NOTES

SUPERPOWERS WITH VILLAINOUS OBJECTIVES: HOW THE EXECUTIVE BRANCH'S IMMIGRATION ENFORCEMENT "POWERS" UTILIZE TECHNOLOGY TO VIOLATE NONCITIZENS' PRIVACY

NINA-SIMONE EDWARDS*

ABSTRACT

The United States border, for noncitizens, has a unique quality to it. Each time a noncitizen crosses that border, they are no longer private individuals. They can no longer choose to give up their information–instead, there is a forced exchange: data for entry. Who they are, what they are, and everything that connects them to the world is given up in exchange for a new life in a new land. Once the border is crossed, noncitizens no longer have the privacy that they may have known before. This Note first builds on scholarship theorizing that noncitizens do have a right to privacy. Whenever anyone is forced to give up information about themselves, their privacy is violated, and noncitizens are no exception to this rule. Unfortunately, this right is often disrupted by one of three powerful branches of the United States government: the Executive Branch. The Executive Branch has statutory and constitutional immigration authority, as well as Executive Departments that influence immigration policy daily–all of which comprise what this Note calls "powers." While previous scholarship has focused on the President's immigration authority, this Note proposes that the Executive Branch uses its "powers" to not only impact immigration policy but also the individual privacy of

* Georgetown University Law Center, J.D. 2024; University of Tennessee at Chattanooga, B.S. 2019; Senior Communications and Technology Editor, *Georgetown Law Journal*, Volume 112; Managing Editor, *Georgetown Law Technology Review*, Volume 8. I'm so thankful for the *GILJ* team for providing necessary insights and edits for this Note. As always, I feel blessed that my thoughts are being published.

noncitizens. As technology continues to advance, the Executive Branch increasingly wields its "powers," in conjunction with different technological systems and databases, in ways that threaten the privacy of every noncitizen who dares to cross the border.

TABLE OF CONTENTS

INTRODUCTION 233

I. EXECUTIVE BRANCH POWERS 235
A. *The Many "Powers" of the Executive Branch* 235
B. *The Executive Branch "Powers" Often Utilize Technology In Pursuit of Its Objectives* 237
C. *The Legislative Branch's Limitations* 238

II. THE IDEA OF NONCITIZEN PRIVACY 240
A. *Legal Background and Understandings of Privacy* 241
B. *The Fourth Amendment and Noncitizen Privacy* 243

III. EXECUTIVE BRANCH POWER HAS BEEN USED TO VIOLATE NONCITIZEN PRIVACY 246
A. *National Security Entry-Exit Registration System (NSEERS)* 246
1. Overview of the Program 246
2. Discrimination 247
3. Data collection and misuse 248
B. *Deferred Action for Childhood Arrivals (DACA)* 250
1. Overview of the Policy 250
2. Data collection and misuse 251
3. Electronic Monitoring 252
4. Database Insecurity 253
C. *Recent Notice of Proposed Rulemaking* 255
1. Overview of the Rulemaking 255
2. Data collection and misuse 255

CONCLUSION 256

INTRODUCTION

"The government has easy access to our house, so it leaves me with, like, a sense of – it's frightening. I'm scared. Just thinking about it makes me, like, get the chills," Maria stated.[1] Maria, a Deferred Action for Childhood Arrivals (DACA) recipient, says that the "government already knows where she lives and where her parents live because she had to *supply that information to apply for DACA*."[2] She is frightened of what will happen now that the government has her data, and she is not alone in her fear. Another DACA recipient stated: "A few of my friends, one by one their parents are getting detained. And for, like, the rest of us, it feels like it's just a waiting game."[3] Many noncitizens are afraid of the unknown—what will happen to them after they gave up their information to pursue their dreams?

DACA is a program that allows undocumented individuals to gain deferred removal and is housed in the Executive Branch, the focus of this Note. Although immigration laws and policies are written and enforced by all three branches of government, and Congress plays a specific and important role in the immigration sphere, Congress does not work alone. Immigration laws today are enforced in tandem with the Executive Branch and the Judicial Branch. The Judicial Branch also has a necessary role of review, but this Note focuses on the Executive Branch because of its influence within the immigration sphere.

The Executive Branch arguably has as much power to change immigration laws and policies as the Legislative Branch. The Executive Branch enforces immigration laws through its agencies and administrative decisions, and includes the offices of the President and Vice President, as well as the Cabinet, Executive Departments, Independent Agencies, and other commissions, committees, and boards.[4] Executive agencies write federal regulations, and the President has the ability to declare executive orders, memoranda, and proclamations that are directives to the Executive Branch.[5] Thus, immigration law may change through a Presidential Executive Order; a Department of Homeland Security memorandum; or an agency's federal regulation.

These mechanisms are consistently used by the Executive Branch to violate the privacy of noncitizens like Maria. The thesis of this Note rests on two key ideas: the idea of Executive Branch "powers" and the violations of noncitizens' privacy. The Executive Branch "powers" that this Note refers to consist of all the different faculties that the Executive Branch has at its disposal. This includes the many different departments and agencies, as mentioned

---

1. Richard Gonzales, *Immigrants Fear Data Collected Under DACA Could Give Government Deportation Power*, NPR (Mar. 25, 2017, 5:56 PM), https://perma.cc/BW8JJXZ6.
2. *Id.* (emphasis added).
3. *Id.*
4. *See Branches of the United States*, USA.GOV, https://perma.cc/ZUB4-DCKY (last visited May 3, 2023).
5. *See Immigration and the Roles of the Three Branches of Government*, LEAGUE OF WOMEN VOTERS OF THE ST. PETERSBURG AREA (Oct. 2020), https://perma.cc/HK9X-8KVV.

above. These departments and agencies are only present within the Executive Branch, and many of them deal specifically with immigration. Anything that those departments or agencies do, including laws and regulations, is a "power", in the context of this Note, of the Executive Branch as a whole. Often, these "powers" work in conjunction with different forms of technology, which, especially in the immigration context, only amplifies the powers.

Further, Congress created statutory abilities, for entities within the Executive Branch, such as the parole power or the ability to defer action. It is any or all of these powers, this Note argues, that often work to violate noncitizens' privacy.

Although there are arguments for legitimate governmental interests in gathering data and information about those entering the country, this Note argues that each time a noncitizen is required to give up their data, their privacy is being violated, regardless of whether there are governmental interests at stake.

This Note will proceed as follows: part I will discuss the powers that the Executive Branch has in relation to immigration law, and how those powers interact with, impact, and violate the privacy of immigrants. Part II discusses the idea of the privacy of noncitizens.[6] While there are international understandings of privacy that could theoretically be applied, noncitizens are not necessarily granted any privacy within the United States. However, some Fourth Amendment protections and Privacy Act protections do apply: Fourth Amendment protections pertain to noncitizens' interactions with the United States Immigration and Customs Enforcement (ICE) agents, and the Privacy Act protections pertain to noncitizens' data being collected and stored by a government agency.

Most of the focus of this Note is the right to data privacy. Data privacy includes the proper handling of personally identifiable information, such as one's name or address. Part II explains how different definitions of privacy interact with noncitizens, and what rights they may potentially have. Data privacy is a right that is only protected by some states within the United States, but noncitizens do have some data privacy rights under the Privacy Act.

Part III focuses on three examples of the Executive Branch using its authority to violate immigrant privacy: the NSEERS program, the DACA program, and a 2020 Notice of Proposed Rulemaking. Each of the examples will explore how the Executive Branch violated noncitizens' privacy through their programs or proposals. Often, it was a side effect, but this still does not take away from the fact that noncitizens must give up their privacy in order to have the life they dream of in the United States. Additionally, as part III

6. For the purposes of this Note, the term noncitizen will be used to refer to anyone who is not an American citizen. The use of the term immigrant may be used (instead of noncitizen) based on certain sources using the term immigrant.

explores, the data that is collected may not be protected in storage. This is the fear of Maria and many other noncitizens: their data privacy may be compromised decades after the initial invasion of privacy from the collection of the data.

I. EXECUTIVE BRANCH POWERS

A. *The Many "Powers" of the Executive Branch*

The Executive Branch has a wide variety of powers that it may wield in the immigration sphere. This Note's reference to the Executive Branch's "powers" includes both the specific powers at its disposal, including "the parole power, the executive authority over foreign affairs, and Section 212(f) of the Immigration and National Act,"[7] the actual members of the branch, and any programs implemented. Thus, the capabilities of the Department of Homeland Security (DHS) are included as an Executive Branch "power" in that this department, and others, allows the Executive Branch to impact immigration law and therefore noncitizens.

The Executive Branch has the power to decide how to implement the law, set priorities, and allocate resources per their agenda. Some of this power is delegated to the Executive Branch by Congress. This broad delegated authority may be used to specify how immigration laws are implemented.

The Immigration and National Act (INA) is the statutory source of this delegated authority. The INA was enacted in 1952[8] and "changed the face of America"[9] by putting an end to immigration admissions policies based on race and ethnicity, and giving rise to large-scale, both authorized and unauthorized, immigration. INA §212(d)(5)(A) defines the parole power: the Secretary of Homeland Security may exercise discretion to temporarily allow certain noncitizens to physically enter the United States for a specific purpose if they are applying for admission and are not admissible or if they do not have a legal basis for admission.[10]

INA §212(f) gives the President extraordinary immigration powers, such that a former President deemed this section his "'magical authority' to restrict immigration."[11] Under this section, should the President find that the entry of "any aliens . . . into the United States . . . detrimental to the interests of the United States, he may by proclamation . . . suspend the entry of all aliens . . . or impose on the entry of aliens any restrictions he may deem to be

---

7. Michele Waslin, *The Use of Executive Orders and Proclamations to Create Immigration Policy: Trump in Historical Perspective*, 8 J. MIGRATION & HUM. SEC. 54, 56 (2020) (citing Adam B. Cox & Cristina M. Rodriguez, *The President and Immigration Law*, 119 Yale L. J. 458, 511 (2009)).

8. *See* 8 U.S.C. § 1101 (1952).

9. Muzaffar Chishti, Faye Hipsman & Isabel Ball, *Fifty Years On, the 1965 Immigration and Nationality Act Continues to Reshape the United States*, MIGRATION POL'Y INST. (Oct. 15, 2015), https://perma.cc/AA8B-7KWW.

10. 8 C.F.R. § 212.5 (1982).

11. *Discriminatory Bans and 212(f) Authority*, ACLU (Dec. 23,2020), https://perma.cc/2CFN-YWTN.

appropriate."[12] There is no definition of "detrimental" that is given to guide Presidents, nor any other guidelines regarding any proclamations, suspensions or restrictions.

INA §103 allows for deferred action, or the decision to defer the removal of individuals.[13] This is recognized by immigration statutes, regulations, and courts as an act of prosecutorial discretion.[14] The legal authority for this comes from the grant of authority that Congress gave the Department of Homeland Security to administer and enforce immigration laws.[15] Federal courts have acknowledged this executive power since the 1970s.[16]

Outside of statutory authority, the Executive Branch may also exercise its constitutional plenary power over foreign affairs. The U.S. Constitution grants the President the power to make treaties and the power to receive ambassadors from foreign sovereign States.[17] Furthermore, in a 1936 Supreme Court case, the Court found that "the President is the sole organ of the federal government in the field of international relations."[18] In 2015, the Supreme Court also recognized the President's power to grant formal recognition to a foreign sovereign.[19] These powers are displayed in, for example, deferred enforced departure, which has also been an authority recognized by federal courts.[20]

The President has also been known to use "powers expressly delegated to him by Congress to advance his own immigration agenda."[21] The President may use powers vested to him through the Constitution or in statutes in innovative ways, "accomplishing objectives Congress almost certainly did not intend and expanding or repurposing Congress's original design."[22]

With Congress writing the laws, and the judiciary reviewing decisions, the Executive Branch is poised to utilize its "magical authority"–or other authorities that are not as magical–to enforce immigration laws and policies. The Executive Branch powers work in tandem with the other branches yet are unique to the branch. No other branch can deem an "alien's" entry "detrimental" to the interests of the United States and thus change the trajectory of that person's life. Without any strict boundaries or definitions, the President can

---

12. 8 U.S.C. § 1182(f) (2013).
13. *See* 8 U.S.C. § 1103(a) (2009).
14. *See id.*
15. *See id.*
16. *See* NATIONAL IMMIGRATION LAW CENTER, THE PRESIDENT'S BROAD LEGAL AUTHORITY TO ACT ON IMMIGRATION (2014) [hereinafter NILC].
17. *See* U.S. CONST. art. 2, § 3, cl. 2.
18. *See* United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936).
19. *See* Zivotofsky v. Kerry, 135 S. Ct. 2076, 2094 (2015).
20. *See* Hotel and Restaurant Employees Union, Local 25 v. Smith, 846 F.2d 1499, 1510 (D.C. Cir. 1988) (en banc); American Baptist Churches in the U.S.A. v. Meese, 712 F. Supp. 756, 768 (N.D. Cal. 1989). Deferred enforced departure has been granted to people who are from countries where a natural disaster or domestic conflict has made it dangerous for people to return to their home state. *See* NILC, *supra* note 16.
21. Waslin, *supra* note 7 at 54, 56.
22. Adam Cox & Cristina Rodriguez, *The President and Immigration Law Redux*, 125 YALE L. J. 104, 116 (2015).

run amuck with this power. Being that many of the Executive Branch's powers and authorities are broad, they are in a unique position to significantly alter immigration laws and policies. In making these alterations, there are unprecedented privacy violations.

B. *The Executive Branch "Powers" Often Utilize Technology In Pursuit of Its Objectives*

The U.S. government has followed technological trends just as much as any other industry. As technology continues to advance, citizens and noncitizens alike expect to be able to interact with governmental agencies with the same ease that they interact with their favorite store or restaurant, which has compelled the government to keep up with technological advancements.[23] However, beyond general interactions, the advancement of technology has aided in the advancement of governmental programs and objectives. For example, the Federal Bureau of Investigation has collected biometrics since 1924.[24] The identification division began collecting fingerprints that year, and in 1999, an automated fingerprint identification system was created due to a growing demand for such automation.[25] Now, the government not only collects fingerprints to identify individuals, but also iris patterns and facial features.[26] Governmental agencies may also choose to use the multitude of surveillance cameras available, some of which have real-time facial recognition or license plate readers, to identify individuals.[27] Or they may instead comb through the already-collected data that is shared among different agencies. Technology, though a valuable resource, is only aiding the government's ability to watch and monitor everyone on American soil.

The Executive Branch fully takes advantage of the benefits of technology; while the Judicial Branch is beginning to incorporate more technology in the courtroom, the human judge is the final arbiter, and the Legislative Branch has yet to use artificial intelligence to conduct debates or votes. It is within the Executive Branch, however, where there is an increase in the use of technologies, particularly biometric-collecting technologies, that aid in achieving the goals of the Executive Branch. ICE recently signed a $7.2 million dollar contract with a private company to build technology to collect biometric data

---

23. *See* Tod Newcombe, *Government Technology's Complicated History*, GOVERNING (Sept. 27, 2017), https://perma.cc/89ZP-HUKV.

24. "A biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition." *Biometrics*, DEPT. HOMELAND SEC., https://perma.cc/MZ7C-P255 (last visited Feb. 2, 2024); *See CJIS Division Observes Milestone*, FBI NEWS, https://perma.cc/8XNR-6W9S (last visited Feb. 2, 2024).

25. *See Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability*, FED. BUREAU INVESTIGATION, https://perma.cc/596R-RXAX (last visited Feb. 12, 2024).

26. *See Biometrics*, *supra* note 24.

27. *See Street-Level Surveillance*, EFF, https://perma.cc/4PX5-4HBE (last visited Feb. 2, 2024).

from, and increase location tracking of, noncitizens.[28] Yet, even without any new technology, data sharing occurs within the different departments of the Executive Branch and exacerbates fears of deportation.[29] DHS has a national network of fusion centers that enables data sharing between local, state, tribal, and federal agencies.[30]

The Executive Branch "powers" may utilize technology to further any immigration law objectives. Some of the objectives the government proffers, which are discussed in this Note–national security efforts, or identification of every individual who crosses a border–are amplified by technology.[31] Unfortunately, this means that noncitizens and their privacy are violated.

C. *The Legislative Branch's Limitations*

There are many reasons why this Note posits that the Executive Branch is particularly poised to violate noncitizens' privacy, instead of Congress. One reason is that it is often difficult for Congress to pass comprehensive immigration reform due to the values and beliefs of their constituencies. "House Republicans . . . represent constituencies haunted by anxiety associated with the perception that they're 'losing their country' to immigrants from south of the border."[32] While Congress maintains power and responsibility for a large portion of immigration reform,[33] the positions are elected. The House and the Senate are held accountable by their constituencies, so they are less likely to move forward with attempting to pass a large program like DACA, for example.

Further, the extended timeline for action by the Legislative Branch has made the Executive Branch comparatively powerful in the immigration sphere. A bill must pass both the House and the Senate before it is presented before the President. The bill must be introduced, there are committee

---

28. *See* Caroline Haskins, *ICE spends $7.2 million to increase facial recognition and location tracking of migrants*, BUSINESS INSIDER (May 2, 2022, 5 AM), https://perma.cc/DH5E-8VGB.

29. *See* Gonzales, *supra* note 1; Joshua Rodriguez, *How Does Information Sharing Between DHS and Other Non-Enforcement Agencies Work?*, BIPARTISAN POL'Y CTR. (Apr. 17, 2018), https://perma.cc/8SAB-4UA7; Jen Fifield, *Cities, states try to protect immigrants' data from federal officials*, PBS NEWSHOUR (Apr. 20, 2017, 11:56 AM), https://perma.cc/48NS-QWN6.

30. *See* Dia Kayyali, *Why Fusion Centers Matter: FAQ*, EFF (Apr. 7, 2014), https://perma.cc/2XSV-PVWX.

31. *See* OBIM, *infra* note 45.

32. Christopher Parker, *The (Real) Reason Why the House Won't Pass Comprehensive Immigration Reform*, BROOKINGS (Aug. 4, 2014), https://perma.cc/QF9A-JHRM.

33. The Supreme Court, in 1875, declared regulation of immigration a federal responsibility so Congress began to pass more immigration legislation. *See* Chy Lung v. Freeman, 92 U.S. 275 (1875). The Supreme Court decided unanimously in favor of Chy Lung. Its primary argument was that the federal government, rather than that of the States, oversaw immigration policy and diplomatic relations with other nations. *See id*. That Supreme Court case illuminated the specific and important role that Congress must play in the immigration sphere. The Immigration and Nationality Act, which is the main law governing immigration in the United States, came from Congress. Further, the Constitution delegates to Congress the power "[t]o establish an uniform Rule of Naturalization . . . throughout the United States." U.S. CONST. art. 1, § 8, cl. 4. Thus, the Constitution gives Congress the power to determine who can become a citizen and under which conditions.

meetings, markup sessions, reports that must be written, debates, and then voting before it even hits the President's desk. None of this process happens very quickly, outside of emergency situations.[34] Additionally, immigration issues are often difficult to reconcile, for both the House and the Senate, which only exacerbates the amount of time the bill spends in the initial stages of debate and discussion. An example of this is illustrated by House Republicans drafting the Border Protection, Antiterrorism, and Illegal Immigration Control Act of 2005. This bill included harsher penalties for illegal immigration—classifying anyone who entered the United States unauthorized, as a felon. The bill also included a provision to build a fence along the U.S.-Mexico border. This bill only passed the House.[35] The following year, the Senate passed the Comprehensive Reform Act of 2006, which included a path to legal status, some border and interior enforcement, and English as the national language which would mean that individuals would not have a legal entitlement to services in other languages. Both bills were attempts at comprehensive immigration reform, but they were not able to be reconciled.[36] At that time, the House (in 2005) and the Senate (in 2006) wanted different things and were unable to come to an agreement.

Unfortunately, these differences are often rooted in ideological and political differences. In 2005, the Republicans maintained control of the House.[37] In 2006, the Democrats gained control of the Senate.[38] Democrats and Republicans have different immigration priorities: Republicans emphasize border security and removing any undocumented noncitizens, while Democrats emphasize paths to legal status.[39] This goes beyond the aforementioned constituency fears: these varying interests are seen in the different bills that are introduced and debated on, often during periods when one party gains control over another. The two parties have a hard time reconciling those differences, and it is even more difficult when the opposing party has control over the House or the Senate.

This struggle for reconciliation is demonstrated by a 2021 bill that would have brought DACA to life through federal legislation: the American DREAM and Promise Act of 2021. This bill would have allowed migrants physically present in the United States continuously since January 1, 2021 to

---

34. The Emergency Economic Stabilization Act of 2008 was originally rejected by the House of Representatives on September 29, 2009. The revised version was sent to Senate and the Senate passed it on October 1, the House signed off on it on October 3, and President Bush signed it 3 hours later. Emergency Economic Stabilization Act of 2008, 12 U.S.C. §1201 (2008). *See also* Andrew Glass, *Bush signs bank bailout, Oct. 3, 2008*, POLITICO (Oct. 3, 2013, 5:10 AM), https://perma.cc/M2J2-MHBK.

35. *See* H.R. 4437, 109th Cong. (2005).

36. *See* Suzanne Gamboa, *Congress has failed for more than two decades to reform immigration—here's a timeline*, NBC NEWS (Jan. 7, 2023, 6:00 AM), https://perma.cc/287Z-9BAZ.

37. *See Congress Profiles*, HISTORY, ART & ARCHIVES, https://perma.cc/6YW7-3NQG (last visited Jan. 27, 2024).

38. *See* John M. Broder, *Democrats Gain Senate and New Influence*, N.Y. TIMES (Nov. 10, 2006), https://perma.cc/GD75-K5JB.

39. *See* Nolan Rappaport, *Crafting an immigration bill that could pass Congress*, THE HILL (Nov. 8, 2022, 11:30 AM), https://perma.cc/U4HM-G7U6.

gain legal status.[40] About 2.7 million undocumented migrants would have been able to meet this requirement.[41] This bill was not particularly attractive to Republicans, though, which resulted in it not becoming law. It possibly could have been more attractive, if the bill was limited to include only those who were brought here as children with no knowledge of another country.[42] Even if that was not an option, comprehensive immigration reform could have passed from January 2009 to January 2011 without the need for a single Republican vote because the Democrats held the majority of the House and had enough votes to stop a filibuster in the Senate.[43] Whether these arguments have merit is beyond the scope of this Note; however, there are many variables that must be debated and discussed before a bill becomes law. On the other hand, when the Executive Branch wanted something like DACA, they did not have to wait for a vote to pass through 535 members of Congress, or wade through heavy political waters—the President was able to write an Executive Order that immediately set the program in motion.

II. THE IDEA OF NONCITIZEN PRIVACY

This Note argues that when noncitizens give up data, their privacy has been violated. Each time a person is forced to give up details about their life, that is considered a privacy violation—violating the "right to be let alone," a concept introduced by legal scholars, Louis Brandeis, and Samuel Warren.[44] Noncitizens, when forced to give up their DNA, fingerprint, or their birthday, are not fully allowed to be let alone. It is a distinct invasion, though, because their privacy must be violated in order to be granted entry into the country. Sometimes, their privacy is continually violated as a condition of that entry (through continual access to the data that is stored, for example). This is a particular privacy violation that is unique to noncitizens.

There may be legitimate governmental interests in wanting to gather that information. For national security purposes, gathering identifying information is important.[45] However, this governmental interest alone does not automatically override the right to privacy. There are often balancing tests, for example in the Fourth Amendment context, where the government must balance their interests against the intrusion on someone's privacy.[46] If the governmental interest outweighs the level of intrusion, then the government may

40. *See id.*
41. *See id.*
42. *See id.*
43. *See id.*
44. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).
45. OBIM states that they need to collect biometric information to "enable national security and public safety decision making." *See Office of Biometric Identity Management*, DEPT. HOMELAND SEC., https://perma.cc/869P-U9DU (last visited Feb. 6, 2024) [hereinafter OBIM].
46. An example of a balancing test involving governmental interests can be found in *Skinner v. Railway Labor Executives Association* where it was found that the governmental interest was furthered by the search and would be placed in jeopardy without the search. *See* 489 U.S. 602, 624 (1989).

conduct that search or seizure.[47] This does not, however, mean that the privacy of that individual does not exist—it simply means that it was outweighed.[48] Thus, even though there may be governmental interests at stake, this does not automatically mean that noncitizens do not have a right to privacy.

For example, should someone have to undergo a border search, the government may cite public safety as the reason for the search.[49] This does not mean that the person being searched does not have a right to privacy–only that it was outweighed by the governmental interest. The right to privacy always exists, but it is weighed against governmental interest or suspicion; when it is outweighed, a search or seizure may occur.[50] Section B of this part discusses the Fourth Amendment in full, but it is important to first emphasize that the Fourth Amendment only protects against *unreasonable* searches and seizures so if there is a particularly "weighty" governmental interest, the search or seizure could be considered reasonable and would outweigh the right to privacy that a person possesses.

A. *Legal Background and Understandings of Privacy*

The right to privacy is defined as the right to personal autonomy.[51] Additionally, ideas of dignity and control are entrenched in privacy definitions.[52] Louis Brandeis and Samuel Warren, as mentioned, were the first legal scholars to conceptualize the idea of privacy within the law in a law review article published in 1890.[53] From that article came the idea of "the right to be let alone."[54] This right has conceptually guided many discussions regarding privacy, as well as the creation of privacy torts. Definitions of privacy alone, however, do not lend themselves to legal authority.

The U.S. Constitution does not explicitly afford a right to privacy to American citizens; however, the Fourth Amendment is an avenue to allege privacy violations from the government.[55] There are also specific laws that many use to allege privacy violations. There are four privacy torts that allow

---

47. *See id.*

48. In *Camara v. Municipal Court*, the Court discusses the fact that the right to privacy yields to the right of a search if a judicial officer decides that the search is reasonable and grants a warrant. Thus, the right to privacy does still exist outside of the right to search, and an analysis must occur to decide whether it was reasonable for the search to occur. *See* Camara v. Mun. Ct. of City & Cnty. Of San Francisco, 387 U.S. 523, 529 (1967).

49. *See generally Border Searches,* LEGAL INFORMATION INST., https://perma.cc/3T8T-KAET (last visited Feb. 6, 2024).

50. *See* II.B for a more thorough explanation of the Fourth Amendment, searches, and seizures.

51. *See, e.g. Right to privacy*, Black's Law Dictionary (10th ed. 2014).

52. *See, e.g. id*; *see also* Anil Kalhan, *The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement*, 41 U.C. DAVIS L. REV. 1137, 1174 (2008); Sadiq Reza, *Privacy and the Post-September 11 Immigration Detainees: The Wrong Way to a Right (and Other Wrongs)*, 34 CONN. L. REV. 1169, 1171 (2002).

53. *See* Warren & Brandeis, *supra* note 44.

54. *Id.*

55. U.S. CONST. amend IV.

for civil suits: intrusion on seclusion, disclosure of private facts, false light, and appropriation.[56]

For purposes of particularity, it is important to note that noncitizens are not included in much of the privacy law discussion. Definitions of privacy and Constitutional safeguards from the government do not easily extend to noncitizens because they were written for American citizens. There are, however, international treaties and covenants that the United States has ratified that pertain to privacy.[57] Unfortunately, this ratification does not mean that noncitizens are free from interferences.

For the purposes of this Note, definitions of privacy relating broadly to the right to be let alone and dignity will be used, as well as any privacy afforded because of the Fourth Amendment. Further, extending some of the definitions from some international treaties that the United States has ratified: all noncitizens are humans and thus deserve the right to privacy.[58]

More specific than the general right to privacy is the right to data privacy, affording protection to noncitizens' data. Data privacy is defined as the proper collection, use, and dissemination of personally identifiable information (while maintaining and enforcing data-sharing norms and expectations).[59] Personally identifiable information is "any 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."[60] In the United States, there are, as of this writing, currently only nine states that have enacted comprehensive data privacy laws[61] which protect personally identifiable information,[62] and an upcoming comprehensive federal law that could do the same. [63] However, noncitizens are not easily afforded the protections of the current state laws and potential federal law.[64] If noncitizens are

---

56. *See Invasion of Privacy*, LEGAL INFORMATION INST., https://perma.cc/XV9R-T5J5 (last visited Feb. 6, 2024).

57. For example, in 1992, the International Covenant on Civil and Political Rights (ICCPR) was ratified by the United States. This human rights treaty guarantees privacy rights. In Article 17, everyone is protected from unlawful interferences to their "privacy, family, home or correspondences." International Covenant on Civil and Political Rights (ICCPR), Dec. 16. 1996, 999 U.N.T.S. 171; *Human Rights and Privacy*, ACLU, https://perma.cc/YB6S-YW3W (last visited Feb. 29, 2024).

58. *See id.*

59. *See* DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION-CRS REPORTS, CONGRESSIONAL RESEARCH SERVICE 1 (2022); Edward J. Janger, *Locating the Regulation of Data Privacy and Data Security*, 5 BROOK. J. CORP. FIN. & COM. L. 97, 99 (2010); s*ee also What does privacy mean?,* IAPP, https://perma.cc/7WBJ-RHD5 (last visited Feb. 6, 2024).

60. *Guidance on the Protection of Personally Identifiable Information*, U.S. DEPT. LABOR, https://perma.cc/6Z67-QRVR (last visited Feb. 12, 2024). This can include voiceprints, photographs, fingerprints, financial information, biographical information, and anything else that may be used to identify someone.

61. *See* Anokhy Desai, *US State Privacy Legislation Tracker*, IAPP (May 26, 2023), https://perma.cc/PQ8V-WQPN.

62. *See* sources cited, *supra* notes 59, 60.

63. *See* Joseph Duball, *US House lawmakers keep federal privacy legislation top of mind*, IAPP (Mar. 1, 2023), https://perma.cc/52CT-Y55Q.

64. For example, only California residents have rights under the CCPA. *See California Consumer Privacy Act*, STATE CA DEPT. JUST., https://perma.cc/T9VT-6V2K (last visited Feb. 11, 2024). Thus, a

not afforded the right to be let alone, their personally identifiable data may not be afforded any protections either. Further, the Executive Branch's violations of privacy do not stop with the individual, physical violations. The Executive Branch uses technology in ways that do not protect or handle noncitizens' data correctly, which extends the privacy violations for years beyond the one instance that the Executive Branch program or policy was unnecessarily invasive.[65]

This Note argues that the Privacy Act should afford immigrants some level of data privacy. The Privacy Act of 1974 safeguards privacy by creating procedural and substantive rights in personal data held by governmental agencies.[66] The Act protects personally identifiable information and allows individuals the right to seek access to, or request correction of, any records that are maintained about them. The Privacy Act requires records to be described in the System of Records Notices and binds federal agencies and all records under the control of federal agencies. This Act also prohibits the "disclosure [. . .] of such records without the prior, written consent of the individual(s) to whom the records pertain, unless one of the twelve disclosure exceptions enumerated in subsection (b) of the Act applies."[67] The exceptions of disclosure are broad enough that most governmental data transfers, such as to ICE, are able to fly under the radar and are not violative of the Privacy Act.[68]

One may not be aware that their information has been disclosed to ICE. Even if they knew and they wanted to pursue a civil action, they must fully exhaust administrative remedies first[69] (meaning that a noncitizen would have to make a request to DHS. There may be fear of repercussions or a general lack of resources or knowledge to exhaust administrative remedies). Thus, there are unlikely to be any civil remedies.

B. *The Fourth Amendment and Noncitizen Privacy*

The Fourth Amendment protects people from "unreasonable searches and seizures by the government."[70] This is not a guarantee against all searches and seizures, however, only those deemed "unreasonable." Officers are

---

noncitizen would have to prove that they are a California citizen. Although not impossible (if they have a driver's license or some other form of ID, they would have already had to prove their residency/domicile requirements), they are not immediately included under this law in a way that an American citizen would be—especially if the noncitizen is not a lawful permanent resident.

65. *See* the discussion of DACA in Part III.

66. *See* The Privacy Act of 1974, 5 U.S.C. § 552(a); *see also The Privacy Act of 1974*, EPIC, https://perma.cc/HLQ6-4BH7 (last visited Feb. 11, 2024).

67. *The Privacy Act*, U.S. DEPT. HEALTH HUM. SERVICES, https://perma.cc/HEQ9-6RZ4 (last visited Feb. 11, 2024).

68. They could say that, for example, it is a "routine use." The Privacy Act of 1974, 5 U.S.C. § 552 (a)(7).

69. *See id.* at § 552a(g)(1)(A); s*ee also Overview of the Privacy Act: 2020 Edition,* OFF. PRIVACY & C.L., https://perma.cc/T5W3-8AGL (last visited Feb. 11, 2024).

70. U.S. CONST. amend. IV.; *see also What does the Fourth Amendment mean*?, U.S. COURTS, https://perma.cc/7R66-BB87 (last visited Feb. 11, 2024).

allowed to conduct investigatory stops based on reasonable suspicion that criminal activity is afoot.[71] Searches incident to an arrest are also permissible, as well as border searches, and consensual searches. When analyzing the unreasonableness of a search or seizure, judges will consider a variety of factors, some of which are applicable to immigrants.

ICE, an agency of DHS, is the organization primarily responsible for immigration enforcement in the United States. ICE has the "authority to arrest and detain non-United States nationals ("aliens," as the term is used in federal law) identified for removal because of immigration violations."[72] ICE is also authorized to conduct interrogations and brief detentions to investigate possible immigration violations. Exercise of this authority—INA §287(a)(1) provides that an immigration officer may "interrogate any alien . . . as to his right to be or to remain in the United States" without a warrant—is subject to Fourth Amendment constraints.[73]

Law enforcement officers do not violate the Fourth Amendment when questioning noncitizens in public places. In *INS v. Delgado*, the Court held that officers were not in violation of the Fourth Amendment when entering factory buildings, which were considered public places due to a warrant or the employer's consent.[74] In that case, the questioning was brief, and it did not prevent employees from doing their jobs.

Longer, more intrusive encounters are only justified if there is reasonable suspicion that criminal activity is afoot. This requires specific facts, instead of a hunch, that would reasonably warrant suspicion. In cases like *INS v. Delgado* where there is no requirement of reasonable suspicion because the employees were not detained, it is important to differentiate between brief encounters with the police, and a brief detention.[75] While this analysis cannot begin without specific facts of a particular case, the difference lies in being asked a few questions versus being stopped, detained, and potentially searched.[76] As it pertains to longer, intrusive searches at the border, in *United States v. Brignoni-Ponce*, the Supreme Court held that random car stops near the border requires reasonable suspicion that the car's occupants are noncitizens who may be unlawfully within the United States.[77]

Reasonable suspicion is not required for searches, however, if the governmental interest outweighs the privacy intrusion: a search can occur without a warrant.[78] The governmental interest may thus fall under one of the

71. *See* Terry v. Ohio, 392 U.S. 1, 30 (1968).
72. HILLEL R. SMITH, IMMIGRATION ARRESTS IN THE INTERIOR OF THE UNITED STATES 1 (2021).
73. *Id*. at 4.
74. *See* INS v. Delgado, 466 U.S. 210 (1984).
75. *See id*.; SMITH, *supra* note 72.
76. Sometimes, it can be hard to tell the difference which only makes the analysis even more important. Going through the specific facts of the case can point in the direction of either an intrusive encounter or a brief search.
77. United States v. Brignoni-Ponce, 422 U.S. 873 (1975).
78. *See Warrantless*, LEGAL INFORMATION INST., https://perma.cc/6G62-M9ZL (last visited Feb. 2, 2024).

exceptions to the warrant requirement. This is seen in border searches, which are generally considered reasonable, "pursuant to the long-standing right of the sovereign to protect itself."[79] A search in the immigration context could also meet the special needs exception, because a search that serves a special government need, that is beyond the normal needs of law enforcement, is considered reasonable.[80]

DHS regulations have provided guidance for immigration law enforcement that reflects the Fourth Amendment constraints. An immigration officer may question someone if the officer "does not restrain the freedom of an individual, not under arrest, to walk away."[81] A noncitizen may be briefly detained for questioning only if there is reasonable suspicion that this person is "engaged in an offense against the United States or is an alien illegally in the United States."[82] Any information obtained from this questioning can be used to provide a basis for any subsequent arrests.[83] Therefore, noncitizens are afforded some Fourth Amendment protections. However, these protections do nothing against many of the governmental programs that violate noncitizens' privacy. It may even be argued that these programs violate the Fourth Amendment—if the Fourth Amendment were easily applied to the immigration sphere. Noncitizens and their data are treated differently than American citizens and their data. The government is allowed to conduct searches or seizures, and violate noncitizens' privacy, pursuant to their governmental interests (which meets a warrant exception), which can include the purported safety or security of American citizens.[84]

The ideas of privacy discussed in this section will be applied to the Executive Branch programs and policies discussed in part III. These programs display different ways that the Executive Branch has, or is trying to, violate the privacy of noncitizens. However, the programs discussed do not form an exhaustive list. Rather, they were chosen because they are not always specifically discussed in the privacy law sphere, and never as it pertains to the Executive Branch violations in particular.

---

79. United States v. Ramsey, 431 U.S. 606, 616 (1977); *see also* Anil Kalhan, *The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement*, 41 U.C. DAVIS L. REV. 1137, 1189, 1197 (2008).

80. *See Border Searches,* JUSTIA, https://perma.cc/R7TK-66NJ (last visited Feb. 2, 2024); *see also Skinner, supra* note 46 (where the governmental interest outweighed the privacy interests of employees, and suspicion-less drug and alcohol tests were allowed).

81. 8 C.F.R. § 287.8 (2016).

82. *Id*. at § 287.8(b).

83. *See id.*

84. As discussed, if the governmental interest outweighs the level of intrusion, then the government may conduct that search or seizure. Governmental interests, such as national security and public safety, are generally cited as the reason for data collection. *See* OBIM, *supra* note 45. Thus, they are allowed to conduct searches and seizures to collect that data. This data collection, as discussed *infra* in Part III, may violate noncitizens' privacy.

III. EXECUTIVE BRANCH POWER HAS BEEN USED TO VIOLATE NONCITIZEN PRIVACY

A. *National Security Entry-Exit Registration System (NSEERS)*

1. *Overview of the Program*

The National Security Entry-Exit Registration System (NSEERS) is one example of an Executive Branch program that violates noncitizen privacy. The program was initiated under the Department of Justice (DOJ) in 2002, but was later inherited by DHS, both Executive Branch departments. The framework of the NSEERS program is linked to §110 of the United States Illegal Immigration Reform and Immigration Responsibility Act (IIRAIRA) of 1996 which mandated an automated entry-exit data system.[85] This technology-based data system is meant to collect records of every "alien departing the United States and match the records of departure with the record of the alien's arrival in the United States."[86]

NSEERS was implemented in 2002 after the September 11, 2001 terrorist attacks to address national security concerns. The program required all noncitizen men and boys from specific countries[87] to register through the NSEERS program. NSEERS was designed to record the arrival, stay, and departure of those who were from specific countries designated by the program to be possible national security threats.[88] The NSEERS registration added an additional inspection, lasting about 30 minutes, each time a person arrived.[89] There were also designated ports of departure, ultimately limiting the travel flexibility of those from countries on the NSEERS country list because individuals had to register at one of those ports upon departure.[90]

After the creation of this program, DHS implemented automated systems that captured both arrival and departure information.[91] These systems also captured information for other visitors, regardless of nationality.[92]

In May 2011, DHS announced that it would remove the list of countries from the NSEERS program.[93] This effectively ended the NSEERS registration process, according to DHS.[94] However, the regulatory structure of

85. Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRAIRA), Pub. L. No. 104-208, 110.a.1 Stat. 3009. 46.

86. *Id.*

87. Afghanistan, Algeria, Bahrain, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, North Korea, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen.

88. *See DHS Removes Designated Countries From NSEERS Registration (May 2011)*, DEPT. HOMELAND SEC., https://perma.cc/6PGR-YKKC [hereinafter DHS REGISTRATION REMOVAL].

89. *See id.*

90. *See id.*

91. *See id.*

92. *See id.*

93. *See* Removing Designated Countries From the National Security Entry-Exit Registration System (NSEERS), 76 Fed. Reg. 23830 (Apr. 28, 2011).

94. *See* DHS REGISTRATION REMOVAL, *supra* note 88.

NSEERS remained in place until 2016.[95] Until then, individuals continued to be subjected to the consequences of this program, including deportation or the "denial of immigration benefits" for which they may have been eligible otherwise.[96]

2. *Discrimination*

NSEERS targeted foreign nationals from twenty-five countries based on religion, ethnicity, and national origin. NSEERS was a program that relied on discriminatory profiling of foreign nationals from countries with predominantly Muslim populations (other than North Korea). The false assumption that guided this program was that Muslims or those of a particular nationality were more likely to be terrorists or be involved in terrorism-related crimes.[97] People from the Middle East, Arabs, Muslims, and South Asians from the designated countries were subjected to enhanced scrutiny. DHS stated that they did not profile based on religion because every male from the designated country list was required to register regardless of their religious affiliation.[98] However, other sources have stated that, due to the disproportionate impact this program had on Muslims, there was a religious profile.[99]

NSEERS was expanded multiple times and specified different requirements during each expansion, or registration component. During the port of entry registration component, NSEERS required individuals to register at all ports of entry. Every arriving male from the designated countries would have their fingerprints tested against a database of "known terrorists."[100] The program then expanded and required certain male foreign visitors over sixteen years of age from designated countries and already present within the United States to register at specific immigration offices. During this registration component, there were groups of countries designated, and noncitizens from those countries had to register during a particular period.[101] This component

---

95. *See National Security Entry-Exit Registration System*, ACLU, https://perma.cc/YKW4-A822 (last visited Feb. 1, 2024).

96. RIGHTS WORKING GROUP & CENTER FOR IMMIGRANTS' RIGHTS, THE NSEERS EFFECT: A DECADE OF RACIAL PROFILING, FEAR, AND SECRECY 5 (2012) [hereinafter RWG].

97. *See id*. at 4.

98. *See id*. at 4. According to DHS, there was also no profiling because the countries were targeted due to their affiliation with terrorist organizations, and it was also not an exclusive list: "all non-immigrant visitors from other countries eventually will be included as the US-VISIT program is implemented." FACT SHEET: CHANGES TO NATIONAL SECURITY ENTRY/EXIT SYSTEM (NSEERS), DHS 3 (2003).

99. *See id*. at 11.

100. John Ashcroft, Attorney General, Prepared Remarks on the National Security Entry-Exit Registration System (June 6, 2002).

101. "The registration requirement was first applied to nonimmigrant males from Iran, Iraq, Libya, Sudan, and Syria. These individuals were required to register with INS between November 15, 2002, and December 16, 2002. The second group required to register were from Afghanistan, Algeria, Bahrain, Eritrea, Lebanon, Morocco, North Korea, Oman, Qatar, Somalia, Tunisia, United Arab Emirates, and Yemen. Their registration occurred between December 2, 2002, and January 10, 2003. The third group included individuals from Pakistan and Saudi Arabia who were to register between January 13, 2003, and March 21, 2003. The last group of visitors required to register were from Bangladesh, Egypt, Indonesia, and Kuwait and were to register between February 24, 2003, and April 25, 2003." *See* RWG, *supra* note 96, at 15.

of NSEERS was criticized due to the requirements essentially profiling males of a certain age, from predominantly Muslim countries–thus, there was profiling based on gender, age, religion, and nationality.

The program also expanded again and required each NSEERS registrant to register each time they departed from the United States. Each component of the program was seen to target individuals: Denyse Sabagh, an immigration attorney, observed,

> "the Muslim communities felt very much under siege. It seemed that the legal standard changed and they were guilty until they were proven innocent. They were placed in a state of constant anxiety and fear. NSEERS sure looked like racial profiling. It targeted individuals based on nationality, age, gender, and religion. If the government wanted to create an effective counterterrorism tool, it could have developed a list of criteria that would be related to the actual focus of identifying terrorists, rather than profiling against whole classes of people based on their nationality."[102]

It is this discrimination that led to certain noncitizens' data being collected and potentially misused. While discrimination can occur due to a penumbra of circumstances, this program discriminated and chose whose privacy they wanted to violate. This regulation relied on that discrimination to collect data from certain male foreign visitors over sixteen years of age. Therefore, without this discrimination, those individuals (that the program discriminated against) would not have had their data collected or their privacy violated.

3. *Data collection and misuse*

More than 80,000 men responded to the NSEERS registration component that required them to register at a designated location.[103] DHS subjected thousands of others to fingerprinting, photographs, lengthy and invasive interrogations (that included gathering information about their background, financial situations, and biographical information), and detention through this program.[104] Although it is now "dormant,"[105] the residual effects of the program and its data collection (as well as misuse of that data) should be addressed and rectified.

The data that was collected through this program was consistently used in other governmental programs: Operation Frontline is one program that used the data from NSEERS. Operation Frontline was started in 2004 to prevent terrorist attacks during the presidential election season.[106] The program

---

102. *See* RWG, *supra* note 96, at 13.
103. *See id.*, at 4.
104. *See id.*
105. Press Release, DRUM, DRUM Welcomes Victory in Ending NSEERS and Calls for Accountability for Thousands (Apr. 28, 2011) https://perma.cc/9JX4-DXV6.
106. *See* CENTER FOR HUMAN RIGHTS & GLOBAL JUSTICE, UNDER THE RADAR: MUSLIMS DEPORTED, DETAINED, AND DENIED ON UNSUBSTANTIATED TERRORISM ALLEGATIONS 3 (2011).

targeted and arrested alleged immigration law violators, identified as national security threats after ICE mined data from NSEERS (and two other immigration programs).[107] More than 2,500 noncitizens were targeted as national security threats before the 2004 Presidential election.[108] In 2008, ICE spokespeople stated that they did not believe that there were similar programs underway, but that is not persuasive: there could be similar programs that use NSEERS' data as even Operation Frontline was not publicly known during its tenure, and there is still not a lot of publicly available information about the program.[109]

Further, even without an official operation or program, the data collected through NSEERS is still available to DHS and is potentially available to other government agencies. The data that was gathered included private and sensitive information such as financial information, biographical information, photographs, and fingerprints. Unfortunately, "[d]ata captured in the NSEERS database are transferred automatically to other DHS systems or captured initially in other systems, including the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) and Enforcement Case Tracking System (ENFORCE)."[110]

The data collection that NSEERS started was succeeded by the US-VISIT Program in 2004.[111] This program, established to "verify the identities and travel documents of aliens,"[112] also collects detailed biographical information and biometric data such as fingerprint scans and photographs of those entering the United States. Arab and Muslim men were often singled out and registered as potential national security threats through this program.[113]

US-VISIT was replaced by the Office of Biometric Identity Management (OBIM). OBIM was created in March 2013 and is focused on "delivering accurate, timely, and high assurance biometric identity information and analysis."[114] OBIM prioritizes improving biometric services and expanding access to biometric data. Thus, the original purpose and data collection of NSEERS still lives today, through OBIM, including the data that was collected, and the privacy that was invaded.

---

107. *See* RWG, *supra* note 96, at 29.

108. *See* Eric Lichtblau, *Inquiry Targeted 2,000 Foreign Muslims in 2004*, N.Y. TIMES (Oct. 30, 2008), https://perma.cc/F8G3-44CS.

109. *See id.*

110. CHARLES K. EDWARDS, INFORMATION SHARING ON FOREIGN NATIONALS: BORDER SECURITY 4 (2012).

111. *See* LISA M. SEGHETTI & STEPHEN R. VINA, U.S. VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY (US-VISIT) PROGRAM 14 (2005).

112. United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"); Enrollment of Additional Aliens in US-VISIT; Authority To Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 73 Fed. Reg. 77473 (Dec. 19, 2008).

113. *See Potential Threats and Potential Criminals: Data Collection in the National Security Entry-Exit Registration System*, U.S. DEPT. JUST. (2005) https://perma.cc/4BUX-NSDY.

114. *See* OBIM, *supra* note 45.

B. *Deferred Action for Childhood Arrivals (DACA)*

1. *Overview of the Policy*

DHS established the DACA policy on June 15, 2012. The policy describes the exercise of prosecutorial discretion by the Secretary of Homeland Security–in light of the limited resources within DHS for the removal of undocumented noncitizens.[115] The policy further directed U.S. Citizenship and Immigration Services (USCIS) to create a deferral process for certain noncitizens who came to the United States as children and who meet other criteria.[116] More than 825,000 DACA recipients have successfully gained deferred removal.[117] Additionally, under DACA, they are able to apply for driver's licenses (in some states) and obtain temporary work permits.[118]

In 2017, the Trump Administration issued a memorandum that rescinded the 2012 DHS memorandum that established DACA.[119] Then-Attorney General Jeff Sessions declared, "Such an open-ended circumvention of immigration laws was an unconstitutional exercise of authority by the Executive Branch."[120] This memorandum was meant to phase out the DACA program, but on June 18, 2020, the Supreme Court ruled against the attempt to rescind the program.[121] The majority ruled that deferring removal is a legal exercise of prosecutorial discretion.[122]

On January 20, 2021, President Biden directed DHS to preserve and fortify DACA.[123] On July 16, 2021, the U.S. District Court for the Southern District of Texas vacated the memorandum that created DACA and permanently enjoined DHS from administering and reimplementing DACA without compliance with the Administrative Procedure Act (APA). The action was based on the conclusion that the June 2012 memorandum required notice-and-comment rulemaking and thus did not go through the proper process.[124] After the district court remanded DACA, DHS appealed the district court's decision. DHS put forward a proposed rule for consideration on September 28, 2021.[125] This proposed rule was pursuant to the Secretary of Homeland Security's broad authority to administer and enforce immigration laws, as

115. *See* Deferred Action for Childhood Arrivals, 86 Fed. Reg. 53736 (Sept. 28, 2021).
116. *See id.*
117. *See id.*
118. *See DACA Fact Shee*t, DEFINE AMERICAN, https://perma.cc/GK8B-USN4 (last visited Feb. 12, 2024).
119. *See Deferred Action for Childhood Arrivals (DACA)*, ASU SANDRA DAY O'CONNOR ROSS-BLAKLEY L. LIBRARY, https://perma.cc/T5H8-BFVU (last visited Feb. 1, 2024).
120. *Letter from Jeff Sessions, then-Attorney General, to then-Acting DHS Secretary Elaine C. Duke* (Sept. 4, 2017), https://perma.cc/E9TB-YBJT.
121. *See* Dept. Homeland Sec. v. Regents U. Cal., 140 S. Ct. 1891, 1895 (2020).
122. *See* Peter Margulies, *The Supreme Court Rules That Trump's DACA Rescission Doesn't Pass Muster*, LAWFARE (June 18, 2020, 5:12 PM), https://perma.cc/QP45-MMHQ.
123. *See* Deferred Action for Childhood Arrivals, *supra* note 115.
124. *See id.*
125. *See id.*

well as the many arguments and conclusions that spurred the district court's decision.[126]

Most individuals granted deferred action under DACA on or before July 16, 2021, including their renewal requests, were not included in the district court's action. The final rule became effective on October 31, 2022, with amendments.[127] USCIS will continue to process and accept applications for current DACA recipients; however, although new DACA requests are accepted, they are not processed.[128]

2. *Data collection and misuse*

DHS, pursuant to 8 C.F.R. §236.23(e)(1), will not use any information about DACA applicants (gained through the application), to initiate immigration enforcement proceedings.[129] As it pertains specifically to ICE, "[i]ndividuals whose cases are deferred under DACA will not be referred to ICE."[130] However, there is the caveat that it is possible for information to be shared with national security and law enforcement agencies, including ICE, for purposes other than removal. This includes assistance in DACA application approval; to identify or prevent fraudulent claims; for national security purposes; or for criminal offense investigations. Thus, there are data security concerns due to these contradictory statements from ICE: they state that individuals will not be referred to ICE, but that it is also possible for information to be shared. Even if the likelihood of information being shared with ICE "for purposes . . . including assistance in the consideration of DACA" is small, the chance is still there.[131]

ICE's purpose lies in securing the United States' borders and "safeguarding the integrity of [the] immigration system."[132] Immigration enforcement is purported to be a "critical component of the overall safety, security, and well-being of" the United States.[133] While there is a purported focus on security and safety of those within the United States, noncitizens seem to be exempt from this purpose as they continuously suffer in detention or through deportations.[134] The information that is volunteered in a DACA application,

---

126. *See id.*

127. *See* Deferred Action for Childhood Arrivals, 87 Fed. Reg. 53152 (Oct. 31, 2022).

128. *See* Press Release, USCIS, DHS Begins Limited Implementation of DACA under Final Rule (Nov. 3, 2022), https://perma.cc/Q46T-Q9BU.

129. 8 C.F.R. §236.23(e)(1) (2024). If there is a criminal offense, fraud, a national security threat, or public safety concerns, however, then immigration enforcement proceedings may be initiated.

130. *Frequently Asked Questions*, U.S. CITIZENSHIP IMMIGR. SERVICES, https://perma.cc/8DBN-5Q2K (last visited Feb. 2, 2024).

131. *See id.*

132. *U.S. Immigration and Customs Enforcement (ICE)*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT, https://perma.cc/3YHS-YVZ4 (last visited Feb. 12, 2024).

133. *See id.*

134. Juliana Kim, *ICE arrests and deportations started to pick up in 2022, a federal report shows*, NPR (Jan. 7, 2023), https://perma.cc/AFW5-MEGX (explaining that "ICE also carried out more than 72, 000 deportations — a slight increase from fiscal year 2021, when numbers dipped to a historic low since the agency's creation in 2003.").

should it be given to ICE, could lead to the eventual detention or removal of the DACA applicants.[135] Thus, in order to have the right to work or the right to have one's removal deferred, a noncitizen must fill out their information for their DACA application. This information may not be safe or protected in a way where it could not be used for harmful purposes. As it pertains to information potentially shared for purposes of assisting in DACA application consideration, the uncertainty in the language itself presents the fear that the data is not fully protected from ICE, and thus noncitizens are not protected from removal. Personally identifiable information, including biometric and health information, may possibly be shared with ICE in this way.

To better elucidate the issue, here is an example: an American citizen has decided to apply for governmental benefits. They submit personally identifiable information to a secure database of one governmental agency, and they are told that the information may be shared, to assist in their application, with their local police station. Even if they have never committed a crime, why would they want the local police station to have this information? What are they going to do with it? Will the information ever be used against them? *Could* the information be used against them (by filling out the application, is this person waiving any rights they may have had)? Their data is not safe within the application, but they have to apply because they need those governmental benefits.

Overall, within this data collection is a lack of data privacy, which comprises proper handling of personal data or personally identifiable information. The data collection alone could be a violation of privacy, in that there is no right to be let alone in order to work or enjoy a full life within the United States. Given the immigration enforcement in this country, unfortunately, this is expected. However, the data that is collected should enjoy some data privacy; sadly, there is a lot of uncertainty regarding the security of the data, as will be discussed.

3. *Electronic Monitoring*

If a noncitizen is currently in an immigration detention center, yet they believe that they meet the requirements to be a recipient of DACA, they must explain to their case officer that they meet the requirements.[136] After reviewing the case, it is possible for the noncitizen to be released to an alternative form of supervision to pursue their DACA application with USCIS.[137]

ICE's current Alternatives to Detention (ATD) program uses technology to monitor noncitizens who have final orders of removal or are conditionally

135. *See* Gonzales, *supra* note 1.

136. *See Deferred Action for Childhood Arrivals*, U.S. IMMIGR. & CUSTOMS ENFORCEMENT, https://perma.cc/VBU3-SBMN (last visited Feb. 5, 2024).

137. *See id.*

released while immigration proceedings are pending.[138] There are three distinct subprograms of ATD: Intensive Supervision Appearance Program (ISAP), Young Adult Case Management Program (YACMP), and the Case Management Pilot Program (CMPP).[139] Two are focused on helping noncitizens navigate the immigration process, but ISAP is where noncitizens find themselves subject to electronic monitoring.

There are three forms of technology that ICE uses to ensure compliance within ISAP: telephonic reporting, Global Positioning System (GPS) monitoring, and SmartLINK.[140] Telephonic reporting requires a noncitizen to report in using a telephone and the voiceprint obtained during enrollment is used to verify the identity of the person speaking. GPS is used to monitor a noncitizen's location and movement history through an ankle monitor. SmartLINK uses facial matching technology and GPS monitoring through an app on the noncitizen's phone or one that is provided. Regardless of which technology is used, a noncitizen's data (biometric, location, voiceprints, etc.) has to be collected. While the direct use of that data through ATD or ISAP may not be malicious, this does not mean that the data cannot eventually be shared.[141] Thus, again, someone in a detention center who wants to apply for DACA is forced to give up data in the application, and then even more as they are released to continue the application process.[142]

Note that, generally, electronic monitoring extensively violates noncitizens' privacy.[143] The purpose of this Note is to focus on specific programs. Here, should a DACA applicant be in a detention center at the time of their application, they may be subject to electronic monitoring. However, electronic monitoring programs have continuously and extensively violated noncitizen privacy since their integration into the immigration system as it pertains to both the original intrusion of privacy and the retention of data.[144]

4. *Database Insecurity*

The previous discussion has centered on the possibility that data, immediately following DACA application receipt, is shared with ICE, or the possibility of electronic monitoring for a DACA applicant already in a detention

138. *See Alternatives to Detention*, DEP'T HOMELAND SEC., https://perma.cc/86QD-499M (last visited Feb. 5, 2024).

139. *See id.*

140. *See id.*

141. *See* Johana Bhuiyan, *Migrant advocates sue US government for data from surveillance program*, THE GUARDIAN (Apr. 14, 2022), https://perma.cc/CQ4H-YXPB (explaining that ICE has been reluctant to share what data it is acquiring, the length of time it is being stored, and how it is using that data).

142. Even if the person did not want to apply for DACA, they may experience ATD.

143. *See generally #NoDigitalPrisons: Challenging E-Carceration,* MEDIAJUSTICE, https://perma.cc/M6BM-Z3QU (last visited Feb 3, 2024).

144. *See ICE Digital Prisons*, JUST FUTURES LAW, https://perma.cc/L74W-652Y (last visited Feb 3, 2024).

center. Each case and each noncitizen are different. But what happens to the database housing all DACA applicants' information?

Since 2012, the program has collected personal data from more than 800,000 applicants.[145] Although DHS claims that information would not be shared with ICE or CPB for immigration enforcement proceeding purposes, when the program was set to expire in 2017, there were concerns about the data being at risk of use for unauthorized purposes after the program ended.[146] In 2017, then-Secretary of Homeland Security Elaine Duke said that she could not promise that the data submitted by DACA applications would not be shared with ICE.[147] Additionally, internal emails show that ICE has access to DACA recipients' information despite the previous promises that ICE would not have access to the data.[148] This technically does not implicate the statute ensuring that data will not be used to start an immigration proceeding, but it does prove that the data is unsafe. What is stopping ICE, after they have access to the database, from initiating an immigration proceeding perhaps five to ten years after their initial access?

In 2017, President Trump issued an Executive Order that stated that "Agencies shall . . . 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."[149] This Executive Order was revoked,[150] but the little privacy protections afforded to noncitizens' data may be at risk in the future. As discussed, the Privacy Act safeguards privacy by creating procedural and substantive rights for personal data held by governmental agencies.[151] Removing Privacy Act protections from data that is within governmental databases is extremely dangerous. These Executive Orders are yet another way that the Executive Branch can impact the privacy of noncitizens. And as it pertains to the DACA database, the constant uncertainty and lack of affirmative promises regarding database security lends to worry about the data truly being protected, and thus, the data truly being granted privacy.

---

145. *See Deferred Action for Childhood Arrivals ("DACA"),* EPIC, https://perma.cc/PG7P-YWSW (last visited Feb. 5, 2024).

146. *See id.*

147. *See* Sam Sacks, *DHS Chief Can't Promise She Won't Hand Over Dreamer Data to ICE*, THE DISTRICT SENTINEL (Sept. 27, 2017), https://perma.cc/L3YU-U69S.

148. *See* Dara Lind, *ICE Has Access to DACA Recipients' Personal Information Despite Promises Suggesting Otherwise, Internal Emails Show*, PROPUBLICA (Apr. 21, 2020, 11:15 AM), https://perma.cc/3V7M-HMFP.

149. Enhancing Public Safety in the Interior of the United States, 82 Fed. Reg. 8799 (Jan. 30, 2017).

150. *See* Revision of Civil Immigration Enforcement Policies and Priorities, 86 Fed. Reg. 7051 (Jan. 25, 2021).

151. *See The Privacy Act of 1974*, EPIC, https://perma.cc/EP9E-JJ7P (last visited Jan. 27, 2024).

C. *Recent Notice of Proposed Rulemaking*

1. *Overview of the Rulemaking*

85 F.R. 74162, titled "Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States," was proposed to expand current biometric data collection at the border.[152] This Notice of Proposed Rulemaking was first introduced by DHS in 2020, and is another example of the Executive Branch violating noncitizen privacy. The proposal was meant to integrate the current entry-exit system with a comprehensive biometric system that permits the collection of biometrics from all noncitizens upon entry and/or departure.[153]

The current system allows DHS to require only certain noncitizens to provide biometrics when entering and departing the United States. "As the regulations currently exempt certain aliens from the collection of biometrics, including those under 14 and over 79, as well as individuals in certain visa classes, CBP does not use fingerprints to confirm the traveler's identity in these cases."[154] The proposed system would require all noncitizens to have their data collected through the use of facial recognition technology. Facial recognition has been particularly useful to apprehend individuals in the past,[155] thus, this proposed rulemaking hopes to expand the current system to provide DHS "with more reliable information to better identify persons of law enforcement or national security concern."[156]

2. *Data collection and misuse*

In addition to facial recognition, the proposed system would collect voice and iris patterns as well.[157] The proposal would also authorize DHS to collect DNA or DNA test results to verify any claimed genetic relationships if a noncitizen is unable to provide sufficient information that would establish a claimed relationship. DHS is hoping to use the DNA evidence to dispel any misrepresentations of those in custody attempting to claim minors that are not biologically related to them.[158]

This data collection, purported to maintain national safety and security, comes with major privacy concerns. Facial recognition technology poses a

---

152. *See* Collection of Biometric Data from Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162 (Nov. 19, 2020).

153. *See id.*

154. *Id.* CBP is the U.S. Customs and Border Protection, a law enforcement agency of DHS.

155. *See id.* ("CBP's facial recognition generated a 'no-match' result for a passenger resulting in further inspection by a CBP officer which then confirmed that the traveler was an alien who was present in the United States without admission or parole and was wanted for aggravated sexual abuse of a minor. Other examples of aliens identified through DHS's biometric verification system include previously removed aliens who committed felonies such as armed robbery with a firearm, assault with a deadly weapon, and aggravated assault.").

156. *See id.*

157. *See DHS, USCIS to Modernize, Define the Collection of Biometrics*, DEPT HOMELAND SEC. (Sep. 1, 2020) https://perma.cc/4KTR-94ZM.

158. *See id.*

privacy threat because it would allow the government to continue to track noncitizens without their knowledge or aid in the unauthorized and unknown development of portfolios of the photographs taken.[159] Facial recognition technology is not the only technology that poses that threat: in order to enter the country, noncitizens are forced to give up other personally identifiable, intimate information about themselves with no information about where that data is going, or how it will be used. This Notice of Proposed Rulemaking is just one example of proposals aimed at expanding current systems to collect data from every noncitizen, simply because they are a noncitizen. This proposal did not come in the wake of a national emergency–the Executive Branch is simply attempting to collect as much data as possible while violating as much privacy as its powers allow.

CONCLUSION

This Note discusses the Executive Branch powers before focusing on three specific examples of those powers in use and violating noncitizens' privacy. It is entirely possible for these privacy violations to occur without the aid of the Executive Branch. Congress could propose legislation tomorrow that violates noncitizens' privacy in an unprecedented way. However, the Executive Branch has an arsenal of ways to violate the privacy of noncitizens, and this Note has discussed some examples. Technology has continuously been wielded as a weapon against noncitizens and their privacy: in the NSEERS program, biometric data was collected and now continues to be collected through OBIM; electronic monitoring is a threat for DACA applicants in detention, but there is also the constant threat of data sharing and the lack of data protection and privacy; under the 2020 Notice of Proposed Rulemaking, invasive data collection will extend to every noncitizen. This Note does not provide an exhaustive list: it is also possible for the President to issue Executive Orders or use his "magical" power detailed in INA §212(f) that may have intended or unintended effects on noncitizens' privacy. For noncitizens like Maria, a DACA recipient, there is always the potential threat of their privacy being violated by the Executive Branch, its powers, and its use of technology.

159. *See* Stephanie Beasley, *Big Brother on the U.S. border?,* POLITICO (Oct. 9, 2019, 4:59 AM), https://perma.cc/W56A-CRFB. *See generally* CLARE GARVIE & LAURA A. MOY, AMERICA UNDER WATCH: FACE SURVEILLANCE IN THE UNITED STATES (2019).