Data Without Due Process: Legal Implications of ICE's Emerging Data Mining Practices

Gabriella Majeski

Introduction

Since 2025, the Department of Homeland Security's (DHS) Immigration and Customs Enforcement (ICE) has been leveraging AI-driven data mining to analyze and consolidate sensitive medical, employment, biometric, and personal data of individuals across the United States, raising significant legal and privacy concerns. Data mining, the practice of gathering information from large datasets to uncover patterns or extract insights, allows ICE to flag individuals that may be subject to arrest or deportation, based on the information it gathers about them. These practices coincide with an immigration system backlog exceeding three million cases in 2025. This technology, aimed at expediting deportations in the U.S., could further increase the backlog. The rapid spread of AI-driven surveillance, coupled with the absence of clear legal boundaries governing these practices, has heightened concerns about due process and the erosion of privacy protections for both immigrants and non-immigrants. ICE has been able to acquire a vast amount of sensitive information through private contracts with other government agencies, rather than through the legislature. Since these enforcement mechanisms function within limited judicial oversight, they pose significant risks of constitutional violations and unchecked state power. ICE's increased reliance on private data contracts and information gathering exposes a legal loophole: the government may be achieving through private agreements what certain privacy protections would prohibit. This paper argues that ICE's AI-driven data-mining operations, conducted under vague statutory authority and limited oversight, circumvent Fourth

Amendment protections and threaten fundamental privacy rights, demanding urgent legal review and legislative reform.

Data Mining

There are currently no statutes or laws that specifically grant ICE the authority to enter into data-sharing agreements with private companies or other government agencies. Rather, these actions were taken in private and were not released to the public, according to AP News in July 2025.[1] Furthermore, laws such as the Immigration Nationality Act of 1952, which largely shape the legal landscape of immigration issues in the United States, do not currently address the capabilities of the use of AI-driven analytics to detect individuals and deport them.[2] This is largely because the INA was passed into law long before AI and other sophisticated technologies were developed. As a result, the legality of ICE's practices cannot be clearly determined through the INA alone, leaving those who wish to sue the Department of Homeland Security (DHS) for ICE's practices to look to other provisions for their argument.

In July 2025, a coalition of twenty states, including California, Illinois, Arizona, and Colorado, challenged a recent data-sharing agreement between the Centers for Medicare and Medicaid Services (CMS) and DHS by grounding their claims in privacy concerns.[3] They relied on laws such as the Social Security Act of 1934, the Health Insurance Portability and Accountability Act of 1966 (HIPAA), and the Privacy Act of 1974.[4] By invoking these laws, the states shifted the focus from

[1] Kimberly Kindy & Amanda Seitz, *Trump Administration Hands Over Medicaid Recipients' Personal Data to ICE, AP News* (June 13, 2025), https://apnews.com/article/immigration-medicaid-trump-ice-ab9c2267ce596089410387bfcb40eeb7

[2] Immigration and Nationality Act of 1952 § 287, 8 U.S.C. § 1357 (2018).

[3] Olga R. Rodriguez, *20 States Sue After Trump Administration Releases Private Medicaid Data to Deportation Officials*, AP News (July 1, 2025), https://apnews.com/article/trump-medicaid-immigrant-california-161f7e1b9087512d674258f32f822878

[4] Immigration and Nationality Act of 1952 § 287, 8 U.S.C. § 1357.

ICE's authority to immigration enforcement to the right to privacy and due process, arguing that the transfer of sensitive health information stored in CMS databases violated privacy rights rooted in HIPAA, the Social Security Act, and the Privacy Act. This lawsuit brought into question whether personal data held by government agencies can genuinely remain private when shared through inter-agency agreements that are not released to the public. Later paragraphs of this paper will demonstrate that these practices also overreach the boundaries of the Fourth Amendment's reasonable expectation of privacy standard and the legal precedent set in multiple landmark Supreme Court cases throughout the 20th century.[5]

To understand the scope of ICE's data mining practices, it is important to first examine how this strategy is defined by experts such as senior immigration attorney Heather Yountz and David Morris, former general counsel at Snyc. In an interview with Heather Yountz, an immigration attorney at the Massachusetts Law Reform Institute (MLRI), data mining was defined as "a process of gathering as much personal data about individuals as possible, and then culling through that data to find anything that you're looking for."[6] In ICE's case, Yountz noted how the practice of data mining has been utilized: "The Trump Administration has made data mining its avenue to complete its mass deportation goals. ICE has been trying to collect vast data pools through interagency agreements to gather and glean information from the IRS, I-9 employment documents, and Social Security. The goal of culling through this data is to create a searchable database that would assist ICE in streamlining deportations." The database is known as

Social Security Act of 1934 § 42, U.S.C. § 1396.
Health Insurance Portability and Accountability Act of 1996 § 42 U.S.C. § 1320d.
Privacy Act of 1974 § 5 U.S.C. § 552a

[5] U.S. CONST. amend. IV.

[6] Zoom Interview with Heather Yountz, Senior Immigration Attorney, Mass. Law Reform Institute (Dec. 12, 2025).

the Immigration Lifecycle Operation System.[7] Attorney Yountz further implied that AI technology would then search this database to identify individuals who may be eligible for arrest. She cited instances in which ICE is already disregarding immigration statuses during deportation arrests, such as in a workplace raid where nine employees were arrested in Allston, Massachusetts, in November 2025.[8] These employees all had work authorization, and yet, they were still detained by ICE. She noted that unjust arrests, such as the case in Allston, could be exacerbated by the Immigration Lifecycle Operation System.

In typical fashion, private-sector companies employ techniques such as AI facial recognition and data collection to enhance services or to secure and protect their systems. In contrast, ICE's adoption of such technology could lead to a government-driven erosion of privacy rights in the United States. To gain more insight into the AI-driven security sector, David Morris, former general counsel at Snyk and a Brandeis University alumnus, was consulted regarding the evolving intersection of AI innovation and government regulation of its use. Morris describes cybersecurity as a "vast ecosystem where tools designed for identity protection possess multifaceted capabilities." While these technologies are developed with the genuine intent to combat crime, fraud, and enhance safety, he noted that their power necessitates rigorous oversight. He emphasized that as these tools become more sophisticated, the focus must remain on maintaining the balance between robust public safeguarding and the preservation of individual privacy.[9]

---

[7] Caroline Haskins, ICE Is Paying Palantir $30 Million to Build "ImmigrationOS" Surveillance Platform, WIRED (Apr. 18, 2025), https://www.wired.com/story/ice-palantir-immigrationos/

[8] Abby Patkin, *Backlash Mounts After Boston University Student Claims Credit for Allston ICE Arrests*, Boston.com (Nov. 17, 2025), https://www.boston.com/news/local-news/2025/11/17/backlash-mounts-boston-university-student-claims-credit-allston-ice-arrests/

[9] Zoom Interview with David Morris, Former General Counsel, Snyk AI Security Fabric November 24, 2025.

Morris asserted that the barrier between safeguarding the public and infringing upon their privacy has weakened, as illustrated by ICE's growing reliance on surveillance technologies through its private contracts with companies such as Clearview AI, Palantir, LexisNexis, and Paragon Spyware.[10] Therefore, addressing ICE's overreach could require more than litigation, but rather, legislative reform as well, in order to define the manner in which the Fourth Amendment may allow ICE to data mine, if at all.

Legal Landscape: The Right to Privacy

The modern legal conception of the "right to privacy" was first articulated by Louis Brandeis and Charles Warren in their 1890 Harvard Law Review article, which emphasized the "right to be let alone." This concept is relevant today as ICE data mines in a manner that may infringe on the right to be let alone. Brandeis recognized the impact of science and technology in the 20th century and anticipated their potential to threaten the right to privacy.[11] This foundational definition of privacy influenced Brandeis' dissent in *Olmstead v. United States* (1928), where the Supreme Court considered the constitutionality of using evidence obtained from a wiretap that recorded private conversations without a user's consent.[12] The Court ruled that no violation of Fourth Amendment privacy rights had occurred. In his dissent, Brandeis stated: "The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping…by which it will be enabled to expose to a jury the most intimate

[10] Caroline Haskins, ICE Is Paying Palantir $30 Million to Build "ImmigrationOS" Surveillance Platform, WIRED (Apr. 18, 2025), https://www.wired.com/story/ice-palantir-immigrationos/

[11] Thomas T. Lewis, Constitutional Right to Privacy, EBSCO Research Starters (2025), https://www.ebsco.com/research-starters/law/constitutional-right-privacy

[12] Olmstead v. United States, 277 U.S. 438, 488 (1927).

occurrences of the home."[13] Although the majority rejected Brandeis' opinion at the time, his dissent, along with a later decision in *Katz v. United States* (1967), would shape the legal precedent underlying our modern understanding of privacy rights, which may be applied against ICE's practices.[14]

Katz v. United States (1967) established the reasonable expectation of privacy doctrine. In Katz, federal agents attached an eavesdropping device to a public telephone booth used by the defendant, suspecting him of sharing gambling information through phone calls. Based on the wiretap recordings, Katz was convicted of illegally transmitting wagering information across states. He appealed, arguing that the recordings should not have been admissible as evidence since they violated his Fourth Amendment right to privacy. The Supreme Court ultimately ruled that Katz was entitled to Fourth Amendment protection. Justice Potter Stewart wrote for the Court: "The Fourth Amendment protects people, not places."[15] This standard remains critical in assessing the legality of government surveillance today. The reasoning in *Katz* builds on earlier Fourth Amendment precedent set in decisions such as *Silverthorne Lumber Co. v. United States* (1920), where the court held that illegally seized evidence is "tainted" and that the government cannot benefit from information obtained in violation of the Constitution. This principle suggests that if ICE collects data illegally, the government should not be permitted to use it in immigration removal proceedings.

The right to privacy is further clarified in *Nardone v. United States* (1937), which precedes *Katz v. United States* (1967). In *Nardone*, federal agents tapped the defendant's telephone wires to intercept his calls, using this information as

[13] Laura Gardner, *To Be Let Alone: Brandeis Foresaw Privacy Problems*, BrandeisNOW (July 24, 2013), https://www.brandeis.edu/now/2013/july/privacy.htm

[14] Katz v. United States, 389 U.S. 347, 376 (1967).

[15] Katz v. United States, 389 U.S. 347, 376 (1967).

evidence to charge him with smuggling alcohol and possession of smuggled items. The Supreme Court ultimately ruled that evidence obtained through warrantless wiretaps is inadmissible in court under Section 605 of the Communications Act of 1934, which prohibits unauthorized interception and disclosure of communications.[16] This ruling affirmed two key principles that continue to influence current discussions on privacy rights under the Fourth Amendment. First, the government cannot use illegally obtained information in court; second, surveillance must be explicitly authorized by Congress to be admissible as evidence.[17] Therefore, if ICE gathers data in violation of privacy protections laid out in the Fourth Amendment, such data should not be used against the individual in deportation proceedings. Currently, no federal statute explicitly authorizes ICE to purchase extensive consumer data profiles, tax returns, sensitive medical information, conduct facial recognition scraping from social media, or monitor digital activity. Concerns regarding the constitutionality of ICE's actions stem from the fact that this data is acquired through private contracts rather than through legislatively sanctioned channels. This leaves ICE's extensive data-mining operations in a legally ambiguous position.

By relying on interagency data-sharing agreements and I-9 inspections, ICE circumvents traditional warrant requirements to gather personal information. If ICE conducts searches and collects personal information without a warrant, the absence of probable cause could render such collection unconstitutional. A notable example is the I-9 notice of inspection (NOI), which permits ICE to inspect I-9 documents in workplaces without a warrant.[18] These practices undermine both aspects of the Fourth Amendment test: they disregard individuals' subjective belief that

[16] Nardone v. United States, 302 U.S. 379, 387 (1937).
[17] Weeks v. United States, 232 U.S. 383, 399 (1914).
[18] U.S. Immigration & Customs Enforcement, *I-9 Inspection/Unauthorized Employment*, U.S. Department of Homeland Security. (March 16, 2026), https://www.ice.gov/factsheets/i9-inspection

their personal information remains private, and they challenge societal norms regarding reasonable expectations of privacy. When personal data is collected outside established warrant procedures rooted in the Fourth Amendment, information gathering may conflict with reasonable expectations of privacy and may therefore be unlawful.

ICE's Contracts

ICE's rapidly expanding surveillance capabilities are driven by an unprecedented network of contracts with private technology companies and federal agencies, such as the Centers for Medicare and Medicaid Services (CMS), the Children's Health Insurance Program (CHIP), Palantir, Clearview AI, LexisNexis, Paragon spyware, and Magnet Forensics. These agreements, which were effected privately, collectively grant ICE access to millions of U.S. citizens' most sensitive personal data. In November 2025, the CMS signed an "Information Exchange Agreement," providing ICE with login credentials to federal medical databases containing the records of more than 80 million people.[19] This agreement led to the sharing of their medical history, home addresses, phone numbers, IP addresses, and Social Security numbers.[20] The contract also required CMS to give ICE access to the Transformed Medicaid Statistical Information System (T-MSIS), the nationwide CHIP data system.[21] This agreement

[19] Centers for Medicaid and Medicare Service, *The Network for Public Health Law* (2025), Fact Sheet Centers for Medicare and Medicaid Services Announces Policy of Sharing Medicaid Data with Department of Homeland Security

[20] Leah Feiger et al., *ICE Is Getting Unprecedented Access to Medicaid Data,* WIRED (July 17, 2025), https://www.wired.com/story/ice-access-medicaid-data

[21] Centers for Medicaid and Medicare Services, *Children's Health Insurance Program (CHIP)*, CMS (2026), https://www.medicaid.gov/chip. CHIP is a federal and state funded health coverage program that "Provides health coverage to eligible children through both Medicaid and separate CHIP programs. Children eligible for CHIP are in families with incomes too high to qualify for Medicaid, but too low to afford private coverage."

granted ICE near-direct access to intimate information with minimal procedural safeguards. Simultaneously, ICE has expanded its partnerships with major surveillance and analytics firms to enhance its data analysis capabilities. In 2025, data analytics firm Palantir was awarded a $30 million contract to build the Immigration Lifecycle Operation System, a massive database designed to provide ICE with "near real-time visibility" into self-deportations, visa overstays, and enforcement targets. Facial recognition platform Clearview AI, whose system is notorious for scraping billions of images from private databases without consent, secured a $3.75 million contract in September 2025 to enhance ICE's biometric identification capabilities.[22] ICE has also entered into agreements with Paragon spyware, Magnet Forensics, and LexisNexis, each of which is slated to provide ICE with technology that will identify "suspicious activity"[23] and track migrants proactively, often before any alleged offense is committed. Paragon Spyware, a "sophisticated hacking tool," is capable of extracting data from mobile phones by accessing encrypted apps. This could provide the Department of Homeland Security (DHS) with access to private messages, app usage information, and call logs.[24] Magnet Forensics, a digital surveillance and cyber attack preventative tool, can extract data from both Android and IOS software, conduct

[22] Robert Hart, *Clearview AI—Controversial Facial Recognition Firm—Fined $33 Million for Illegal Database*, Forbes (Sept. 3, 2024), https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/. Notably, Clearview AI was founded with the investment of Palantir co-founder, Peter Thiel.

[23] Zack Whittaker, *Here's the Tech Powering ICE's Deportation Crackdown*, TechCrunch (Aug. 24, 2025), https://techcrunch.com/2025/08/24/heres-the-tech-powering-ices-deportation-crackdown/.

[24] Stephanie Kirchgaessner, *ICE Obtains Access to Israeli-Made Spyware That Can Hack Phones and Encrypted Apps*, Guardian (Sept. 2, 2025), https://www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware

media investigations, and provide data collection, sharing, and analyzing services, each of which can assist DHS in its data mining practices.[25] LexisNexis, a legal research platform, offers risk solutions for businesses and government agencies seeking analytics to support different legal topics, such as compliance or fraud detection.[26] This service could largely assist with the predictive nature ICE aims to achieve with the Immigration Lifecycle Operation System.

ICE justifies these contracts under statutory exceptions in the Privacy Act of 1974 and the Immigration and Nationality Act (1952).[27] The Privacy Act prohibits the government from sharing personal data. However, there are thirteen exceptions to this rule in Section 552A(b), one of which authorizes the release of personal records "for a civil or criminal law enforcement activity if the activity is authorized by law."[28] Because ICE aims to hasten its immigration enforcement by using gathered sensitive data, it can argue that its data mining practices are legal under this exception. Furthermore, Section 1360(b) of the INA states that "any information in any records kept by any department or agency of the Government as to the identity and location of aliens in the United States shall be made available to the Service upon request made by the Attorney General to the head of any

[25] Magnet Forensics, https://www.magnetforensics.com/ (last visited Apr. 21, 2026).
[26] LexisNexis, https://www.lexisnexis.com/en-us/gateway.page (last visited Apr. 21, 2026).
[27] Immigration and Nationality Act of 1952 § 287, 8 U.S.C. § 1357; Privacy Act of 1974, 5 U.S.C. § 552a (2018). The Privacy Act (1974) is a federal law that protects personal information held by the United States government (such as social security). It established guidelines on how federal agencies can collect and share personal information.
[28] Privacy Act of 1974, 5 U.S.C. § 552a(b) (2018); Nolan Rappaport, *ICE Data Mining Raises Privacy Concerns for Immigrants*, Hill (Aug. 24, 2025), https://thehill.com/opinion/immigration/5462199-ice-data-mining-privacy-immigrants/.

department or agency."[29] This provision could be leveraged by ICE to argue that their practices are necessary to keep track of the identity of undocumented immigrants.

Do these statutory provisions truly authorize ICE's aggressive enforcement practices and the development of surveillance tactics? And are the private agreements the agency has made with LexisNexis, Paragon Spyware, etc., considered legal under these statutes as well? The contracts' cumulative effect is the creation of an enormous, largely unregulated surveillance system that blurs the line between civil immigration enforcement and illegal mass data mining. The cumulative effect of these contracts is the creation of a vast, largely unregulated surveillance system that blurs the line between civil immigration enforcement and illegal mass data mining. Furthermore, this situation raises significant legal concerns about privacy, consent, and due process for the millions of legal American citizens whom ICE is surveilling. This raises a critical issue that both a plaintiff and DHS will need to address if this continues to be brought to the courts: Does ICE truly have authority under the "fine print" exceptions to the Privacy Act and the INA, or do the privacy rights protected by the Fourth Amendment, HIPAA, and other provisions take precedent?

The I-9 Inspection

The I-9 form was established under the Immigration Reform and Control Act of 1986 (IRCA),[30] and an amendment to the Immigration and Nationality Act (INA), which aimed to impose civil and criminal penalties on employers who knowingly hired unauthorized workers, such as undocumented immigrants. IRCA operates under the framework of the INA of 1952, which significantly restructured the U.S. immigration

[29] Immigration and Nationality Act § 290, 8 U.S.C. § 1360(b) (2018); Rappaport, *supra* note 30.
[30] Immigration Reform and Control Act of 1986, Pub.L.No. 99-603, 100 Stat.3359

system. The INA has been amended several times over the years and includes many key provisions related to immigration in the United States, including IRCA. Under IRCA, all employers that recruit for a fee or hire employees in the U.S. must complete I-9 verification to confirm their employees' identity and work authorization.[31] IRCA also granted ICE the authority to investigate an employer's I-9 forms by issuing a Notice of Inspection (NOI) when they have a suspicion of unauthorized employment. Some may request that an employer bring an I-9 Form to a USCIS field office, while others may arrange an inspection at the location where forms are stored. The risk in an ICE officer visiting a physical location is that they are in closer proximity to immigrant employees during the inspection, which can isolate an inspection more rapidly. It is important to note that an NOI is *not* a search warrant, but rather an administrative tool ICE can use if it suspects I-9 violations. ICE also does not clarify what circumstances trigger an I-9 inspection, which can leave employees and employers uncertain about the scope of enforcement, and can also leave the door open for unnecessary enforcement operations.[32] Today, however, I-9 inspections sit squarely within the larger erosion of privacy rights, because they are one of the many emerging ways ICE has begun to data mine. Undocumented immigrants comprise approximately 4.8% of the U.S. workforce, which illustrates the number of individuals who could be affected by intensified ICE operations that are supported by data mining tools.[33] Thus, what was originally designed as a process of

[31] U.S. Department of Labor, *I-9 Central*, https://www.dol.gov

[32] U.S. Citizenship and Immigration Services, *Inspections*, U.S. Department of Homeland Security (November 27, 2019), https://www.uscis.gov/i-9-central/legal-requirements-and-enforcement/inspections

[33] Jeffrey S. Passell and Jens Manuel Krogstad, *What We Know About Unauthorized Immigrants Living in the U.S.*, Pew Research Center (July 22, 2024), https://www.pewresearch.org/short-reads/2024/07/22/what-we-know-about-unauthorized-immigrants-living-in-the-us

inspecting employment verification forms has, in practice, become an entry point for ICE to initiate arrests, detentions, raids, and deportations.

In most states, employers are not obligated to inform their employees about an I-9 inspection. This lack of notification can put immigrant employees at risk, as they may face increased chances of arrest or detention by ICE if they do not have their status documents on hand, leading to both physical danger and emotional distress.[34] In Massachusetts, the frequency of I-9 inspections and the escalation of ICE's response have been increasing rapidly, in accordance with ICE Director Tom Holman's promise of "more workplace enforcement than you've ever seen before in the history of this nation."[35] In the past six months, heightened enforcement activity stemming from I-9 inspections has occurred at a Market Basket in New Bedford, a carwash in Allston, a business in Lowell, and at Harvard University.[36] During an I-9 inspection in Allston, nine employees were detained despite pleas to retrieve their immigration status documents, which

[34] Zoom Interview with Heather Yountz, Senior Immigration Attorney, Massachusetts Law Reform Institute December 12th, 2025.
[35] Massachusetts Law Reform Institute, Fact Sheet 11/12, Mass Legal Services (January 20, 2026)
[36]Abby Patkin, *Backlash Mounts After Boston University Student Claims Credit for Allston ICE Arrests*, Boston.com (Nov. 17, 2025), https://www.boston.com/news/local-news/2025/11/17/backlash-mounts-boston-university-student-claims-credit-allston-ice-arrests/; Trea Lavery, *Six of the Allston Car Wash Employees Arrested in Immigration Raid Released*, MassLive (Nov. 21, 2025), https://www.masslive.com/boston/2025/11/six-of-the-allston-car-wash-employees-arrested-in-immigration-raid-released.html; U.S. Immigration & Customs Enforcement, *ICE Arrests 11 "Illegal Aliens" During Lowell Worksite Enforcement Operation*, ICE Newsroom (May 19, 2025), https://www.ice.gov/news/releases/ice-arrests-11-illegal-aliens-during-lowell-worksite-enforcement-operation; Emily Piper-Vallillo, *Harvard Turns Over Employee Work Authorization Forms to Homeland Security*, WBUR (July 30, 2025), https://www.wbur.org/news/2025/07/30/harvard-turns-over-employee-work-authorization-forms-to-homeland-security

were rejected by ICE officials. This case exemplifies how I-9 inspections have evolved from simple, reputable employment verification into a targeted process that resembles modern-day witch hunts. The Allston employees attempted to comply with the requirements of an I-9 inspection by proving their status, but were barred from doing so by ICE, infringing on their due process rights. Reports show that the Allston case was prompted by a tip sent by a Boston University student; however, as ICE's Immigration Lifecycle Operation System grows more sophisticated and interconnected, tips could be rapidly integrated with the growing technology supporting ICE's enforcement efforts. In this context, it has become clear that the I-9 system has been repurposed from a labor compliance tool under IRCA to a tracking and surveillance practice.[37] This unconventional use of I-9 data means that immigrants' "expectations of privacy" in this regard are both objectively and subjectively "reasonable." Given that Massachusetts has taken a leading role in data privacy protection, particularly in the service sector, it has a heightened responsibility to protect residents' information.

The increasing frequency and intensity of I-9 inspections in Massachusetts are alarming and threaten the protections of the Data Privacy Act (2025) and privacy rights more generally. Passed unanimously in the House and Senate in September 2025, the Data Privacy Act makes "Massachusetts one of the states with the strongest privacy laws in the U.S."[38] It grants consumers specific rights, such as the right to know what data companies collect and the ability to opt out of having their data sold for targeted advertising. It also

[37] Abby Patkin, Backlash Mounts After Boston University Student Claims Credit for Allston ICE Arrests, Boston.com (Nov. 17, 2025), https://www.boston.com/news/local-news/2025/11/17/backlash-mounts-boston-university-student-claims-credit-allston-ice-arrests/

[38] Annie Jonas, *Massachusetts Senate Backs Data Privacy Bill Giving Consumers More Control of Their Data*, Boston.com (Oct. 9, 2025), https://www.boston.com/news/local-news/2025/10/09/senate-passes-data-privacy-bill

restricts the amount of data that companies collect by limiting this information to what is "reasonably necessary" to provide a product or service. Lastly, the law also banned the sale of any sensitive data, such as biometrics, health information, IP addresses, data from minors, and immigration status. By including the protection of immigration status, the Massachusetts legislature signals its intent to safeguard immigrant communities in the future from the data mining practices of DHS. As one of the first laws of its kind, Massachusetts must reaffirm its commitment to the privacy protections established by the Data Privacy Act. This commitment is crucial for upholding both employment protections and data privacy safeguards, ensuring that I-9 inspections do not infringe upon the rights guaranteed by the Data Privacy Act and the Fourth Amendment.

Call to Action

ICE's expanding use of data mining raises questions about the agency's statutory authority. My interview with Attorney Yountz shed light on the significant risks immigrants face daily, as well as steps they can take to protect their communities. While individuals have limited options for shielding themselves from current data-mining practices, because of their invisibility, they can prepare for direct interactions with ICE. It is crucial to understand your privacy rights at home, at work, and in public. If you are or know an undocumented immigrant, creating a care plan for their children or pets in the event of separation or deportation is essential. A caretaker affidavit is required for the caretaker to assume immediate custody, and granting the caretaker power of attorney is a critical component of family contingency planning. Meeting with an immigration attorney can also provide valuable guidance.

Additionally, immigrants should be aware of and inquire about the types of data public schools request from students, particularly concerning Social Security and

immigration status. Local data collection can become fuel for the large-scale data mining efforts that are building the Immigration Lifecycle Operation System. Attorney Yountz emphasized the importance of keeping their status documents with them at all times. Furthermore, she highlighted several community-based organizations that have supported immigrant communities in Massachusetts, including the LUCE Network, the Boston Immigration Justice Accompaniment Network (BIJAN), and the Massachusetts Immigrant and Refugee Advocacy Coalition (MIRA). Accessing these resources through "Know your rights" training, connecting with LUCE's ICE Watch hotline, and obtaining legal counsel are steps immigrants can take to further protect their due process rights amid an intensifying U.S. immigration landscape.

The protective measures individuals can take highlight the urgency of the moment, but they also underscore a larger truth: safeguarding immigrant communities requires collective advocacy and generational leadership. In an era where ICE increasingly relies on sophisticated data systems to track, surveil, and target immigrants, the work of activism against these practices becomes crucial for protecting vulnerable communities and challenging the mechanisms that enable harmful immigration enforcement. March for Our Lives youth leader Alfonso Calderon stated in 2018 that "every social movement in this country has had teenagers at the helm of it." [39] Much of the social change in the United States has relied on younger generations, as Jerusha O. Connor highlights in her book New Student Activists: *The Rise of Neoactivism on College Campuses* (2020), which features Calderon's activism. Attorney Yountz acknowledged this impact during our interview and shared several ways Gen Z can get involved in protecting our immigrant communities. These included attending the Massachusetts Immigrant and Refugee Advocacy

[39] Jerusha O. Connor, *The New Student Activists: The Rise of Neoactivism on College Campuses* (Johns Hopkins Univ. Press 2020).

Coalition (MIRA) "Know Your Rights" training [40] and signing up to present these sessions on college campuses. Supporting immigrant-serving groups through time or financial contributions, and creating a welcoming environment for immigrant communities on college campuses, are also vital. Lastly, she advised against posting about the issue on social media due to the privacy risks associated with ICE's data mining.[41] Each of these steps outlines ways younger generations can help ensure that the United States upholds the promise of the American Dream, including the rights to Privacy, Due Process, and opportunity.

Furthermore, states should continue to sue DHS under the guise of privacy rights laid out in the Fourth Amendment, and by the precedent set by landmark Supreme Court Cases in the 20th century. Congress should also take swift action to either reform an existing law or establish a new law that would offer a comprehensive definition of what personal information can and cannot be shared between interagency agreements, such as between CMS and ICE.

Conclusion

The expanding data mining agenda of Immigration and Customs Enforcement is eroding the traditional expectation of privacy that constitutional law has long protected. By consolidating medical, employment, biometric, and personal data into a single surveillance system, ICE is creating a mechanism that not only threatens the privacy of immigrants but also undermines due process, civil liberties, and public trust in institutions such as hospitals, employers, and government agencies tasked with protecting sensitive information. This evolving landscape raises urgent questions about the limits on

[40] Massachusetts Immigrant & Refugee Advocacy Coalition, *Know Your Rights*, MIRA (February 11, 2025), https://www.miracoalition.org/news/know-your-rights

[41] Zoom Interview with Heather Yountz, Senior Immigration Attorney, Massachusetts Law Reform Institute December 12th, 2025.

government access to personal data and who has the authority to define and enforce those limits. Addressing these questions is essential to ensuring that data collection and immigration enforcement uphold constitutional protections, respect human dignity, and maintain public confidence in America's legal and social institutions.