STREAMLINING WORK AUTHORIZATION OR ENDANGERING PRIVACY RIGHTS?
THE RAMIFICATIONS OF A NATIONAL E-VERIFY MANDATE

Anabella Lojpur
INTRODUCTION

With the current public divisions over immigration policy, it is no surprise employers face heightened scrutiny of hiring practices to ensure the work authorization of their employees. Most recently, E-Verify, an electronic eligibility verification system through which employers can confirm identity documents against federal databases, became the subject of renewed public attention after the murder of a young woman.\(^1\) The alleged killer was an undocumented immigrant and worked at a nearby farm.\(^2\) To verify the worker’s employment eligibility, the employer completed the required Form I-9 but used an employment verification system other than E-Verify.\(^3\) Both lawmakers and citizens began calls for a national E-Verify mandate.\(^4\) However, the belief that a national E-Verify mandate would have prevented the tragedy is misplaced because the worker assumed another's identity, which allowed him to circumvent the E-Verify system, an all too common occurrence.\(^5\) Rather than stopping undocumented immigrants from gaining employment—the system’s intended purpose—E-Verify has created a string of unintended consequences, and if its use is nationally mandated, the verification system has potential to become a privacy catastrophe.

---


\(^2\) Id.

\(^3\) The employer used the Social Security Number Verification Service (SSNVS) that verified that the name and number matched. *Id.*


This paper discusses the ramifications that a national E-Verify mandate will have on Personally Identifiable Information (\textquotedblleft PII\textquotedblright)\textsuperscript{6} and the system’s increased threats to employees’ overall privacy rights. Specifically, the retention of PII and detriment to employees’ public access rights are analyzed in terms of individual employees, as well as their bargaining representative’s ability to protect these rights. Part I discusses the beginnings of required employment authorization for undocumented immigrants in order to understand the incidental impacts of the verification process. Part II provides a background on E-Verify, the electronic verification system itself, and the current state of the system; it also emphasizes the differences in standpoints among states. The system’s fatal flaws are highlighted and the deficiency in attaining its purpose: turning off the “wage magnet,” an illusory magnet that attracts migrants to reside in the United States for employment opportunities.\textsuperscript{7} This paper presents the argument that a nationally mandated E-Verify system, being disguised as a promising solution to unauthorized employment, is only a temporary mend that will threaten employees’ privacy rights by increasing third party access, curtailing employee access rights, and prolonging retention periods of PII. Unless Congress passes a comprehensive immigration reform bill that gives heavy consideration to employee privacy rights, a national E-Verify mandate will certainly threaten workers’ privacy rights.

\textsuperscript{6} PII can include “[a]ny representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.” U.S. Dep’t of Labor, \textit{Guidance on the Protection of Personal Identifiable Information}, DOL.GOV, https://www.dol.gov/general/ppii (last visited Dec. 4, 2018).

I. BEGINNINGS OF REQUIRED EMPLOYMENT AUTHORIZATION

In the late 1980s, long-time undocumented immigrants, individuals without authorization to reside or work in the United States, became eligible to apply for legal resident status and work authorization through the Immigration Reform and Control Act of 1986 (“IRCA”). Specifically, the Act’s stipulations allowed noncitizens who could prove continuous residence in the United States before January 1, 1982, to petition the government for status, as long as they did so by May 4, 1988. Since the Act’s intended purpose was to control and deter illegal immigration to the United States by cutting of the “wage magnet,” Congress incorporated a provision ensuring the authority to sanction employers who knowingly hire undocumented workers. While simultaneously constructing a pathway towards legal status for noncitizens who were previously undocumented, the Act closed off possibilities of legal employment for noncitizens who failed to meet the stringent residence requirements. As a result, these undocumented immigrants became unable to enter the formal labor market.

For practical purposes, the Act created an employment verification process for new hires through completion of a Form I-9. To comply with the Act, a work authorization document, such as an individual’s Social Security Card (“SSC”) and an identifier, a Driver’s License, was sufficient to prove the individual’s identity and eligibility to work in the United States. Consequently, these identity documents became items of extreme

---

9 Id. § 1255.
10 Id. § 1324a(4)(A)(i)–(iii).
value, which led to a “massive boom in the creation and sale of black market SSNs, identity theft, and voluntary identity loans\(^\text{13}\) that allow[ed] employers to obey the letter of the law when collecting I-9 Forms and for illegal immigrants to continue to work.”\(^\text{14}\) Undocumented immigrants who had become ostracized from the formal labor market were now able to circumvent the system by fraudulent means. Individuals that were unwilling to succumb to fraudulent means or simply unable to attain facially valid documents did not leave the United States; the incentive to remain in the country after the Act was not reduced as intended. Instead, undocumented workers faced a significant reduction in wages\(^\text{15}\) and worsened employment conditions\(^\text{16}\) because employers could turn a large profit knowing the desperation of the workers. Thus, the Act had the pervasive effect of increasing use of fraudulent documents and the number of opportunistic employers rather than decreasing the “wage magnet.”\(^\text{17}\) To combat these unfavorable results, the Immigration and Naturalization Service\(^\text{18}\) (“INS”) launched the

\(^{13}\) It is much harder for the government to identify when identity loans are occurring since the lender is voluntarily allowing another to use their identity. Nowrasteh, \textit{Mandatory E-Verify will Increase Identity Theft}, supra note 5 (“Retired workers, relatives, and legal immigrants who return to their home countries . . . sell or give their identities to [undocumented] immigrants so they can work legally.”).

\(^{14}\) \textit{Id.}

\(^{15}\) Workers found themselves facing up to 24 percent reductions in wages. Freedman et al., \textit{supra} note 11, at 124.

\(^{16}\) \textit{Id.}

\(^{17}\) After the amnesty period expired, the monthly immigration rate was nearly 0.7 percent higher than it had been during the period. \textit{Id.}


II. E-VERIFY: THE ELECTRONIC VERIFICATION SYSTEM

E-Verify is an electronic employment verification system that compares information completed from an individual's Form I-9 to the records of the Social Security Administration (“SSA”) and Department of Homeland Security (“DHS”). Once an employee completes Section I of the Form I-9, the employer then completes Section II, and if enrolled in E-Verify, inputs the information from both sections into the electronic portal. Use of the electronic system does not replace an employer’s duty to complete the physical form; rather, the relationship between the two is akin to one of companionship. However, it does provide insulation for employers from liability and civil fines by creating a rebuttable presumption that the employer did not knowingly hire an unauthorized worker since a government system processed the verification. The employer must comply with all other responsibilities noted in the contract with DHS to maintain this rebuttable presumption. The program is available in all states, but mandatory usage of the electronic verification system varies across states. Some states require that employers use the program, others restrict the system’s use, and many states maintain

---

21 EMPLOYER HANDBOOK, supra note 7, at 10–19.
24 Id.
a middle ground of voluntary participation. However, if the employer has federal contracts or subcontracts that are subject to the Federal Acquisition Regulation E-Verify clause, usage is mandatory regardless of state laws.

In those states whose law mandates E-Verify usage for all employers, compliance has been less than ideal. For example, in Arizona, a state with one of the strictest immigration laws, only 59 percent of new employees were verified through the electronic system in 2017. South Carolina, another state with mandated E-Verify usage and strict state-wide immigration laws, managed to achieve compliance rates of a mere 55 percent in 2017. The reasoning behind lower compliance rates despite mandates involves economic interests for both employers and states. Employers weigh the risks when determining whether or not to comply with E-Verify usage after registration, and states shy away from enforcement actions because they do not want their local economy to suffer. The end result is the use of unauthorized workers. For instance, South Carolina relies heavily on its immigrant workers to maintain one of the largest poultry industries.

27 Nowrasteh, E-Verify Wouldn’t Have Prevented Mollie Tibbetts’ Murder, supra note 1.
29 Nowrasteh, E-Verify Wouldn’t Have Prevented Mollie Tibbetts’ Murder, supra note 1.
in the U.S.;\textsuperscript{31} in 2017, two percent of employers in the state were audited for their E-Verify compliance, and only 17 percent of those employers faced penalties.\textsuperscript{32}

According to DHS, the E-Verify system has high accuracy rates since it confirms 98.91 percent of employees as authorized to work within 24 hours.\textsuperscript{33} However, this appearance is a façade because it does not consider the reality of document fraud. In 2009, “E-Verify authorized 54 percent of workers that it was supposed to reject, mainly because of document fraud.”\textsuperscript{34} This inaccuracy highlights a fundamental design flaw in the system still present today—confirmation of the documents the worker hands the employer against government databases, fails to verify the worker himself. To combat this deficiency, DHS implemented a photo matching feature within E-Verify.\textsuperscript{35} However, the photo matching feature is less sophisticated than necessary; it can only match photos from U.S. passports, permanent resident cards, and employment authorization cards.\textsuperscript{36} It does not have the ability to match driver’s license photos,\textsuperscript{37} which is the most frequent identity document presented to employers.\textsuperscript{38} The employer is not allowed to specify which

\textsuperscript{32} Jan, supra note 30.  
\textsuperscript{37} Id.  
\textsuperscript{38} Driver’s Licenses are presented 80 percent of the time as identity documents in the work authorization process. U.S. Dep’t of Homeland Sec., U.S. Citizenship & Immigration Servs.,
identity document a worker presents for authorization; doing so would run afoul of the anti-discriminatory protections offered by the Immigration and Nationality Act (“INA”) and the Civil Rights Act of 1964 (“Title VII”).

Employers are hesitant to confront workers if they have any suspicions about the worker’s name or identity because they do not want to be exposed to discrimination lawsuits. The worker allegedly responsible for the tragic murder of a young woman presented a Social Security Card and matching Driver’s License under the name of John Budd. Even if the employer had used E-Verify, the photo matching service would not have been triggered since the worker presented a Driver’s License. Thus, the documents the employee presented were verified, rather than the employee himself. If the employer were to question the name and identity of the farm worker, or even ask for another identity document, it would have exposed itself to a serious discrimination charge or lawsuit.

As a further wrinkle, the online based system can only be used for initial verification of the newly hired worker. If the employee presents documents evidencing work authorization such as an “Employment Authorization Document” (“EAD”), a card issued to immigrants when they gain lawful status that allows for work authorization,

39 EMPLOYER HANDBOOK, supra note 7, at 54.
40 Nowrasteh, E-Verify Wouldn’t Have Prevented Mollie Tibbetts’ Murder, supra note 1.
41 Id.
42 The employer used the Social Security Number Verification Service (SSNVS) that verified that the name and number matched, supra note 1.
43 See Driver’s License Verification, supra note 38.
the employer must re-verify that employee’s work authorization upon the expiration of
the document.45 Most EADs are valid for a period of one year.46 Since E-Verify cannot be
used for reverification, the employer must fill out the appropriate portion of the Form I-
9 instead.47 If the employee is a U.S. citizen or Legal Permanent Resident (“LPR”),
rererification is forbidden unless the employee departs and is then rehired after three
years.48 Thus, mandated E-Verify across states will fail to guarantee continued
employment authorization of those workers who are viewed as having the most likelihood
of being unable to attain renewed employment authorization, i.e., those with temporary
status.

The loopholes of the electronic verification system will only continue should a
national mandate be enacted, preventing the system from achieving its intended purpose
in both the short-term49 and long-term.50 Instead a mandate will likely result in threats
to employees' privacy rights by increasing third party access, curtailing employee access
rights, and prolonging retention periods of PII.51 This situation is a result of the
government’s failure to combat the deficiencies effectively without requiring draconian
measures. Some measures explored in the past by members of Congress include adding
additional biometric identifiers such as fingerprints to the process through “biometric

45 Id.
46 With the exception of EADs granted to asylees, which are valid for a period of two years.
U.S. Dep’t of Homeland Sec., U.S. Citizenship & Immigration Servs., USCIS Increases
Validity of Work Permits to Two Years for Asylum Applicants, USCIS.GOV (Oct. 6, 2016),
https://www.uscis.gov/news/alerts/uscis-increases-validity-work-permits-two-years-asylum-
applicants.
47 Section 3 of the I-9 Form is used for reverification. U.S. CITIZENSHIP & IMMIGRATION
48 EMPLOYER HANDBOOK, supra note 7, at 20.
49 As a result of document fraud.
50 As a result of E-Verify’s inability to conduct reverification of workers.
51 See infra Part III.
identity cards” which would be used by employers in the work authorization process. Of course, privacy concerns and high start-up costs soon rendered the measure inoperative and likely remain valid obstacles today.

III. IMPEDING PRIVACY CATASTROPHE

A. Third Parties

If a national E-Verify mandate were to be enacted, third party contractors will gain access to employees PII at alarming rates while at the same time being thrown into a revitalized market of employers seeking their E-Verify contractor services. For those employers who wish to outsource the E-Verify process, DHS allows for employers to use third party agents, E-Verify Employer Agents (“employer agents”), to confirm a new hire’s work authorization. For businesses who want to avoid the ancillary expenses of implementing E-Verify into their administrative structure, outsourcing is often the most reasonable option. The dual focus of smaller employer agents—to remain competitive in an emerging market while simultaneously developing safeguards for


highly sensitive PII—will likely result in inadequate protection of an employees’ PII. The PII entered into the E-Verify system does not simply include an individual’s name, contact information, or SSN like information used in traditional background checks; it includes scans of highly sensitive documents such as passports, Legal Permanent Resident cards, and other work authorization documents. Of course, outsourcing would also increase data transmission rates between the employer and the employer agent. The process of outsourcing the electronic verification, as well as the transmissions between employer and employer agent, would substantially rise if employers found themselves forced to comply with a process they viewed as unfamiliar, burdensome, and expensive. Not only does outsourcing electronic verification increase the number of individuals with access to the information, more concerning is the fact that DHS does not certify these employer agents or control the fees that may be charged for their services.\footnote{Using E-Verify Agent, supra note 54.}

To use a recent example, Equifax was the subject of a massive data breach that affected 143 million individuals.\footnote{Alex Johnson, Equifax breaks down just how bad last year’s data breach was, NBC NEWS (May 8, 2018, 6:25 PM), https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496.} Specifically, hackers gained access to SSNs and identifiers such as driver’s license numbers that individuals uploaded into an online credit dispute portal.\footnote{182,000 to be exact. Id.} Equifax is used by employers for a variety of services including background checks, credit reports, and most important to this analysis, as an E-Verify Employer Agent. Currently, it is one of the largest E-Verify employer agents\footnote{Product Overview, EQUIFAX, https://www.equifax.com/business/simplify-e-verify/ (last visited Dec. 4, 2018).} and is also used by DHS as its third-party identity assurer to process the information in its “Self-
Check E-verify” portal. Although the compromised data in last year’s breach was specific to a dispute portal related to credit reports, it is eerily similar to portals used by E-Verify. The online Self-Check E-Verify portal allows individuals to check their own employment eligibility by inputting the required identity and work authorization information and then sending that information to Equifax to confirm an individual’s identity. DHS even boasts that the “process is very similar to what a bank or credit agency does to confirm someone’s identity online,” attempting to assure the user of the ordinariness of its operations.

The E-Verify portal used by employers and their employer agents goes even further. Instead of simply inputting an employee’s PII, if an employee presents certain identity documents with the Form I-9, the photo matching tool is automatically triggered within E-Verify. Now, the employer must compare the identity documents presented by the employee with the photo derived from E-Verify. If the employer has multiple hiring sites, common with dispersed workforces, each hiring site will be required

61 Id.
63 If the identity document is a passport, LPR card, or EAD card the photo matching tool is triggered.
65 Id.
to relay the PII to the employer agent.\textsuperscript{66} Equifax has access to millions of PII submitted by employees and photos from DHS’s databases and must process it back and forth between itself and the employer.

The Memorandum of Understanding (“MOU”) between DHS and the employer agent states, “If data is transmitted between the E-Verify Employer Agent and its client, the [employer agent] agrees to protect personally identifiable information during transmission to and from the [employer agent].”\textsuperscript{67} But the MOU does not specify how the employer agent must protect the PII. It provides no guidance or mechanisms for the employer agent to adhere to, unlike the privacy provision in the MOU between the DHS and the employer.\textsuperscript{68} Furthermore, DHS boasts that it protects an individual’s PII collected and used through E-Verify in accordance with the Privacy Act of 1974 (“Privacy Act”).\textsuperscript{69} However, since approximately 80 percent of individuals present driver’s licenses when completing the Form I-9, the Privacy Act would fail to protect information from the submitted Driver’s License, as well as the scan of the document itself because the PII is derived from a state agency. The Privacy Act’s protections are limited; it only provides


safeguards for information from documents that have been issued by federal agencies. Employees will find their privacy rights hinging on inadequate provisions within the MOU and state laws, all varying in the level of protections afforded to residents. Additionally, individuals who are not citizens or LPRs are no longer afforded protections under the Privacy Act of 1974 Act because their privacy rights were repealed in last year's executive order. As a result, under the MOU, “a two-tier system is created for data protections” that would distinguish employees with temporary status. These workers will have the added concern about DHS sharing their PII with other agencies unbeknownst to them.

Equifax and other large employer agents will see huge opportunities for increased profits under a national E-Verify mandate. Employer agents are free to increase fees associated with its service because DHS does not regulate the financial aspect of its

---

71 See John Feere, An Overview of E-Verify Policies at the State Level, Center for Immigration Studies (July 26, 2012), https://cis.org/Overview-EVerify-Policies-State-Level, for an overview of privacy protections and recourse offered by various states.
72 Non-citizens and those who do not have permanent resident status have had their protections revoked through President Trump’s executive order. Exec. Order No. 13,768, 82 Fed. Reg. 8,799 (Jan. 30, 2017) (“Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.”).
74 The MOU includes a provision about how information can be used by signatories to the document and other partner agencies limited to purposes for work authorization. Commitment to Privacy, supra note 69. This list has potential to become infinite for those with temporary immigration status.
Employers would face high implementation and maintenance costs, leading them to search for smaller, more affordable employer agents. The smaller employer agents will have to ensure competitiveness within the market, which will likely result in employee privacy as collateral damage. Many employer agents are authorized by USCIS, but this authorization follows an online registration for the E-Verify system, a brief tutorial, and the signing of the MOU. It is by no means an attestation of adequate privacy standards. There is no established method for DHS to assess the privacy measures of each employer agent. Perhaps this is the reason DHS refuses to certify the authorized employer agents. If one of the nation’s largest and most sophisticated identity assurers such as Equifax can be the victim of a large-scale breach, one can only ponder the privacy risks that would result from a surge of smaller employer agents with less security resources, all competing to establish themselves in the newly revitalized industry of electronic employment verification.

B. Employee Access Rights

Employee access rights to PII will further deteriorate under a national E-Verify mandate. When an employer enters the employee’s information from the completed I-9 Form into the E-Verify system, the system cross-checks the entered information with that of DHA and SSA records. If the information does not match, a “Tentative Non-Confirmation” (“TNC”) specific to either DHS or SSA results. However, the TNC does not

---

77 See About E-Verify, supra note 20.
always mean that the worker is not authorized for work.\textsuperscript{78} There are various reasons why a TNC may be issued. Some examples include: name changes after marriage, a change in immigration status, or errors committed while entering the information from the I-9 Form into the E-Verify system.\textsuperscript{79} Through the first quarter of 2018, 98.91 percent of new hires were automatically confirmed to work through the E-Verify System.\textsuperscript{80} This statistic is misleading because it does not take into consideration the system’s deficiencies such as document fraud. This aside, it is important to note the ramifications to the 163,114 individuals who were initially not confirmed as work eligible.\textsuperscript{81} A small number of cases were confirmed after the initial mismatch\textsuperscript{82} but approximately 91,343 individuals did not contest the mismatch, some because they chose not to, and others because they were not aware of the opportunity to do so. Another 57,089 individuals were left with unresolved cases due to a delay in awaiting further processing by the SSA or DHS.\textsuperscript{83}

When the mismatch results, employers are required to provide the individual with a “Further Action Notice,” which contains the employee’s basic PII such as their name, DOB, and SSN, in order for the worker to confirm whether the information is correct. The form also instructs the individual on how to correct a TNC, which they must do within eight federal government workdays otherwise the employer can terminate the

\textsuperscript{80} See E-Verify Performance, supra note 33.
\textsuperscript{81} Id.
\textsuperscript{82} Approximately 13 percent of initial non-confirmations are later confirmed. Id.
employment relationship.\textsuperscript{84} Although employers are required to ensure distribution of the “Further Action Notice” by the MOU, they often fail to do so\textsuperscript{85} and the employee is left without knowledge of where to turn. For individuals faced with unfamiliarly of the appropriate government agencies, figuring out a way to remedy the situation is often a daunting task.

Although DHS offers the E-Verify Self-Check Portal,\textsuperscript{86} the portal fails to provide full access rights. Through the portal, an individual can check their employment eligibility as job seekers. It does not provide the employee with information entered by employers or employer agents for purposes of employment verification once the employee has been hired or terminated as a result of a TNC. For example, if an employer or employer agent made a typographical error while entering the employee’s information, the employee would not be able to view the inaccurate information through their own portal. Consequently, the self-check portal fails to provide full access rights.

Failure to provide full access rights to PII used for employment verification is an issue states have been grappling with since the inception of E-Verify. As a result, some states have created their own E-Verify compliance laws, allowing employees, or prospective employees, to bring private actions against their employers for violations. In 2007, Illinois amended its own “Right to Privacy in the Workplace Act” prohibiting private employers from using E-Verify.\textsuperscript{87} Specifically, the state legislature called the federal government’s authority into question, noting their concerns about inaccurate non-

\textsuperscript{84} Id.
\textsuperscript{86} See sources cited supra note 62 and accompanying text.
confirmations and privacy issues. To no surprise, DHS challenged the legislation in federal court before it took effect. Ultimately, the court held that the amendment was “invalid in violation of the Supremacy Clause of the United States Constitution, and the State of Illinois [became] permanently enjoined from enforcing this invalid act.” Despite the loss, the state legislature persisted in attempts to protect its citizens and passed another amendment to the same Act. The new law placed additional responsibilities on employers that choose to use E-Verify, such as the completion of a sworn attestation from the Illinois Department of Labor. Additionally, the amendment mandated that employers notify individuals of the TNC and give them the option to contest the result.

Although the amendment does not prevent all occurrences of employers’ failure to provide notice and basic PII, it does give individuals a right of private action against their employers for failure to do so, creating the incentive for employers to be vigilant about adherence to the requirements. Illinois is only one of two states that has attempted to block the use of E-Verify, leading it to create supplementary protections to atone for inadequate MOU privacy provisions. Residents of other states who are not U.S. citizens or LPRs are not as fortunate when it comes to additional privacy protections beyond the MOU. Since the MOU is between the employer and DHS, or the employer agent and

88 Id.
89 Id.
90 Id. at *3.
91 820 ILL. COMP. STAT. ANN. 55/1 (West, Westlaw through P.A. 100-1114).
92 Id.
94 E-Verify States Map, supra note 25.
95 Feere, supra note 71.
DHS, only the government has the ability to begin legal actions against either entity, which rarely occurs unless the employer or employer agent is a repeat violator.

Most interventions by IER are not legal in nature but simple telephone interventions that provide guidance to the employer after the violation has occurred. For example, an employee was suspended from work after receiving a TNC from the electronic verification system. The employer failed to provide the prospective employee with the notice paperwork that includes instructions for contesting the TNC as well as the basic PII. The employee eventually got in contact with IER, who then reached out to the employer to explain proper E-Verify procedures. After a prolonged period, the employer offered reinstatement to the employee. By this point, the employee had moved on to another job. The administrative hassle of dealing with attempts to gain access to PII to confirm whether the data was accurate often leads many employees to simply move on because they cannot afford periods without pay. Thus, unless the individual lives in a state that has created private actions for E-Verify violations, the individual is often left without recourse.

The difficulty of accessing PII is not limited to the individuals seeking employment themselves; if a workforce is unionized, elected bargaining representatives also have experienced hurdles in accessing information on behalf of their employees. For example, the National Labor Relations Board (“NLRB”) recently held that enrollment into E-Verify, in those states which enrollment is voluntary, without Union consent violates the

---

96 See generally E-VERIFY MOU FOR AGENTS, supra note 67; E-VERIFY MOU FOR EMPLOYERS, supra note 68.
97 See Telephone Interventions, supra note 85.
98 See Example: New York, New York for Fiscal Year 2018. Id.
99 Id.
The National Labor Relations Act (“NLRA”). The Board, and the Administrative Law Judge, found that the employer violated various provisions of the NLRA when it enrolled into E-Verify without the Union’s authorization; the Board considered the inability of the representatives to assist affected employees either by accessing copies of relevant records to allow the individual to confirm the records or help direct them to the appropriate agencies in order to establish work authorization. The employer was ordered to rescind its participation in the E-Verify System.

It seems as other countries are increasing their worker’s privacy rights, the U.S. is doing the opposite, with added detriment to its immigrant population. A similarity between the recent U.S. Executive Order restricting the privacy rights of those with temporary status and the acts of the United Kingdom highlight the deterioration of privacy protections for immigrant workers in the two countries. The United Kingdom recently introduced the Data Protection Act of 2018, with an exception that states GDPR rules “do not apply to personal data processed for . . . the maintenance of effective immigration control.” Taking note of the United Kingdom’s exit from the European Union, the bill is still moving through parliament, but if enacted, means that where status or work authorization was refused, individuals would not be able to see and challenge the information that the decision relied upon. They would be denied their

---

101 See generally id.
102 Id.
103 See generally European General Data Protection Regulation 2016/679 [hereinafter GDPR].
105 Woollacott, supra note 73.
right to “Subject Access Requests”\textsuperscript{106} should the exemption be found to apply. Human rights groups have requested judicial review of the exemption, stating that the exemption “[is] contrary to the General Data Protection Regulations as well as incompatible with EU law generally and the European Convention on Human Rights.”\textsuperscript{107} The exemption also applies to non-government agencies including, but not limited to, employers, landlords, and banks.\textsuperscript{108} Could this be where the United States is headed if it were to accept a national E-Verify mandate?

C. **Retention of PII**

If a national E-Verify mandate is enacted, retention duration of employees’ PII will exponentially rise, resulting in increased security risks for employees. Employers will be led to retain PII information longer than any business necessity requires in fear of penalties. The regulations concerning the retention of I-9 records\textsuperscript{109} vary based on whether the employee is a current or past employee. “Once the individual’s employment has terminated, the employer must determine how long after termination the Form I-9 must be retained, either three years after the date of hire, or one year after the date employment is terminated, whichever is later.”\textsuperscript{110} If E-Verify is used, records are maintained for *ten years*, and purged annually after that in accordance with the National

\textsuperscript{106} Admin, *GDPR—Could This Be the End to Subject Access Requests in Immigration Cases?*, JM WILSON SOLICITORS (Apr. 9, 2018, 12:12 PM), http://jmwilsonsolicitors.com/gpdr-immigration/.

\textsuperscript{107} Woollacott, *supra* note 73.

\textsuperscript{108} Id.

\textsuperscript{109} I-9 Records consist of the I-9 Form itself, as well as copies of the identity and work authorization documents.

Archives and Records Administration\textsuperscript{111} ("NARA") to reduce security and privacy risks. The seven-year difference between retention regulations of Form I-9s and E-Verify records should be of concern to both employees and employers.

As related to employers, DHS does not simply have access to the E-Verify records for ten years, authorized by the MOU, but the federal agency has monitoring capabilities during this period as well. The Monitoring and Compliance Branch ("M&C") of DHS is responsible for "monitoring behaviors and use of the system and to ensure compliance with the program’s statutes and guidelines."\textsuperscript{112} The M&C Branch currently does not have the ability to assess any monetary penalties.\textsuperscript{113} It simply relays its compliance findings to Immigration and Customs Enforcement ("ICE"), which has the ability to initiate audits, or the Office of Special Counsel ("OSC"),\textsuperscript{114} which has the ability to begin legal proceedings against the employer. However, this may soon change while the branch has goals of eventually attaining the authority to access fines "[a]s more employers use it and possibly, if it becomes mandatory, the M&C division will get the ability to assess fines."\textsuperscript{115} Instead of minimizing the employer’s use of the employee’s PII, the employer will now be incentivized to maintain records longer. Once the worker has received a confirmation through E-Verify, the employer has collected the PII that is necessary to perform its

\begin{thebibliography}{99}
\bibitem{113} Id. at 2.
\end{thebibliography}
business function—the verification of the new hire. Anything beyond this is in the employer’s self-interest and at the expense of the employee’s privacy.

Employers will fear fines resulting from the M&C Branch’s assessment of their current E-Verify behavior compared with the standards outlined in the MOU. Thus, employers who wish to retain E-Verify records older than ten years in hopes of displaying a past record of compliance or even attempts at compliance, can download the data from the “Historic Records Report” before each annual record clearing.\(^{116}\) This will allow the opportunity for the employer to avoid liability altogether or provide support for its negotiation of monetary fines when it comes to current violations.\(^{117}\) Instead of taking note from the government in refusing to maintain historic PII due to increased privacy and security risks\(^{118}\), employers’ efforts to reduce their liability will undoubtedly do the exact opposite.

As the prolonged retention relates to employees’, their knowledge of the employer’s choice to retain the historic records may be non-existent. The employer is not required to notify the employee of their decision to download the historic data,\(^ {119}\) since the data is synced to the employer’s or the employer agent’s E-Verify account. In cases of notification, the employer is only required to notify the individual if the electronic verification system


\(^{118}\) E-VERIFY FACT SHEET, supra note 119.

\(^{119}\) Id.
results in a TNC during their initial employment verification\textsuperscript{120} to allow the employee opportunity to contest the non-confirmation of their employment eligibility. Even if employers were required to notify a past employee, the process of locating the employee’s whereabouts would likely prove to be a difficult endeavor. Perhaps an employee would feel consolation if they could use the historic data retained by their employer when entering a new job. However, this is not possible because the employee is unable to request data portability of their information submitted into the E-Verify system to new employers.\textsuperscript{121}

CONCLUSION

A national E-Verify mandate fails to provide a resolution to unauthorized employment. It is simply a temporary mend that will threaten employees’ privacy rights by increasing third party access, curtailing employee access rights, and prolonging retention periods of PII. In addition to the privacy risks, E-Verify creates a two-tier system; the system affords those who are citizens and legal permanent residents more privacy protections than those who are not. Congress should consider as an alternative a comprehensive immigration reform bill that gives heavy consideration to employee privacy protections and eradicates the inequality towards those who do not have permanent status. In an increasingly technological world, privacy protections of employees should be of highest concern.


\textsuperscript{121} EMPLOYER HANDBOOK, \textit{supra} note 7, at 4.