach out to the giant bureaucracies at the Social Security Administration or the Department of Homeland Security (it will be up to them to figure out which) and set about fixing whatever bureaucratic problem is blocking them from getting a job. If the employee decides to contest the TNC, s/he must visit SSA or contact DHS within [eight federal workdays](#) and inform the employer of the decision. They must then wait for their employer to receive their results. In the weeks or months it takes to overcome these challenges, workers can be fired or have employment offers withdrawn through no fault of their own. Many workers never learn they have the right to appeal their determinations and are forced to just find another job. Others don't have the time, education, or ability to tackle the problem effectively. Ultimately, the threat is that this system will result in the creation of a de facto 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.

For these reasons, we ask you to vote ‘no’ on House Bill 1170.

⁴ Westat on behalf of the U.S. Department of Homeland Security, “Findings of the E-Verify Program Evaluation,” December 2009; http://www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20EVerify%20Report%202012-16-09_2.pdf.

⁵ U.S. Citizenship and Immigration Services, *Summary of the Evaluation of the Accuracy of E-Verify Findings*, http://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/EVerify%20Studies/E-Verify%20Accuracy%20Report%20Summary.pdf.

⁶ American Civil Liberties Union, *Prove Yourself To Work: The 10 Big Problems With E-Verify* (2013), https://www.aclu.org/sites/default/files/field_document/everify_white_paper.pdf.

⁷ Gov't Accountability Off., *Federal Agencies Have Taken Steps To Improve E-Verify, But Significant Challenges Remain* (2010) at 40, <http://www.gao.gov/products/GAO-11-146>.

⁸ National Immigration Law Center, “Expanding E-Verify Will Undermine Job Growth and Cripple Small Business,” Jan. 2011, www.nilc.org/document.html?id=327.

⁹ Alex Nowrasteh & Jim Harper, *Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate*, CATO Inst. July 7, 2015, at 4, https://object.cato.org/sites/cato.org/files/pubs/pdf/pa775_1.pdf.