THE (IN)VISIBLE IMMIGRANT'S PRIVACY

Christopher Muhawe*

Abstract

Digital technology has significantly augmented U.S. immigration enforcement. For refugees and asylum seekers, navigating the immigration system involves traversing a complex data labyrinth. Their personal information is collected and used by both immigration authorities and private entities, often without transparency and accountability. This unchecked data collection fuels a surveillance state that disproportionately targets them, violating their agency, autonomy, and self-determination. They engage with immigration authorities at their most vulnerable, compromising their capacity for informed choice and consent. This results in the surrender of extraneous personal information while they remain the least protected by U.S. privacy laws. They become highly visible to immigration enforcement but effectively invisible to privacy laws.

The (in)visible immigrant experiences three distinct but related forms of harm resulting from diminished privacy, which I categorize as (1) data surrender—the yielding of information prompted by the overwhelming need of the powerless to survive; (2) personality curation—the undue self-discipline, subordination, loss of self-esteem and erasure of personal identity and history prompted by the need to appear acceptable to authorities; and (3) weaponization of personal information— the harmful use of data obtained through coercion, vulnerability, or unequal power dynamics.

This Article argues that privacy for refugees and asylum seekers should be protected as a fundamental human right in order to safeguard their agency, autonomy, and self-determination. While acknowledging public safety and national security, this Article advocates for recognition of the unique data privacy challenges

* Christopher Muhawe is a Postdoctoral Research Fellow at the University of Pennsylvania Carey Law School. Many thanks to Anita L. Allen, Ingrid Eagly, Peter Margulies, Leila H. Hlass, Dorothy E. Roberts, Jonathan Klick, Trevor Gardner, Shaun Ossei-Owusu, Serena Mayeri, Michael Morse, Areto Imoukhuede, Julian M. Hill, Alia Al-Khatib, John Boeglin, and participants in the Summer Ad Hoc Workshop at Penn Law and the John Mercer Langston Workshop for helpful comments, conversations and feedback on earlier drafts.

refugees and asylum seekers face. At a minimum, they should be protected by the Fair Information Practice Principles (FIPPs), but they merit more.

***

TABLE OF CONTENTS

INTRODUCTION

Exhaustion gnawed at Dr. James Muntu as he stood at the gates of a United States immigration processing center on the U.S.–Mexico border in Texas. He had narrowly escaped Eritrea's authoritarian regime, where his commitment to human rights activism led to his arrest and five months of incommunicado detention by the military. During his captivity, he was subjected to persecution and torture that left him on the verge of death. After a daring escape from detention in April 2023, he fled Eritrea, seeking asylum in the United States.

Dr. Muntu and other asylum seekers at the U.S.–Mexico border were required to download the AI-powered CBP One app onto their phones to schedule immigration appointments. The U.S. Customs and Border Protection (CBP) had mandated the now-discontinued app as the sole mode of scheduling an appointment with an immigration officer at the Southern border for an asylum application.[1] After eight months of waiting for his appointment, he finally stood in a sterile room at the Ciudad Juárez/El Paso port of entry in front of a CBP officer whose face was hidden behind a computer screen. A barrage of questions rained down on him. Fingerprints, iris scans, and DNA samples—each piece of sensitive personal data meticulously collected and stored without explanation.[2] Throughout the interrogation and data collection process, Dr. Muntu felt as though he was reliving his previous torture ordeal, albeit in a non-physical manner and in a distant land. "This is not about understanding my plight," Dr. Muntu thought. "It is about building a digital dossier on a person who has lost their agency, dignity, and everything."

---

[1] *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR CBP ONE, DHS/CBP/PIA-068 (2021); *cf. USA: Mandatory CBP One Violates Right of Asylum*, AMNESTY INT'L (May 8, 2023), https://www.amnesty.org/en/latest/news/2023/05/usa-mandatory-cbp-one-violates-right-asylum/ [https://perma.cc/PGZ2-LHWR]; *CBP Home Mobile Application*, U.S. CUSTOMS & BORDER PROTECTION, https://www.cbp.gov/about/mobile-apps-directory/cbpone [https://perma.cc/6DKV-68GY] (last updated Mar. 12, 2025) (providing information on the CBP app, which as of Jan. 2025 is no longer available for asylum seekers to submit information or schedule appointments under President Trump's executive orders).

[2] DHS's regulation governing the collection, use, and storage of biometric information under Title 8 of the CFR, part 103, subpart B, starting with 8 C.F.R. § 103.16. A related regulation, 8 C.F.R. § 235.1(f)(1)(ii) authorizes DHS to require any non-exempt alien to provide biometric identifiers.

This account mirrors the broader experience of refugees and asylum seekers whose personal data is collected by and shared among U.S. immigration and government agencies.[3] The U.S. immigration system has created a digital panopticon targeting refugees and asylum seekers. While national security and public safety concerns are legitimate, extensive data collection and prolonged retention expose these vulnerable individuals to disproportionate surveillance and its associated harms, including exclusion and discrimination.[4] By contracting profit-oriented private entities to develop and manage immigration enforcement technologies, the government cedes many aspects of its immigration control duty—an inherently governmental function—to these businesses. It incentivizes them to continuously collect extensive personal information from these individuals. This data is frequently used for commercial surveillance and is often sold to third parties without the refugees' and asylum seekers' consent, further eroding privacy.[5]

Privacy is a fundamental human right.[6] Refugees and asylum seekers deserve a chance to rebuild their lives without having their privacy diminished. The privacy rights and concerns of refugees and asylum seekers are often overlooked despite the pervasive use of digital technology in immigration processes and enforcement, including the stark nature of intrusions on their privacy.[7]

---

[3] *See CBP One Mobile Application Violates the Rights of People Seeking Asylum in the United States,* AMNESTY INT'L (May 9, 2024), https://www.amnesty.org/en/latest/news/2024/05/cbp-one-mobile-application-violates-the-rights-of-people-seeking-asylum-in-the-united-states/ [https://perma.cc/3XWZ-95K2].

[4] *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/NPPD/USVISIT/PIA-002 (2012). The records schedule mandates that US-VISIT retains IDENT records in its custody for 75 years. *See generally* Michele Gilman & Rebecca Green*, The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253 (2018).

[5] *See* NINA WANG, ALLISON MCDONALD, DANIEL BATEYKO & EMILY TUCKER, CTR. ON PRIV. & TECH. AT GEO. L., AMERICAN DRAGNET: DATA-DRIVEN DEPORTATION IN THE 21ST CENTURY (2022), https://americandragnet.org/ [https://perma.cc/4QKJ-AM36].

[6] G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 12 (Dec. 10, 1948).

[7] *See* Maurizio Guerrero, *Surveillance Capitalism has Taken Over Immigration Enforcement—Stifling Dissent and Sowing Fear For Profit*, PRISM (Jan. 9, 2024), https://prismreports.org/2024/01/09/surveillance-capitalism-taken-over-immigration-enforcement/ [https://perma.cc/T6HL-5FVR]; Joel Brown, *Digital Cages: How I.C.E. Uses Digital Surveillance to Track Migrants,* BOS. UNIV.: THE BRINK (Jan. 26, 2024),

While existing privacy scholarship has emphasized the data privacy vulnerabilities of other marginalized communities, the privacy needs and challenges of refugees and asylum seekers remain understudied.[8] Similarly, existing scholarship on immigration surveillance has largely overlooked refugees' and asylum seekers' specific privacy concerns.[9] This Article contributes to the discourse at the intersection of privacy and immigration law by addressing the data protection and privacy concerns of refugees and asylum seekers.

Immigration agencies collect, process, analyze, and share a wide array of biographical, biometric data and related information from refugees and asylum seekers, often with little to no transparency and accountability.[10] The long-term effects of this extensive data collection are disproportionate surveillance, discrimination, and diminished privacy.[11] The history of U.S. immigration policy reveals a pattern of exclusionary surveillance and control targeting immigrants and other marginalized communities.[12]

---

https://www.bu.edu/articles/2024/digital-cages-surveillance-to-track-migrants/ [https://perma.cc/3KNV-9GRK].

[8] *See* SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (2015); KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE AND PUNISH THE POOR (2018); CHARLTON D. MCILWAIN, BLACK SOFTWARE: THE INTERNET & RACIAL JUSTICE, FROM THE AFRONET TO BLACK LIVES MATTER (2019); DANIEL K. CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY AND LOVE IN THE DIGITAL AGE 105–30 (2022); NEIL RICHARDS, WHY PRIVACY MATTERS (2021); Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data- Protection Reform*, 131 YALE L.J.F. 907, 913, 921–24 (2022).

[9] *See* MOHAMMAD HASHIM KAMALI, THE RIGHT TO LIFE, SECURITY, PRIVACY AND OWNERSHIP IN ISLAM (2008); Anil Kalhan, *The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement,* 41 U.C. DAVIS L. REV. 1137 (2008); Anil Kalhan, *Immigration Surveillance*, 74 MD. L. REV. 1 (2014); ASAD L. ASAD, ENGAGE AND EVADE: HOW LATINO IMMIGRANT FAMILIES MANAGE SURVEILLANCE IN EVERYDAY LIFE (2023).

[10] *See* WANG, ET AL., *supra* note 5, at 4.

[11] Erica Posey & Rachel Levinson-Waldman, *What Lurks Behind All That Immigration Data?* ACLU (Apr. 6, 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/what-lurks-behind-all-immigration-data [https://perma.cc/Q68X-QPJJ] (detailing instances of data surveillance targeting marginalized communities, including immigrants).

[12] Naturalization Act of 1798, ch. 54, 1 Stat. 566 (repealed 1802); Alien Enemies Act of 1798, ch. 66, 1 Stat. 577; Alien Friends Act of 1798, ch. 58, 1 Stat. 570 (expired 1800); Sedition Act of 1798, ch. 74, 1 Stat. 596 (expired 1801). Combined, these Acts subjected non-citizens to national surveillance and arbitrary arrests, granting the President the power to deport them by

When facing immigration authorities, asylum seekers are questioned about when, how, and why they fled from their home country. Questions include: Are you a victim of violence? Who are the perpetrators? Do you have family or friends in the U.S.? What could happen to them? What could happen if you return to your home country?[13] The answers to these questions create a cache of personal data—information that persists whether asylum or refugee petitions are granted or denied. Refugees and asylum seekers are compelled to share with ''strangers' their traumatic experiences, including torture, rape, and murder, in detail, potentially placing themselves and their families at risk of shame. The immigration screening process is conducted without adequate counseling and psychosocial support, exposing immigrants to the harm of reliving past traumas.[14] None of this personal information is required by law to be deleted once asylum proceedings conclude or a status determination, regardless of the outcome.

The involuntary migration of refugees and asylum seekers often compels them to surrender extensive personal information in exchange for safety and the basic necessities of life.[15] This phenomenon, which I term "data surrender," sets in because they interact with the immigration authorities at their most vulnerable and desperate moments. The inherent power asymmetry in interactions with authorities compromises their ability to make informed choices and consent.[16] As a result, they cede not only the core personal information[17] required for the Refugee Status Determination (RSD)

---

decree.

[13] *See Preparing for Questioning at an Asylum Office Interview on the One-Year Filling Deadline*, CATH. LEGAL IMMIGR. NETWORK, https://www.cliniclegal.org/resources/asylum-and-refugee-law/preparing-questioning-asylum-office-interview-one-year-filing [https://perma.cc/YM6E-EPDN] (last updated May 24, 2024).

[14] *See* Olivia Magwood, Azaad Kassam, Dorsa Mavedatnia, Oreen Mendonca, Ammar Saad, Hafsa Hasan, Maria Madana, Dominique Ranger, Yvonne Tan & Kevin Pottie, *Mental Health Screening Approaches for Resettling Refugees and Asylum Seekers: A Scoping Review,* 19 INT'L J. ENV'T RSCH. & PUB. HEALTH 1, 1–4 (2022).

[15] *See* Dragana Kaurin, *World Refugee Council Research Paper No. 12: Data Protection and Digital Agency for Refugees*, *in* CTR. FOR INT'L GOVERNANCE INNOVATION, WORLD REFUGEE COUNCIL RSCH. PAPER SERIES 1, 1–2 (2019), https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/ [https://perma.cc/4Y8H-CFJG].

[16] *See infra* pp. 17–22.

[17] U.N. HIGH COMM'R FOR REFUGEES, PROCEDURAL STANDARDS FOR REFUGEE STATUS DETERMINATION UNDER UNHCR'S MANDATE 104–116 (2020), https://www.refworld.org/policy/legalguidance/unhcr/2020/en/123306 [https://perma.cc/B5PP-JGH5] (detailing the asylum seekers' registration

process, but also additional information that I term "extraneous data": personal information that is not directly relevant, proportional, or necessary for assessing and processing an asylum claim and providing humanitarian assistance. The extraneous data includes, among other pieces of personal information, pregnancy-related details, familial relationships, sexual orientation, race, color, sex, gender identity, genetic information, bodily markings such as scars and tattoos, religious background, social media handles, and real-time location data.

With the excessive data collection subjected to them, refugees and asylum seekers experience three distinct but related forms of diminished privacy, which I categorize as (1) "data surrender"—an inescapable yielding of information prompted by the overwhelming necessity of the powerless to survive; (2) "personality curation"—undue self-discipline, subordination, loss of self-esteem, and erasure of personal identity and history prompted by the need to appear acceptable to authorities; and (3) "weaponization of personal information"—the harmful, exploitative, and unfavorable use of data often obtained through coercion, vulnerability, or unequal power dynamics.

The current legal regime for data privacy in the U.S. fails to protect refugees and asylum seekers. First, existing privacy laws are outdated and misaligned with the current digital technology landscape.[18] Secondly, the existing civil rights framework has not been adapted or emphasized to keep pace with modern digital technologies, particularly in addressing the harms of surveillance, discrimination, and the attendant digital inequalities experienced by immigrants.[19]

While the Privacy Act of 1974 protects the privacy of information held in federal record systems, it does not apply to non-U.S. citizens and non-Legal Permanent Residents.[20] This, in effect,

---

procedures, required forms, interviews process and identity information involved in refugee status determination).

[18] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 408 (2012) (noting that U.S. privacy law is obsolete in the context of new and emerging technology).

[19] *See* Anita L. Allen & Christopher Muhawe, *Is Privacy Really a Civil Right?* 40 BERKELEY TECH. L.J. 1 (2025); Alvaro Bedoya, *Privacy as a Civil Right*, 50 N.M.L. REV. 301, 305–06 (2020) (advocating for recognition of privacy as a civil right); *see also* Douglas S. Massey & Karen A. Pren, *Unintended Consequences of U.S. Immigration Policy: Explaining the Post-1965 Surge from Latin America*, 38 POPULATION & DEV. REV. 1 (2012) (discussing discriminatory immigration quotas at the height of the civil rights movement).

[20] 5 U.S.C. § 552a(a)(2).

excludes applicants for refugee and asylum status, as they do not fall within the scope of the Act. Additionally, the Act does not apply to information held by private entities, but DHS and its immigration agencies often partner with private tech contractors and start-ups to develop and operate AI-driven immigration enforcement and border control systems.[21]

The result of extensive data collection is that refugees and asylum seekers become hyper-visible to immigration authorities through the deeply personal information obtained from them, yet their privacy interests remain unseen, unheard, and/or unprotected under the existing legal frameworks. The pronounced absence of laws, regulations, and/or policies protecting a refugee and asylum seeker's privacy is why I refer to them as "(in)visible immigrants." Despite being among the most over-documented individuals in the U.S., they are the least protected under the current data privacy regime. Beyond government surveillance, the (in)visible immigrant is disproportionately exposed to commercial data exploitation, algorithmic discrimination, misinformation, and surveillance, often with little to no legal recourse.[22]

Part I of this Article situates refugees and asylum seekers in the complex and politically charged U.S. immigration system. I argue that the current data privacy legal regime fails to protect these individuals, often rendering them "invisible to the law." In this Part, I acknowledge that the collection of personal information from immigrants is essential for various legitimate purposes, such as identification, fraud prevention, public safety, and national security.[23] However, the data collected from refugees and asylum seekers extends far beyond what is necessary to ensure their safety, access to necessities of life, public safety, and national security.

---

[21] *See* Probert v. Kalamarides, 528 F. App'x 741, 742 (9th Cir. 2013); Abdelfattah v. U.S. Dep't of Homeland Sec., 893 F. Supp. 2d 75, 81 n.4 (D.D.C. 2012), *aff'd*, 787 F.3d 524, 533 n.4 (D.C. Cir. 2015) (upholding District Court's dismissal of claims against private entities and affirming that the Privacy Act does not apply to such entities); PETRA MOLNAR, THE WALLS HAVE EYES: SURVIVING MIGRATION IN THE AGE OF ARTIFICIAL INTELLIGENCE 13–18, 32–36 (2024).

[22] S*ee* Becky Chao, Eric Null, Brandi Collins-Dexter & Claire Park, *Centering Civil Rights in the Privacy Debate*, NEW AM., https://www.newamerica.org/oti/reports/centering-civil-rights-privacy-debate/ [https://perma.cc/FJ2R-K4CX] (last updated Aug. 14, 2019).

[23] Implementation of the United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"); Biometric Requirements, 69 Fed. Reg. 468, 477 (interim final rule, Jan. 5, 2004) (supplementary information); *see* Donald Kerwin & Margaret D. Stock, *National Security and Immigration Policy: Reclaiming Terms, Measuring Success, and Setting Priorities,* 1 HOMELAND SEC. REV. 131 (2007).

Part II examines how the (in)visible immigrant with different intersecting identities is thrust into both government and commercial surveillance gazes—with little to no possibility of escaping the resulting diminished privacy violations and their associated harms. Refugees and asylum seekers experience three distinct but interconnected forms of harm in the data cycle: (1) data surrender, (2) personality curation, and (3) weaponization of personal information. This Part also highlights the impact of privacy violations against refugees and asylees, which extends beyond the individuals themselves but also to society. These violations can result in the suppression of freedom of speech, association, and civic participation. While examining how these groups of immigrants are disproportionately subjected to surveillance and exclusion by both government and commercial entities, this Part also sheds a light on similar burdens borne by other marginalized communities.

Part III argues for the protection of the (in)visible immigrant's privacy by advancing the view that privacy is a fundamental human right—one that should be upheld for refugees and asylum seekers regardless of their citizenship and immigration status. I also propose that refugees and asylum seekers be granted the right to data deletion, exercisable upon the grant of citizenship. I also assess the current federal data protection proposals, focusing on the American Privacy Rights Act (APRA)[24] (introduced in the last Congress), to evaluate whether it provides adequate privacy protection for traditionally marginalized groups, including immigrants. To address the key gaps in the APRA, I propose the establishment of an Independent Data Protection Agency (IDPA) tasked with safeguarding the privacy interests of all individuals, including citizens and permanent residents. Within the IDPA, a dedicated office or unit should be created to specifically protect and address the data privacy of refugees and asylum seekers, recognizing their heightened vulnerability throughout the data lifecycle.

I. THE (IN)VISIBLE IMMIGRANT

As Adam B. Cox and Eric A. Posner argue, a central goal of immigration policy for all governments, at a broad level, is to admit desirable individuals.[25] The process involves determining the number and type of people who can be admitted within a country's borders.[26] This determination may be based on the discretionary

[24] American Privacy Rights Act (APRA), H.R. 8818, 118th Cong. (2024).

[25] Adam B. Cox & Eric A. Posner, *The Second-Order Structure of Immigration Law*, 59 STAN. L. REV. 809, 814 (2007).

[26] *Id.* at 814–21.

framework of *ex ante* screening, which involves collecting personal data and historical details before an individual enters the country to assess admissibility, and *ex post* screening, which entails ongoing data collection and monitoring after entry to reassess eligibility and compliance with immigration regulations.[27] Screening processes determine who can be admitted to the U.S. temporarily or permanently under the Immigration and Nationality Act (INA).[28] As such, a non-citizen seeking admission to the U.S. must meet the criteria for either immigrant or non-immigrant status.

Accordingly, a non-immigrant is admitted for a specific temporary period and purpose, such as tourism, work, study, business, medical treatment, exchange visits, athletics, entertainment, attending a particular educational institution, or working a particular job.[29] In contrast, an immigrant is someone seeking to reside in the U.S. permanently.[30] Currently, immigrants fall into four main categories: (1) family-sponsored immigrants, such as spouses and children of U.S. citizens;[31] (2) employment-based immigrants, including skilled workers, professionals, and investors;[32] (3) diversity immigrants selected through the Diversity Visa Lottery;[33] and (4) humanitarian admission, including refugees and asylum seekers fleeing persecution or conflict.[34] Unlike immigrants in the first three categories and individuals who voluntarily leave their countries as non-immigrants, refugees and asylum seekers involuntarily move from their home countries for reasons beyond their control.[35] This Article focuses on refugees and asylum seekers, who are often differentiated from other immigrants. They flee dire circumstances, including wars such as Russia's invasion of Ukraine and the ongoing civil conflicts in the eastern Democratic Republic of Congo; religious persecution like the targeting of Christian converts in Iran; political repression in

---

[27] *Id.* at 836–40.

[28] 8 U.S.C. §§ 1101–1537.

[29] *See id.* § 1101(a)(15) (defining the term "immigrant" and by exclusion establishing the general categories of "non-immigrants").

[30] *See id.*

[31] *Id.* § 1153(a).

[32] *Id.* § 1153(b)(3).

[33] *Id.* § 1153(c).

[34] *Id*. §§ 1157 (refugee admission), 1158 (asylum).

[35] *See id.* § 1101(a)(15); STEPHEN H. LEGOMSKY & DAVID B. THRONSON, IMMIGRATION AND REFUGEE LAW AND POLICY (7th ed. 2018); T. ALEXANDER ALEINIKOFF, DAVID A. MARTIN, HIROSHI MOTOMURA, MARYELLEN FULLERTON, JULIET P. STUMPF & PRADEEPAN GUNASEKARAN, IMMIGRATION AND CITIZENSHIP: PROCESS AND POLICY 729 (9th ed. 2021).

Venezuela; severe economic deprivation; and climate-induced displacement and hunger across the Horn of Africa.[36]

A. REFUGEE AND ASYLUM SEEKER

A refugee is "any person who is outside any country of such person's nationality or, in the case of a person having no nationality, is outside any country in which such person last habitually resided, and who is unable or unwilling to return to, and is unable or unwilling to avail him or herself for the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group or political opinion."[37] The Refugee Act empowers the President, in consultation with Congress, to authorize the resettlement of a specified number of refugees each year and to determine the focus of these resettlement efforts.[38] Once admitted to the U.S., refugees can apply to adjust their status to permanent resident status after one year.[39]

---

[36] THOMAS A. ALEINIKOFF, DAVID A. MARTIN, HIROSHI MOTOMURA, MARYELLEN FULLERTON, JULIET P. STUMPF & PRATHEEPAN GULASEKARAM, IMMIGRATION AND CITIZENSHIP: PROCESS AND POLICY 729, 729 (West 9th ed. 2021); Paul Kirby, *Why did Putin's Russia invade Ukraine?*, BBC (Mar. 18, 2025), https://www.bbc.com/news/articles/cj0q964851po [https://perma.cc/SKK8-J3B6]; Farnaz Fassihi & Hamed Aleaziz, *This Christian Convert Fled Iran, and Ran into Trump's Deportation Policy*, N.Y. TIMES (Feb. 23, 2025), https://www.nytimes.com/2025/02/23/world/middleeast/this-christian-convert-fled-iran-and-ran-into-trumps-deportation-policy.html [https://archive.ph/ets9O]; *Venezuela: Persecution Builds Relentlessly for Civil Society and Dissidents*, AMNESTY INT'L (Apr. 16, 2024), https://www.amnesty.org/en/latest/news/2024/04/venezuela-civil-society-dissident-voices-face-incessant-escalation-persecution/ [https://perma.cc/VSC8-J47N]; *Deadly Climate-Induced Flooding Displaces Nearly 1.6 Million People Across the Horn of Africa*, ACTION AGAINST HUNGER (Nov. 29, 2023), https://www.actionagainsthunger.org/press-releases/deadly-climate-induced-flooding-displaces-nearly-1-6-million-people-across-the-horn-of-africa/ [https://perma.cc/9GHF-9TCS]; Ctr. for Preventive Action, *Conflict in the Democratic Republic of Congo*, COUNCIL ON FOREIGN RELS.: GLOBAL CONFLICT TRACKER, https://www.cfr.org/global-conflict-tracker/conflict/violence-democratic-republic-congo [https://perma.cc/X2NV-YXRC] (last updated Mar. 20, 2025).

[37] 8 U.S.C. § 1101(a)(42)(A).

[38] *See id.* § 1157(a).

[39] *Id.* § 1159(a).

The common denominator between a ''refugee" and an ''asylum seeker" is the search for safety and a plea to stay in the U.S., whether temporarily or permanently.[40] Both groups have fled their country of nationality or are stateless, seek protection from persecution, and face the risk of serious human rights violations. While the INA does not directly define asylum seeker, it adopts the definition of a refugee from the 1951 Refugee Convention and its 1967 Protocol to define who an asylum seeker is.[41] An asylum seeker must demonstrate a well-founded fear of persecution on account of one of the five protected groups: race, religion, nationality, and membership in a particular social group or political opinion.[42] Another way of looking at it is that individuals outside the U.S. who apply for protection based on one of the five protected grounds are considered refugees, while those already present in the U.S. territory or at the border seeking the same protection are classified as asylum seekers.[43] Like other refugees, an asylum seeker must demonstrate a well-founded fear of persecution.[44] In *INS v. Cardoza-Fonseca*, the Supreme Court clarified that asylum eligibility does not require proving a "clear probability" of persecution, but rather a "well-founded fear," citing the definition of "refugee" under § 1101(a)(42) of the INA.[45] The "well-founded fear" in that case was respondent's, Cardoza-Fonseca, who feared persecution if deported to Nicaragua, citing her opposition to the Sandinista regime and the imprisonment and torture of her brother for his political activism in the same vein.[46]

Building on this foundation, the U.S. law grants individuals the right to apply for asylum upon arrival at U.S. borders or from within

---

[40] *Id.* § 1158. Section 1158(b)(1)(A) allows the Secretary of Homeland Security or the Attorney General to grant asylum to individuals who meet this definition of "refugee." This can be distinguished from the separate remedy of withholding of removal, which prevents removal to a country where the person's life or freedom would be threatened. *See* 8 U.S.C. § 241(b)(3).

[41] 8 U.S.C. § 1101(a)(42)(A) (defining "refugee" in a manner consistent with the 1967 Protocol Relating to the Status of Refugees); *see also* Convention Relating to the Status of Refugees art. 1, July 28, 1951, 189 U.N.T.S. 137; Protocol Relating to the Status of Refugees, Jan. 31, 1967, 606 U.N.T.S. 267.

[42] 8 U.S.C. § 1158(b)(1).

[43] *See* LEGOMSKY & THRONSON, *supra* note 35, at 1136–37.

[44] *See* 8 U.S.C. §§ 1158(b)(1)(A)–(b)(1)(B)(i), 1101(a)(42)(A).

[45] INS v. Cardoza-Fonseca, 480 U.S. 421, 424, 430–32 (1987).

[46] *Id.* at 428; (citing 8 U.S.C. § 1101(a)(42)); *see* SUSAN J. COHEN & STEVEN T. TAYLOR, JOURNEYS FROM THERE TO HERE: STORIES OF IMMIGRANT TRIALS, TRIUMPHS AND CONTRIBUTIONS 83–114 (2021) (exploring the struggles and resilience of immigrants as they navigate the challenges of the U.S. immigration system on their path to citizenship).

U.S. territory.[47] Dr. Muntu, a human rights activist who narrowly escaped torture and near-death at the hands of Eritrea's authoritarian regime, seeks asylum on the grounds of political persecution, a category explicitly protected under asylum law.

B. NAVIGATING THE ASYLUM PROCESS

The asylum process in the U.S. generally follows three pathways: affirmative and defensive asylum applications, as well as asylum merits interviews.[48] While all three aim to provide protection from persecution, they differ in procedure and adjudication mechanisms.

Affirmative asylum is initiated by individuals who are present in the U.S. and not in removal proceedings.[49] U.S. Citizenship and Immigration Services (USCIS) manages the process, under which an applicant must file Form I-589, Application for Withholding of Removal, typically within one year of their arrival.[50] Following the submission, applicants are scheduled for a non-adversarial interview with a USCIS asylum officer who assesses the credibility and merits of their claim.[51] If the officer approves the application, the individual is granted asylum. One year after the grant of asylum, the individual can apply for an adjustment of status to become a lawful permanent resident, commonly known as a green card holder.[52] However, if the application is denied, and the applicant does not have lawful immigration status, their case is referred to an Immigration Judge for removal proceedings, with an option to pursue a defensive asylum claim.[53]

The defensive asylum application is made in response to removal proceedings initiated by the Department of Homeland Security (DHS).[54] This procedure occurs before an Immigration Judge of the Executive Office of the Immigration Review, which is part of the Department of Justice (DOJ).[55] This process begins when an

---

[47] 8 U.S.C. § 1158(a)(1).

[48] *Obtaining Asylum in the United States*, U.S. CITIZENSHIP AND IMMIGR. SERVS., https://www.uscis.gov/humanitarian/refugees-and-asylum/asylum/obtaining-asylum-in-the-united-states [https://perma.cc/L8XE-9BL2] (last updated Sept. 13, 2023).

[49] 8 C.F.R. § 208.2(a)(1)(i).

[50] 8 C.F.R. § 208.4(a)(2)(ii) (2025); U.S. CITIZENSHIP AND IMMIGR. SERVS., *supra* note 48 (explaining the affirmative asylum application process).

[51] 8 C.F.R. § 208.9(b) (2025).

[52] *Id.* § 209.2(a)(1).

[53] *Id.* § 208.14(c)(1).

[54] *Id.* § 1208.2(c)(1)(v).

[55] *Id.* § 1208.2(b).

individual is placed in removal proceedings or apprehension at the border.[56] The applicant still files Form I-589 defensively in the adversarial setting to prevent removal.[57] The Immigration Judge hears from both the applicant or their attorney and the DHS attorney in opposition, before deciding on asylum.[58] The determination is either a grant of asylum or a denial, in which case the applicant has the right to appeal the decision to the Board of Immigration Appeals(BIA) and may seek judicial review in federal court.[59] If asylum is granted, the applicant can remain in the U.S. and eventually apply to become a lawful permanent resident.[60] With this status, individuals may also submit derivative applications to facilitate the immigration of qualifying family members, thus enabling family unification in the United States.[61]

In addition to the affirmative and defensive processes, some individuals are placed into the Asylum Merits Interview (AMI) program—introduced in 2022—which serves as a pathway for certain non-citizens who receive a positive credible fear determination.[62] This step in the expedited removal process allows an asylum officer to conduct a more in-depth assessment of the asylum claim based on the existing credible fear interview without initially referring the case to an immigration judge.[63] If the officer grants asylum, the individual may remain in the U.S. and eventually apply for permanent resident status. However, if the asylum is not granted at the AMI stage, the case is referred to immigration court for streamlined removal proceedings, where the record from the AMI will be considered.[64] If the asylum officer recommends denial of all

---

[56] *Id.* § 1229(a).

[57] *Id.* § 1208.4(b)(3)(iii).

[58] *Id.* § 1240.11(c)(3).

[59] *Id.* § 1003.1(b) (establishing the BIA's jurisdiction over appeals from decisions of immigration judges); *see also* 8 U.S.C. § 1252(a)(1) (providing for judicial review of the final removal orders in court).

[60] 8 U.S.C. § 1159(b).

[61] *Id.* § 1153(a)(2)(A)–(B).

[62] Fact Sheet: Implementation of the Credible Fear and Asylum Processing Interim Final Rule, Dep't of Homeland Sec. (May 31, 2022), https://www.uscis.gov/humanitarian/refugees-and-asylum/asylum/fact-sheet-implementation-of-the-credible-fear-and-asylum-processing-interim-final-rule [https://perma.cc/MTU6-XW49]; Procedure for Credible Fear Screening and Consideration of Asylum, Withholding of Removal, and CAT Protection by Asylum Officers, 87 Fed. Reg. 18,078 (Mar. 29, 2022); 8 U.S.C. § 1225(b)(1)(A)(ii) (2023); 8 C.F.R. § 208.30(f) (2023). The Asylum Merits Interview was rolled out in 2022, purportedly to reduce backlog in immigration courts (and fast-track proceedings).

[63] 8 C.F.R. § 208.9(a).

[64] 8 C.F.R. § 208.9(f)(2).

forms of relief, the applicant is entitled to a *de novo* hearing before the immigration judge, who will conduct a new review of the claim, though the record will likely be part of the evidence.[65]

It is important to note that regardless of the pathway undertaken by the asylum seeker, the U.S. immigration authorities collect extensive personal information from refugees and asylum seekers from their first encounter and throughout the screening process to assess and determine their applications.[66] This process subjects them to an inescapable, extensive, and endless information lifecycle over which they have no control.

C. THE (IN)VISIBLE IMMIGRANT'S DATA LIFECYCLE

A data lifecycle refers to the sequence of stages that information undergoes, characteristically involving the phases of collection, processing, dissemination, use, storage, disposition, and deletion.[67] As part of the broader U.S. immigration and border control system, refugees and asylum seekers are subjected to biographic, biometric, and related data collection for national security and law enforcement reasons.[68] The collected information is also used for other administrative purposes such as applicant identification, fraud detection, and grant of immigrant benefits, including work authorization.[69]

While U.S. citizens are also required to provide personal information for travel and various services, their data lifecycle significantly contrasts with that of refugees and asylum seekers. The differences are mainly in the quantity of data collected, the data retention period, and the accountability and remedial process in the

---

[65] 8 C.F.R. § 1240.11(a).

[66] *Vetting, Security, and Fraud Screening in Asylum Process*, HUM. RTS. FIRST (Dec. 4, 2015), https://humanrightsfirst.org/library/vetting-security-and-fraud-screening-in-asylum-process/ [https://perma.cc/E787-7DZC] (last visited Mar. 15 2025).

[67] *Information Life Cycle*, *in* GLOSSARY, NAT'L INST. OF STANDARDS AND TECH. COMPUT. SEC. RES. CTR., https://csrc.nist.gov/glossary/term/information_life_cycle# [https://perma.cc/2C3H-NLXK] (last updated Mar. 19, 2025).

[68] *See* Refugee Processing and Security Screening, U.S. CITIZENSHIP AND IMMIGR. SERVS., https://www.dhs.gov/publication/dhsuscispia-068-refugee-case-processing-and-security-vetting [https://perma.cc/98XH-RRAU] (last updated Sept. 13, 2023); Edward Alden, *Immigration and Border Control*, 32 CATO J. 107, 114 (2012) (explaining the expansion of U.S. immigration and border control policies after 9/11, including universal screening, biometric data collection, and extensive background checks for immigrants).

[69] *See* 8 U.S.C. § 1158; 8 C.F.R. § 274a.12 (2025).

event of privacy violations. For example, CBP deletes photographs of traveling citizens and lawful permanent residents within hours of completing the matching process.[70] In contrast, photographs of non-citizens are stored in the Automated Targeting Storage System (ATS) Unified Passenger Module for 14 days; after which period, they are transferred to the Automated Biometric Identification System (IDENT), where they are retained for up to 75 years.[71]

The distinction is further underscored by the fact that the Privacy Act of 1974 only protects citizens and lawful permanent residents, in effect excluding refugees and asylum seekers.[72] Furthermore, while USCIS cites DHS's Fair Information Practice Principles (FIPPs) as a framework for the protection of refugees and asylum seekers' privacy, these principles fall short of providing meaningful protection in today's environment.[73] The FIPPs—comprising transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing—were initially formulated to promote responsible data practices.[74]

To understand the full extent of the disparity, it is important to examine the specific categories of data collected from refugees and asylum seekers, beginning with the biographic and biometric information that initiates their surveillance.

---

[70] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE 21 (2018), https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service [https://perma.cc/2T32-X4KA].

[71] *Id.; See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM 7 (2017), *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-may2021.pdf* [https://perma.cc/87TM-NBUS].

[72] 5 U.S.C. § 552a(a)(2).

[73] *See USCIS Policy Manual, Vol. 1, Part A*, *Chapter 7 – Privacy and Confidentiality*, U.S. CITIZENSHIP AND IMMIGR. SERVS., https://www.uscis.gov/policy-manual/volume-1-part-a-chapter-7 [https://perma.cc/WK9L-PZ67] (discussing USCIS's use of the FIPPs as a guiding framework for protecting the personal data for refugee and asylum seekers); *see also* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 964–72 (2017) (analyzing the limitations of FIPPs, including their inadequacy in addressing surveillance concerns and the disproportionate burden placed on individuals to protect their own privacy).

[74] Privacy Policy Guidance Memorandum, No.:2007-1 (as amended January 19, 2007), U.S. DEP'T OF HOMELAND SEC. (Jan. 7, 2009), https://www.aila.org/library/hhs-teufel-memo-dhs-privacy-policy-non-us-persons [https://perma.cc/BE2D-YCZJ]; *see* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 16 (2001).

1. *Biographic and Biometric Information*

The INA provides the legal framework for the asylum application process, outlining eligibility, application procedures, and criteria for asylum.[75] With this, USCIS is mandated to collect biographic information from asylum seekers.[76] Executive orders also spell out directives and policies for immigration enforcement, mandating the vetting of refugees and asylum seekers—procedures that routinely include the collection and review of biographic data.[77]

In addition to biographic information, USCIS collects biometric data such as fingerprints, palm prints, facial structures, retinal or iris configurations, DNA, and voice samples.[78] DHS requires biometrics for identification and verification due to their apparent accuracy and reliability in automated recognition processes in immigration and law enforcement.[79] Biometrics are also required for domestic and international data-sharing agreements and to conduct criminal and national security background checks.[80]

---

[75] 8 U.S.C. § 1158.

[76] 8 C.F.R § 1003.47 (2025).

[77] Protecting the Nation from Foreign Terrorist Entry into the United States, Exec. Order No. 13,780, 82 Fed. Reg. 13209 (Mar. 9, 2017).

[78] U.S. DEP'T OF JUSTICE, OFF. OF THE INSPECTOR GEN., REPORT NO. 1-2003-005, STATUS OF IDENT/IAFIS INTEGRATION, at 1 n.5 (2003), http://www.usdoj.gov/oig/reports/plus/e0305/Final.pdf [https://perma.cc/6TV3-P5M8]*; see also* John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 139–40 (1997); BIOMETRICS IDENTITY MGMT. AGENCY, DOD BIOMETRICS COLLABORATION FORUM EVENT REPORT (2011), https://apps.dtic.mil/sti/citations/ADA550048 [https://perma.cc/CW89-RE5U]; System of Records Notice, DHS/USCIS-018 Immigration Biometric and Background Check System of Records, 83 Fed. Reg. 36950 (proposed Jul. 31, 2018).

[79] *See* Press Release, U.S. Dep't of Homeland Sec., New Biometric Technology Improves Security and Facilitates U.S. Entry Process for International Travelers (Mar. 2009), https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-fingerprint_consumer_friendly_content_1400_words.pdf [https://perma.cc/RT6Q-3QLQ]; *see also* REBEKAH ALYS LOWRI THOMAS, GLOBAL COMM'N ON INT'L MIGRATION, *Biometrics, International Migrants and Human Rights*, *in* GLOBAL MIGRATION PERSPECTIVES 1, 7 (2005), https://www.refworld.org/reference/research/gcim/2005/en/19799 [https://perma.cc/8L7X-L68F].

[80] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE UNITED NATIONS HIGH COMMISSION FOR REFUGEES (UNHCR) INFORMATION DATA SHARE (2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf [https://perma.cc/NV3E-X7RF].

2. *Related and Contextual Information*

In addition to biographic and biometric information, USCIS collects related or contextual data as supplementary information about the refugee's or an asylum seeker's claim of persecution or fear thereof.[81] I define related data to mean any supplementary information collected by immigration authorities beyond an individual's biographic and biometric data. This includes digital, contextual and behavioral data obtained through surveillance technologies, social media monitoring, location tracking, and other records beyond what an individual physically and willingly provides.[82] Immigration authorities have leveraged digital technologies, including smartphone applications, ankle monitors, social media, and others, to collect excessive personal information from asylum seekers.

In October 2020, CBP launched the CBP One app—now rebranded as CBP Home—which collected not only location data, but also biographic information (such as names, dates of birth, and countries of origin), biometric data (including facial images), and previous travel details to facilitate immigration processing.[83] Until January 20, 2025, asylum seekers at the U.S.-Mexico border were required to use the CBP One app to schedule appointments for presenting their asylum claims unless they could demonstrate an inability to access it.[84]

---

[81] *See* Directive on Biometrics for Identification and Screening to Enhance National Security, 1 PUB. PAPERS 757, 758 (June 5, 2008) (directing federal agencies to enhance biometric and related data collection for identification, screening, and national security purposes, including in immigration contexts).

[82] *See* Abril Ríos-Rivera, *The Digitization of US Asylum Application Process and Externalization in Mexico*, 73 FORCED MIGRATION REV. 18, 18–23 (2024), https://www.fmreview.org/digital-disruption/ [https://perma.cc/K44B-JMN6] (explaining how digital technologies, through electronic monitoring, extend surveillance by collecting asylums seekers' location data and other personal information beyond physical checkpoints).

[83] *See* Circumvention of Lawful Pathways, 88 Fed. Reg. 31314 (May 16, 2023) (to be codified at 8 C.F.R. pts. 208, 1003, 1208); *Fact Sheet: Circumvention of Lawful Pathways Final Rule*, U.S. DEP'T OF HOMELAND SEC. (May 11, 2023), https://www.dhs.gov/news/2023/05/11/fact-sheet-circumvention-lawful-pathways-final-rule [https://perma.cc/5CWC-7RDC]; CBP One: An Overview, Am. Immigr. Council (Mar. 12, 2025), https://www.americanimmigrationcouncil.org/research/cbp-one-overview [https://perma.cc/JB4Q-HV7D] (noting that the CBP One app has since been replaced by the CBP Home app).

[84] AMNESTY INT'L, CBP ONE – A BLESSING OR A TRAP? 14 (2024), https://www.amnesty.org/en/documents/amr51/7985/2024/en/

Related data is also collected through the Alternative to Detention (ATD) program, under which ICE monitors individuals on bond or awaiting adjudication of their applications. This monitoring involves the use of ankle monitors, smartwatches, and smartphones to gather contextual and behavioral data.[85] Additionally, USCIS can access and review social media and online activity accounts as part of the evaluation process for granting immigration benefits.[86]

Related data is also often embedded in the evidentiary materials submitted in support of an asylum claim. Individuals may provide medical or psychological evaluations, affidavits, and witness statements to corroborate their accounts of torture or persecution.[87] This highly sensitive information—essential to the adjudication of their application—qualifies as related data as it is personally attributable and can directly reveal the applicant's identity.

The extensive collection of biographic, biometric, and contextual information underscores the pervasive surveillance imposed on vulnerable refugees and asylum seekers throughout their immigration journey. The ongoing collection of data throughout and beyond the asylum process creates an expansive, enduring digital footprint. While framed as essential for identification, verification, and security screening, these information practices raise significant concerns about privacy, autonomy, and the long-term implications of a constantly monitored existence. Given the scale of data collection and surveillance, it is crucial to examine how the power imbalance between asylum seekers and immigration authorities

---

[https://perma.cc/CXM5-6JR9]; U.S. DEP'T OF HOMELAND SEC., *supra* note 1 (noting that the CBP app is no longer available for asylum seekers to submit information or schedule appointments under President Trump's executive orders).

[85] *See Alternatives to Detention*, U.S. IMMIGR. AND CUSTOMS ENF'T, https://www.ice.gov/features/atd [https://perma.cc/CLJ5-W6BF] (last updated Jan. 29, 2025); Joel Brown, *Digital Cages: How ICE Uses Digital Surveillance to Track Migrants*, BOS. UNIV.: THE BRINK (Jan. 26, 2024), https://www.bu.edu/articles/2024/digital-cages-surveillance-to-track-migrants/ [https://perma.cc/MFB4-LTMN] (explaining how ICE's digital surveillance results in harm by retraumatizing asylum seekers and imposes constant psychological distress).

[86] *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATIONS MANAGEMENT SYSTEM (CLAIMS) 3 AND ASSOCIATED SYSTEMS 1-3 (2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis016d-claims3-july2020.pdf [https://perma.cc/SYP8-RWUH].

[87] *See* Elizabeth Scruggs, Timothy C. Guetterman, Anna C. Meyer, Jamie VanArtsdalen & Michele Heisler, "*An Absolutely Necessary Piece": A Qualitative Study of Legal Perspectives on Medical Affidavits in the Asylum Process*, 44 J. FORENSIC & LEGAL MED. 72, 73 (2017).

unfold within the immigration data lifecycle, ultimately shaping the experience of the (in)visible immigrant.

D. VULNERABILITY AND BLURRED CONSENT

The (in)visible immigrant often experiences a breach of trust, protection, and support in their home country and failures in the social contract.[88] Against this backdrop, it is difficult to envision a group more deserving of humanitarian support than asylum seekers and refugees. They are often without a home, unable to seek protection from their home governments, and reliant on the goodwill of other people and foreign nations.[89] In *M.S.S v. Belgium & Greece,* the European Court of Human Rights recognized asylum seekers represent a uniquely vulnerable group whose precarious status necessitates heightened humanitarian assistance.[90] This vulnerability becomes acute for refugees and asylum seekers with families, as their needs extend beyond the individual to encompass the well-being of the entire household, particularly minors. The trauma endured by refugee parents often has profound implications on the psychosocial well-being of their children, compounding the urgent need for holistic protections and support.[91]

For refugees and asylum seekers, the core needs encompass basic human necessities such as food, shelter, and healthcare. Critically, they need protection from removal to the country of persecution.[92] In seeking these protections, they face an imbalance in power in their interactions with immigration enforcement authorities. This asymmetry compels them to acquiesce to sweeping and massive data collection out of fear of adverse consequences in their asylum claims, reflecting undue influence and coercion.[93] They

---

[88] *See* Anita L. Allen, *Social Contract Theory in American Case Law,* 51 FLA. L. REV. 1, 35–36 (1999) (explaining the government's duty to protect individual rights and freedoms as part of the social contract).

[89] Jacob Sohlberg, Mattias Agerberg & Peter Esaiasson, *Waiting for Asylum: Reduced Institutional and Interpersonal Trust*, 72 POL. STUD. 343, 344–46 (2024).

[90] App. No. 30696/09, 53 Eur. H.R. Rep. 2, 53 (2011).

[91] *See* Cindy C. Sangalang & Cindy Vang, *Intergenerational Trauma in Refugee Families: A Systematic Review,* 19 J. IMMIGR. & MINORITY HEALTH 745, 751–53 (2017) (discussing the impact of parental trauma on the mental health and adjustment of refugee children).

[92] Thomas Gammeltoft-Hansen & James C. Hathaway, *Non-Refoulement in a World of Cooperative Deterrence*, 53 COLUM. J. TRANSNAT'L L. 235, 242 (2015) (explaining that protection from return to a country of persecution is a core tenet of refugee law rooted in the principle of non-refoulement).

[93] *See* Stephen Manning & Juliet Stumpf, *Big Immigration Law*, 52

often have no informed choice and consent to the data collection in these circumstances. Non-compliance with such data collection schemes may lead to the dismissal of their application or forfeiture of the adjudication rights and related benefits.[94] Thus, asylum seekers face a dilemma: comply and risk exposure to surveillance, discrimination, and diminished privacy, or object to excessive data collection and risk the denial of basic protections and even deportation. This paradigm undermines their autonomy and entrenches them in a cycle of structural vulnerability.

This vulnerability is further compounded by the conditional and time-limited nature of the public benefits to which they may be entitled. Although some federal welfare programs, such as Medicaid or the Supplemental Nutrition Assistance Program (SNAP), may be available to them, access is often restricted and typically limited to five to seven years.[95] To meet basic needs, many must seek employment, which requires securing employment authorization from immigration authorities—a process governed by specific regulatory requirements that subject them to further data collection.[96] In this way, the pursuit of survival and welfare needs deepens their entanglement in a data-intensive system that further erodes their privacy and reinforces their exposure to institutional surveillance.

The vulnerability and uncertainty faced by the (in)visible immigrant diminishes their agency, impairing their ability to make truly informed choices regarding data collection.[97] Informed consent involves a process by which a data subject is fully informed and actively participates in decisions, granting permission with full knowledge of the potential outcomes of using, accessing, or sharing data and related digital identities.[98]

Refugees and asylum seekers are often not adequately informed about their privacy rights, including their right to know what personal data is being collected, how it will be used, and whether

---

U.C. DAVIS L. REV. 407, 413, 423–24 (2018) (explaining power asymmetry between non-citizens and the immigration authorities); Bianca Bruno, *Immigrant Parents Coerced Into Waiving Rights, ACLU Says*, COURTHOUSE NEWS SERV. (July 25, 2018), https://www.courthousenews.com/immigrant-parents-coerced-into-waiving-rights-aclu-says/ [https://archive.ph/wbYiH]

[94] *See* 8 C.F.R. 208.10 (2025); *see also* U.S. CITIZENSHIP & IMMIGR. SERVS., AFFIRMATIVE ASYLUM PROCEDURES MANUAL 66 (2016); *id.* at 55.

[95] *See* 8 U.S.C. § 1612(b)(2)(A)(i)(I)–(III); U.S. CITIZENSHIP & IMMIGR. SERVS., APPENDIX: ELIGIBILITY FOR PUBLIC BENEFITS (2020).

[96] *See* 8 C.F.R. § 274a.12(a)(3), (5), (10) (2018).

[97] *See* Kaurin, *supra* note 15, at 4.

[98] *See* Masooda Bashir, Carol Hayes, April D. Lambert & Jay P, Kesan, *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, 52 PROC. ASS'N FOR INFO. SCI. & TECH. 1, 2 (2015).

they have the ability to limit or contest excessive data collection.[99] Data collection and sharing should occur under conditions of informed consent; however, this is rarely true for refugees and asylum seekers.[100] One major barrier is that asylum application documents and data-sharing terms are often not in the applicant's native language, significantly undermining their ability to fully understand what they are consenting to.[101] This imbalance is further exacerbated by the requirement that affirmative asylum seekers have to find their own interpreters—often at personal expense.[102] This financial burden compels them to proceed in languages they do not fully comprehend and give their information under conditions shaped by desperation rather than genuine consent.[103] These linguistic barriers not only obstruct comprehension but also obscure the broader implications of data collection and sharing, particularly for individuals from different cultures and vastly different privacy norms.[104]

---

[99] *See* Miriam Ganslmeier, *Data Privacy For Migrants: Unrealistic or Simply Neglected?*, HEINRICH BÖLL STIFTUNG (Oct. 29, 2019), https://us.boell.org/en/2019/10/29/data-privacy-migrants-unrealistic-or-simply-neglected [https://perma.cc/3X9N-HFF9] (noting that refugees and asylum seekers often lack the information necessary to give meaningful consent to data collection and usage); *see* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE REFUGEE CASE PROCESSING AND SECURITY VETTING, DHS/USCIS/PIA-068, at 19 (July 21, 2017) (explaining that all applicants aged 14 and above must sign a consent form allowing USCIS to share their information with all departments and agencies involved in the adjudication and administration of the application).

[100] *See* Kaurin, *supra* note 15, at 10–12.

[101] *See* Ganslmeier, *supra* note 99.

[102] *Affirmative Asylum Applicants Must Provide Interpreters Starting Sept. 13*, U.S. CITIZENSHIP & IMMIGR. SERVS. NEWSROOM (Sept. 11, 2023), https://www.uscis.gov/newsroom/alerts/affirmative-asylum-applicants-must-provide-interpreters-starting-sept-13 [https://perma.cc/TUC9-RNSZ].

[103] *See* My Khanh Ngo & Noelle Smith, *The Government Denies People Access to Asylum Because of Language Barriers. We're Fighting Back.*, ACLU (Apr. 18, 2024), https://www.aclu.org/news/immigrants-rights/the-government-denies-people-access-to-asylum-because-of-language-barriers-were-fighting-back [https://perma.cc/V62M-TWXF]; Andrew Deck, *Seeking Asylum at the U.S.- Mexico Border? You'd Better Speak English or Spanish,* REST OF WORLD (June 1, 2023), https://restofworld.org/2023/migrant-languages-challenge-cbp-one-app-haitian-creole/ [https://perma.cc/NT8F-BYES].

[104] *See* Yao Li, *Cross-Cultural Privacy Differences*, *in* MODERN SOCIO-TECHNICAL PERSPECTIVES ON PRIVACY (Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes & Jennifer Romano eds., 2022) (explaining different cultural views on and approaches to privacy).

Fighting for survival, the (in)visible immigrant interacts with personal data-collecting authorities in the United States in a state of severe vulnerability. Their vulnerability subjects them to a condition that I dub "data surrender," as they are helpless and lack discretion and voluntariness. Daniel Solove observes that "[v]oluntariness is at the very foundation of the concept of consent, yet in practice, U.S. privacy law tolerates many situations in which people do not freely agree."[105] Indeed, "[t]oo many choices about privacy are so highly constrained and manipulated that they can hardly be considered voluntary."[106] This reality is particularly stark for asylum seekers and refugees who, in their pursuit of safety, have no choice but to comply with invasive data collection practices to access protection, legal status, or basic necessities.

Asylum seekers are especially choiceless concerning the kinds of information they must share. Of particular concern, immigration enforcement agencies collect and process "extraneous information" beyond what would be necessary to ensure their safety and provision of the best possible assistance to them.[107] Information that is beyond what would be necessary and disproportionate for assessing and processing an asylum claim falls in the extraneous information category, such as an applicant's religious beliefs, sexual orientation, or medical information beyond persecution-related trauma. With the disclosure of such extraneous information, the (in)visible immigrant is subjected to disproportionate surveillance, discrimination, misinformation, and threats of detention and deportation, at times, without due process.[108]

---

[105] Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law,* 104 B.U. L. REV. 593, 607 (2024) (explaining lack of voluntariness in accepting online terms of services).

[106] *Id.* at 607.

[107] This article adopts the term "excessive data collection" to refer to the collection and processing of information beyond what would be required to ensure safety of refugees and asylum seekers and to provide them with assistance. This includes highly sensitive information such as DNA, religious affiliation, sexual orientation and other personal details that extend beyond legitimate security and humanitarian needs. *See* Joan Friedland, *Information Vacuuming: Massive Collection of Data for Government's Surveillance and Deportation Machine*, NAT'L IMMIGR. L. CTR. (Aug. 22, 2018), https://www.nilc.org/2018/08/22/information-vacuuming-immigrants-and-citizens/ [https://archive.ph/kG4dD] (explaining that the Trump administration was collecting extensive, unfiltered data on immigrants to fuel surveillance); Melissa Del Bosque, *Many Asylum Seekers are Being Expelled, But Not Before Giving Up Their DNA*, BORDER CHRON. (Aug. 6, 2024), https://www.theborderchronicle.com/p/many-asylum-seekers-are-being-expelled [https://perma.cc/CG2C-RSUQ].

[108] Manish Singh, *Palantir's Software Was Used for Deportations, Documents Show*, TECHCRUNCH (May 3, 2019),

Significantly, non-citizens outside U.S. territory do not benefit from the protection of the Fourth Amendment, which guards against unreasonable and warrantless searches and seizures by the government.[109] As such, asylum seekers who were using CBP One (now CBP Home) app while still on the Mexico had no constitutional protection. The app's geolocation tracking features, combined with its data retention capabilities and CBP's ongoing surveillance practices, raised serious concerns about privacy violations and the potential for data misuse.[110] Its capabilities of access and tracking, particularly of asylum seekers within U.S. territory, arguably constitute an unwarranted and pervasive ongoing search, potentially violating reasonable expectations of privacy under the Fourth Amendment.[111] In *Carpenter v. United States,* the Supreme Court held that the government's acquisition of extensive historical geolocation data in the form of cell-cite location information (CSLI) from wireless carriers without a warrant constituted a Fourth Amendment (4A) violation.[112] The Court emphasized that the Fourth Amendment protects privacy interests in persons, houses, papers, and effects and recognized the intrusive nature of prolonged location tracking.[113] To this extent, the (in)visible immigrant, though physically present within the U.S. territory, is subjected to sustained digital surveillance through government apps like the CBP One (now CBP Home) and ought to be afforded comparable Fourth Amendment protections. However, in practice, immigration authorities often operate as though these constitutional safeguards do not apply, revealing a troubling disregard for the privacy rights of these "non-citizens". They are subjected to unprecedented digital surveillance at every stage of the immigration process and in accessing related benefits—by both government and private commercial actors.

---

https://techcrunch.com/2019/05/03/palantirs-software-was-used-for-deportations-documents-show/ [https://perma.cc/7R7V-4JPV]; Tonya Riley, *How a Private Company Helps ICE Track Migrants' Every Move*, CYBERSCOOP (Sept. 26, 2023), https://cyberscoop.com/ice-bi-smartlink/ [https://perma.cc/BF9R-A7PM].

[109] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990).

[110] *See* Elec. Priv. Info. Ctr., Comments to CBP and OMB on CBP One Expansion for Biometric Exit, (Apr. 26, 2024), https://epic.org/documents/epic-comments-to-cbp-and-omb-on-cbp-one-expansion-for-biometric-exit/ [https://archive.ph/h60n4].

[111] U.S. CONST. amend. IV (protecting individuals against unreasonable searches and seizures); Katz v. United States, 389 U.S. 347, 361 (1967) (establishing the "reasonable expectation of privacy" standard under the Fourth Amendment).

[112] 585 U.S. 296 (2018).

[113] *Id.*; U.S. CONST. amend. IV.

II. THE SURVEILLANCE GAZE ON THE (IN)VISIBLE IMMIGRANT

Privacy is fundamental in the preservation of an individual's identity and agency; accordingly, the right to privacy should be protected regardless of one's citizenship or individual's socioeconomic condition. In this Part, I begin by examining how intersecting factors—such as gender, race, religion, ethnicity, and class—shape the (in)visible immigrant's experience within the data cycle.[114] Of particular interest is how these overlapping identities influence their exposure to pervasive surveillance and the resulting privacy violations. Today, the majority of immigrants belong to intersecting marginalized groups.[115] Many are Black or Brown, and most are non-European people of color, low-income individuals, and religious minorities—demographics that, within the United States, are disproportionately targeted by digital surveillance and suffer the attendant harms of privacy intrusions.[116]

The convergence of intersecting identities—including race—amplifies the disproportionate impact of discriminatory surveillance.[117] The majority of the immigrants are racial

---

[114] All these factors form the broader discussion on intersectionality. *See* PATRICIA HILL COLLINS, INTERSECTIONALITY AS CRITICAL SOCIAL THEORY 157–88 (2019); Kimberlé Crenshaw, *Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color*, 43 STAN. L. REV. 1241, 1244 (1991) (examining the intersection of race and gender in shaping social economic structures).

[115] *See* Kevin R. Johnson, *The Intersection of Race and Class in U.S Immigration Law and Enforcement*, 72 L. & CONTEMP. PROBS. 1, 4–13 (2009); NICOLE WARD & JEANNE BATALOVA, MIGRATION POL'Y INST., REFUGEES AND ASYLEES IN THE UNITED STATES 5 (2023), https://www.migrationpolicy.org/sites/default/files/publications/SPT-Refugees2023-PRINT-final.pdf [https://perma.cc/D98H-PGK6] (reporting that "[i]n the first eight months of FY 2023, 43 percent of admitted refugees were from Africa, 28 percent from the Middle East and South Asia, 13 percent from East Asia, 11 percent from Latin America and the Caribbean, and 4 percent from Europe and Central Asia"); Chao, et al., *supra* note 22, at 11, 14–15 (explaining the disproportionate prevalence of surveillance against immigrants and other marginalized groups); Kevin R. Johnson, *The End of "Civil Rights" as We Know It?: Immigration and Civil Rights in the New Millennium,* 49 UCLA L. REV. 1481, 1485 (2002) (observing that people of color constitute the majority of the population of both legal and illegal immigrants).

[116] *See* WARD & BATALOVA, *supra* note 115, at 9–10.

[117] *See, e.g.*, I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1272 (2017) (noting the disproportionate concentration of CCTV cameras in communities predominantly inhabited by racial minorities).

minorities.[118] They are often fleeing severe deprivation, natural disasters, and injustice in their countries of origin, only to encounter new forms of structural marginalization and exploitation—now digitally configured upon arrival. Already vulnerable by default, some may belong to economically disadvantaged classes, which compels them to seek government assistance.[119] Many require immediate support for housing and health care upon arrival in the United States.[120] Yet, accessing these essential services inevitably subjects them to additional layers of data collection and surveillance.

Surveillance as a policing and control mechanism exercised by the state disproportionately affects those with intersecting marginalized identities.[121] Immigrants of color, whose experiences are shaped by such intersecting identities, are especially impacted by exclusionary policies, practices, and enforcement in the U.S.[122] In addition to facing significant hurdles in regularizing their legal status, they are frequently subjected to racial profiling, despite its formal disapproval in conventional law enforcement practices.[123] As

---

[118] *See* Shannon Schumacher, Liz Hamel, Samantha Artiga, Drishti Pillai, Ashley Kirzinger, Audrey Kearney, Marley Presiado, Ana Gonzalez-Barrera & Mollyann Brodie, *Understanding the U.S. Immigrant Experience: The 2023 KFF/LA Times Survey of Immigrants*, KFF (Sept. 17, 2023), https://www.kff.org/report-section/understanding-the-u-s-immigrant-experience-the-2023-kff-la-times-survey-of-immigrants-findings/ [https://perma.cc/4M49-FYM2] (reporting that most immigrants in the U.S. identify as people of color).

[119] *See* Ali Noorani, *Race, Class, and the Emergence of an Immigrant Rights Movement*, 31 FLETCHER F. WORLD AFFS. 185, 185–89, 192–93 (2007) (examining the impact of race and class on immigrant rights).

[120] *See* KRISTA M. PEREIRA, ROBERT CROSNOE, KARINA FORTUNY, JUAN MANUEL PEDROZA, KJERSTI ULVESTAD, CHRISTINA WEILAND, AND HIROKAZU YOSHIKAWA & AJAY CHAUDRY, U.S. DEP'T OF HEALTH & HUM. SERVS. OFF. OF THE ASSISTANT SEC'Y FOR PLAN. & EVALUATION, BARRIERS TO IMMIGRANTS' ACCESS TO HEALTH AND HUMAN SERVICES PROGRAMS (May 2012), https://aspe.hhs.gov/reports/barriers-immigrants-access-health-human-services-programs-0 [https://perma.cc/QMR5-KN5T]; BRIDGES, *supra* note 8, at 5–16, 67 (illustrating privacy violations of poor mothers reliant on government welfare programs).

[121] *See* Frank Rudy Cooper, *Intersectionality, Police Excessive Force, and Class,* 89 GEO. WASH. L. REV. 1452, 1490–1503 (2021).

[122] *See* Kevin R. Johnson, *Race, The Immigration Laws, and Domestic Race Relations: A "Magic Mirror" into the Heart of Darkness,* 73 IND. L.J. 1111, 1131–36 (1998) (explaining the exclusionary practices, including targeted deportation against people of color).

[123] *See* Charles Kamasaki, *U.S. Immigration Policy: A Classic, Unappreciated Example of Structural Racism*, BROOKINGS (Mar. 26, 2021), https://www.brookings.edu/articles/us-immigration-policy-a-classic-unappreciated-example-of-structural-racism/ [https://perma.cc/8TPV-

a result, they are disproportionately targeted and surveilled—and often mistakenly and unlawfully deported.[124] Long-established patterns of discriminatory enforcement helped lay the foundation for the digital surveillance state.

Building upon this systematic surveillance apparatus, the fusion of the government and private surveillance regimes has subjected the (in)visible immigrant to persistent disproportionate surveillance and privacy violations throughout their immigration process. U.S. law grants expansive authority to the government over all immigrants, whether they are held in physical detention facilities or monitored electronically.[125] To exercise this authority, ICE contracts private firms to operate detention centers and assigns them to manage electronic monitoring of immigrants under the ATD program.[126] The immigration control technologies developed and deployed by these private actors rely heavily on the collection and use of personal data. Often, the immigrants' information is sold to third parties without consent, further eroding individual privacy.[127] These companies scramble for personal information not only for use in immigration control and enforcement but also for their own commercial purposes.

LS5Z] (reporting that the immigration system treats immigrants differently depending on their race); *see also* TEX. CODE CRIM. PROC. ANN. art. 2B.0052 (West 2023) (outlawing racial profiling, which suggests that profiling continues).

[124] Erica Bryant, *The Immigration System is Racist; Solutions Exist*, VERA (Aug. 16, 2023), https://www.vera.org/news/the-immigration-system-is-racist-solutions-exist [https://perma.cc/JKX8-LHJD] (reporting that Black immigrants are targeted by immigration enforcement).

[125] 8 U.S.C. § 1103 (empowering the federal government, particularly CBP, to manage immigration, which includes detaining immigrants who violate immigration law).

[126] *See* Eunice Hyunhye Cho, *More of the Same: Private Prison Corporations and Immigration Detention under the Biden Administration*, ACLU (Oct. 5, 2021), https://www.aclu.org/news/immigrants-rights/more-of-the-same-private-prison-corporations-and-immigration-detention-under-the-biden-administration **[**https://perma.cc/7K82-K9AF**];** *see also The GEO Group Announces Five-Year Contract with U.S. Immigration and Customs Enforcement for Intensive Supervision and Appearances Program (ISAP),* BUSINESS WIRE (Mar. 24, 2020), https://www.businesswire.com/news/home/20200324005145/en/The-GEO-Group-Announces-Five-Year-Contract-With-U.S.-Immigration-and-Customs-Enforcement-for-Intensive-Supervision-and-Appearance-Program-ISAP [https://archive.ph/4iRy2].

[127] Sebastian K. Skelton, *LexisNexis Sued by Immigration Advocates over Data Practices*, COMPUTERWEEKLY (May 12, 2022), https://www.computerweekly.com/news/252523969/LexisNexis-sued-by-immigration-advocates-over-data-practices [https://perma.cc/Q5RN-YEYF].

A. THRUST UNDER THE "IMMIGRATION SURVEILLANCE STATE"

Refugees and asylum seekers are subject to surveillance from the time of their first interaction with U.S. immigration authorities until they either leave the country or are granted permanent status.[128] Anil Kalhan characterizes the significant expansion of surveillance in federal immigration enforcement, coupled with substantial investment in building the digital monitoring infrastructure, as the embodiment of the "immigration surveillance state."[129] He describes aspects of this enforcement as a form of "immigration surveillance" in four essential immigration processes and functions: identification, screening and authorization, mobility tracking and control, and information sharing.[130] In all these processes, immigrants have their biographic, biometric, and other pertinent data extensively collected, analyzed, stored, and disseminated among government agencies.

Refugees and asylum seekers are uniquely vulnerable to pervasive immigration surveillance due to their precarious circumstances. This creates a significant power imbalance between them and immigration authorities, who are often viewed as their hope for refuge and safety. This imbalance is further exacerbated by an acute information-decision gap and the absence of robust privacy laws that specifically safeguard their data. With this, the immigration surveillance state emerges from widespread tracking of these individuals not only at the border but also within U.S. boundaries.[131] Despite privacy and surveillance concerns, immigration authorities routinely collect extraneous biographic and biometric data from refugees and asylum seekers.[132]

---

[128] *See* Jake Wiener, *New ICE Privacy Impact Assessment Shows All the Ways the Agency Fails to Protect Immigrants' Privacy*, ELEC. PRIV. INFO. CTR. (Apr. 20, 2023), https://epic.org/new-ice-privacy-impact-assessment-shows-all-the-way-the-agency-fails-to-protect-immigrants-privacy/ [https://archive.ph/7ePRi].

[129] Kalhan, *Immigration Surveillance*, *supra* note 9, at 1–9.

[130] *Id.* at 41.

[131] Elec. Priv. Info. Ctr., Comments of the Electronic Privacy Information Center, Center for Digital Democracy, and Consumer Federation of America on Proposed Rulemaking re Cybersecurity Audits, Risk Assessments, and Automated Decision Making (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/ [https://archive.ph/ykDXU] (noting that biometric surveillance expansion extends monitoring beyond border points into the interior, increasing surveillance of immigrants).

[132] Astha Kapoor, Suha Mohamed & Shefali Girish, *Exploring the*

Surveillance concerns are further compounded by collaboration with foreign governments and states to share immigrants' biographic and biometric data.[133] The shared information is frequently exploited to identify individuals deemed as threats to their home governments, who are then surveilled and targeted for transnational repression within the U.S. borders.[134] These governments can and do exploit shared information for persecution, coercion, and silencing of refugees and asylum seekers.[135]

U.S. immigration authorities are emboldened by the Supreme Court's jurisprudence, which has consistently upheld the government's broad authority over immigration. In *Chae Chan v. United States* (the *Chinese Exclusion Case*), the Court affirmed Congress' plenary power to exclude noncitizens, even those previously admitted, as an inherent aspect of national sovereignty.[136] This decision laid the foundation for the deferential judicial treatment of federal immigration policies, with the effect of the government's virtually unchecked discretion in determining who can enter and remain in the country. Similarly, in *Kleindeinst v. Mandel,* the Court reinforced this principle by ruling that the executive may deny entry to a foreign national on ideological grounds, so long as it provides a facially legitimate and bona fide reason, with courts generally deferring to such determinations.[137] In *United States v. Martinez-Fuerte*, it upheld the constitutionality of immigrant checkpoints, allowing the government's broad authority to stop and question individuals about their immigration status without individualized suspicion, reasoning that such stops were minimally intrusive and justified by the government's interest in the controll

---

Potential of Data Stewardship in the Migration Space, GMF (July 8, 2022), https://www.gmfus.org/news/exploring-potential-data-stewardship-migration-space [https://perma.cc/FQF3-XW6U] (explaining the different data sources that contribute to immigrants' data points).

[133] U.S. DEP'T OF HOMELAND SEC., *supra* note 80 (detailing the memorandum for data sharing between DHS and the United Nations High Commissioner for Refugees (UNHCR)).

[134] *See* Kyaw Zwar Tun v. U.S. Immigr. & Naturalization Serv., 445 F.3d 554, 569–71 (2d Cir. 2006) (presenting evidence of the Burmese government's surveillance of dissidents in the U.S.).

[135] *See* FREEDOM HOUSE, UNSAFE IN AMERICA: TRANSNATIONAL REPRESSION IN THE UNITED STATES, https://freedomhouse.org/sites/default/files/2022-05/TransnationalRepressionReport2022_CaseStudy_United_States_NEW.pdf [https://perma.cc/P7NW-SDN5] (2022) (reporting Saudi Arabia, China, Egypt, and Russia surveil, stalk, and plot to harm their diaspora communities in the U.S. physically).

[136] 130 U.S. 581, 603–04 (1889).

[137] 408 U.S. 753, 769–70 (1972).

and enforcement of immigration.[138] Furthermore, in *United States v. Flores-Montano*, the Court reaffirmed the government's authority to conduct routine searches at the border without a warrant or individualized suspicion, distinguishing them from more intrusive searches that would require greater justification.[139] These cases, among others, illustrate the broad discretion immigration authorities wield in enforcing admission and exclusion rules—discretion that has only deepened with the increased use of digital technologies in immigration enforcement.

Refugees and asylum seekers enjoy some freedoms in the U.S., but they remain subordinate. Even when granted permanent resident status, the retention period of their personal information is unreasonably long, effectively subjecting them to a lifetime of disproportionate surveillance.[140] For the defensive application, there is increased digitization of immigration enforcement and surveillance. ICE closely surveils individuals undergoing removal proceedings or those under the ATD program.[141] While Kalhan's observations on the immigration surveillance state apply broadly to all non-citizens,[142] refugees and asylum seekers are particularly vulnerable within this state due to their need for regularizing their immigration status and acute reliance on government assistance for housing, health care, education, and other social services. These subject them to increased data collection and eventual surveillance.

B. THRUST UNDER COMMERCIAL SURVEILLANCE

The immigration surveillance state is supplemented by commercial surveillance. Online commercial entities are persistently seeking refugees' and asylum seekers' data for exploitation and commercial surveillance.[143] This creates a state that I call "double surveillance," where both government and private commercial entities engage in a relentless scramble for data from refugees and asylum seekers for surveillance. While all immigrant categories and citizens are often subjected to some level of double surveillance,

---

[138] 428 U.S. 543, 562 (1976).

[139] 541 U.S. 149, 152 (2004).

[140] *See* Elec. Priv. Info. Ctr., *supra* note 110 (detailing the data retention policies for non-citizens, including personal data retention for up to 75 years).

[141] U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104529, ALTERNATIVE TO DETENTION: ICE NEEDS TO BETTER ASSESS PROGRAM PERFORMANCE AND IMPROVE CONTRACT OVERSIGHT 17–23 (2022), https://www.gao.gov/assets/gao-22-104529.pdf [https://perma.cc/8W6S-8D3W].

[142] Kalhan, *Immigration Surveillance*, *supra* note 9, at 1–9.

[143] *See* Chao, et al., *supra* note 22, at 5, 8.

refugees and asylum seekers are especially vulnerable to double surveillance because of excessive data collection resulting from their inherent vulnerability. DHS contracts and partners with private commercial entities in its data collection and surveillance efforts on asylum seekers. For example, in 2022, it was reported that for over nineteen years, ICE contracted with Thomson Reuters, a private data broker, and other private data aggregating entities with the capability to access state DMV databases and utility providers such as gas, water, electricity, and phone services.[144] These private entities share their personal information with ICE, enabling the deportation of individuals without public or judicial oversight.[145] Additionally, DHS contracts private, for-profit entities to manage the electronic monitoring of asylum seekers under the ATD program and physical detention facilities, exposing them to increased digital surveillance.[146] Beyond selling the data to immigration agencies, these for-profit entities also sell the data to any willing buyer without consideration for the data subjects' privacy interests.[147] The collaboration between government and for-profit entities in collecting data and surveilling asylum seekers—through contractual arrangements lacking meaningful oversight and accountability—raises privacy concerns. This unchecked data trade exposes them to risks such as identity theft, exploitation by bad actors, and even transnational repression, as authoritarian regimes may acquire such data to target dissidents abroad. Marginalized groups, including refugees and asylum seekers, are more vulnerable to systemic scrutiny, data exploitation, and persistent tracking by both government and private entities.[148] Their intersectional identities also

---

[144] *See* WANG, ET AL., *supra* note 5, at 3–5.

[145] *Id.* at 4.

[146] *See* Ingrid Eagly & Steven Shafer, *Detained Immigration Courts*, 110 VA. L. REV. 691, 695 (2024); AM. IMMIGR. COUNCIL, ALTERNATIVES TO IMMIGRATION DETENTION: AN OVERVIEW 1–2 (2023), https://www.americanimmigrationcouncil.org/research/alternatives-immigration-detention-overview [https://perma.cc/R684-GNFV].

[147] *See* Aaron X. Sobel, *End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem*, 42 YALE L. & POL'Y REV. 176, 179–82, 207 (2023) (explaining the sale of personal data not only to government agencies but also to private entities).

[148] *See* Kiran Wattamwar, *ICE's Privacy Impact Assessment on Surveillance Technologies is an Exercise in Disregarding Reality*, ELEC. PRIV. INFO. CTR. (Oct. 5, 2023), https://epic.org/ices-privacy-impact-assessment-on-surveillance-technologies-is-an-exercise-in-disregarding-reality/ [https://archive.ph/oUVoz]; Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color,* BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-

heighten the risk of disproportionate targeted commercial surveillance.[149]

Refugees and asylum seekers actively participate in the digital economy by purchasing essential goods and services online. Their experience in the digital economy mirrors that of other marginalized populations who are disproportionately subjected to exploitative data practices, including commercial surveillance. Scholar Shoshana Zuboff describes commercial surveillance as collecting, analyzing, and profiting from information about people in the digital age for profit, which she labels "surveillance capitalism."[150] She contends that high-tech commercial entities amass assets and capital by controlling them without adequate consent.[151] Illustrating how one marginalized community, among others, is exploited within this surveillance web, Anita Allen developed a three-fold framework to expose the overly attentive and discriminatory system that targets African Americans in the online commercial space, which she calls the "Black Opticon."[152] The Black Opticon demonstrates susceptibility to "discriminatory over-surveillance, discriminatory exclusion, and discriminatory predation."[153] The depiction in the Black Opticon offers a striking reflection of the immigrants' experience in the digital economy. First, Black Americans face discriminatory over-surveillance, a condition she explains by using Jeremy Bentham's concept of efficient institutional surveillance, "panopticon."[154] Second, she asserts that they confront discriminatory exclusion, termed a "ban-opticon" (after Didier Bigo), and describes a society that permits the use of personal data to target marginalized groups for exclusion from opportunity, pushing their legitimate interests to the wayside and making them

---

recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/YB9M-7XBH].

[149] *See Letter: 30+ Civil Rights Organizations Call on FTC Chair Khan to Put Privacy Protections in Place*, FIGHT FOR THE FUTURE (June 12, 2024), https://www.fightforthefuture.org/news/2024-06-12-letter-30-civil-rights-organizations-call-on-ftc-chair-khan-to-put-privacy-protections-in-place/ [https://perma.cc/N3HB-7TK6] (highlighting that ShotSpotter and similar gun detection companies disproportionately install devices in Black and Brown communities, primarily to surveil residents and collect extensive data).

[150] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[151] *Id.* at 64–65, 99–100.

[152] *See* Allen, *supra* note 8, at 907, 913, 921–24.

[153] *Id.*

[154] *Id.* at 913–21.

invisible to society.[155] Thirdly, they deal with discriminatory predation, a condition she describes as a "con-opticon," a society that enables financial exploitation, targeting and exploiting marginalized groups with deceptive and predatory practices such as con jobs of consumer scams, fraud, and deceit.[156]

I adopt Allen's "Black Opticon" framework to illuminate the experience of refugees and asylum seekers in the digital economy. The metaphor, which highlights the urgent privacy and data-protection challenges facing African Americans, similarly applies to refugees, asylum seekers, and other groups. [157] An "Immigrant Opticon," so to speak, can be used to illustrate how refugees and asylum seekers are surveilled, excluded, and preyed upon through commercial surveillance. Their intersecting identities, particularly as the majority belong to historically marginalized groups, make them especially vulnerable to commercial exploitation. Data brokers collect and aggregate information on the (in)visible immigrant by tracking various data points, including browsing history, purchasing patterns, geographic locations, and other intimate details, which are then used to profile them.[158] For example, Palantir Technologies and Thomson Reuters use covert surveillance techniques to profile and monitor virtually every facet of these individuals' online activities.[159] These firms collect immigrant location data, search history, social

---

[155] *Id.* at 921–25.

[156] *Id.* at 917.

[157] *Cf.* Manning & Stumpf, *supra* note 93, at 415.

[158] *See* JUSTIN SHERMAN, DUKE UNIV. SANFORD CYBER POL'Y PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS 3–5 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/9UWG-VH2N] (detailing how data brokers compile sensitive personal data, including real-time location and consumer behavior, which can be used to profile individuals, including immigrants); ELEC. PRIV. INFO. CTR., HOW DATA BROKERS HARM IMMIGRANTS (2024), https://epic.org/wp-content/uploads/2024/10/Data-Broker-Harms-to-Immigrants-One-Pager-1.pdf [https://perma.cc/2CYZ-FAWZ] (detailing the list of personal information collected by data brokers and the associated risks of targeting and surveillance); *see also* NAT'L ASS'N OF CRIM. DEF. LAWS., THE DATA BROKER LOOPHOLE IS BEING EXPLOITED TO TARGET IMMIGRANT COMMUNITIES (2023), https://www.nacdl.org/getattachment/567b4c71-b702-47d7-a59c-1e42f39b065a/immigration-and-data-purchases.pdf [https://perma.cc/L2S4-M3JK] (describing how immigration enforcement agencies purchase data from brokers to track and detain immigrants, circumventing sanctuary laws and traditional oversight mechanisms).

[159] MIJENTE, IMMIGRANT DEF. PROJECT & THE NAT'L IMMIGR. PROJECT OF THE NAT'L LAWS. GUILD, WHO'S BEHIND ICE? THE TECH AND DATA COMPANIES FUELING DEPORTATIONS (2018).

media connections, and individual languages to build profiles that flag and exclude them from opportunities.[160] They are often targets of digital predatory practices that exploit their vulnerability, for example, charging them high insurance premiums.[161] Their profiles are used to exclude them from housing in specific zip code areas, access to affordable credit, and from employment opportunities through automated flagging and screening algorithms.[162]

In 2023, DOJ, through its Immigrant and Employee Rights Section, sued SpaceX, alleging discrimination against refugees and asylees through its hiring process from at least September 2018 to May 2022 in violation of the INA.[163] The complaint further alleged that SpaceX, among other things, discouraged applications and denied employment opportunities to qualified candidates based on their citizenship status.[164] Such exclusion from job opportunities by SpaceX, along with the effective imposition of a hiring ban on noncitizens regardless of their qualifications, exemplifies the ban-opticon as articulated by Allen's work.[165] Dropping the lawsuit was among DOJ's first actions under the second Trump administration, suggesting that such practices will continue unpoliced for at least the next four years.[166]

Regarding discriminatory predation (the "con-opticon"), refugees and asylum seekers are frequently preyed upon and targeted by online manipulations.[167] Allen describes this as "predatory

---

[160] *Id.* at 1, 56–59.

[161] *See* Leah Zallman, Steffie Woolhandler, Sharon Touw, David U. Himmelstein & Karen E. Finnegan, *Immigrants Pay More in Private Insurance Premiums Than They Receive In Benefits*, 37 HEALTH AFFS. 1663 (2018).

[162] *See* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 3–14 (2016) (detailing leveraging technology to inform decision-making in housing, education, and insurance); *see also* Mekonnen Firew Ayano, *Tenants Without Rights: Situating the Experiences of New Immigrants in the U.S. Low-Income Housing Market,* 28 GEO. J. ON. POVERTY L. & POL'Y 159, 159–61, 168, 178, 183 (2021).

See Complaint at 1–4, United States v. Space Expl. Techs. Corp., OCAHO Case No. 2023B00082 (Aug. 24, 2023), https://www.justice.gov/archives/opa/file/1311656/dl?inline [https://archive.ph/61AG0].

[164] *Id.* at 1–11.

[165] *See* Allen, *supra* note 8, at 921.

[166] *See DOJ drops lawsuit against SpaceX for discriminatory hiring practices against immigrants*, IMMIGR. POL'Y TRACKING PROJECT (Feb 24, 2025), https://immpolicytracking.org/policies/doj-drops-case-against-spacex-for-discriminatory-hiring-practices-against-immigrants/ [https://perma.cc/ND44-A92G].

[167] *See* Juan Manuel Pedroza, Anne Schaufele, Viviana Jimenez,

surveillance," the inverse of "exclusionary surveillance."[168] Cybercriminals leverage the refugees' and asylum seekers' vulnerability in the data lifecycle and target them with telemarketing scams.[169] Online scammers often pose as USCIS officers or ICE agents, using threats to extract personal information, a typical example of predation.[170] They contact victims through phone calls, emails, and in-person visits, falsely claiming to resolve issues with the victim's immigration status. They then offer to fix the problem for a fee, exploiting the victim's fear of deportation and urgency to rectify their status.[171] Under duress and fearing severe consequences, they often provide personal information such as passports and alien numbers.[172] While some lose money to these online scams, others report living under constant fear of potential future harm.[173]

C. CONSEQUENCES OF THE SURVEILLANCE GAZE

The (in)visible immigrant's vulnerability often forces them into a state of resignation—a diminished sense of identity, leaving them susceptible to exploitation and other dire consequences. With each successive interaction with immigration authorities, they become increasingly ensnared in the watchful gaze of both the state and commercial entities, exposing them to over-surveillance, exclusion, and predation. This raises a critical question: what happens when authorities embark on an overdrive of collecting extraneous information? To answer this question, I delineate the multifaceted impacts of such data collection by theorizing that refugees and asylum seekers experience three distinct but related forms of diminished privacy: (1) data surrender—the yielding of information prompted by the overwhelming need of the powerless to survive; (2) personality curation—the undue self-discipline, subordination, loss of self-esteem and erasure of personal identity

---

Melissa Garcia Carrillo & Dennise Onchi-Molin, *Insurgent Citizenship: How Consumer Complaints on Immigration Scams Inform Justice and Prevention Efforts*, 37 GEO. IMMIGR. L.J. 369, 372, 384–85 (2023).

[168] *See* Allen, *supra* note 8, at 925.

[169] *See Immigrants May Be Targets for Cybercriminals: What You Need to Know*, BROWNWINICK L. FIRM (Mar. 22, 2022), https://www.brownwinick.com/insights/immigrants-may-be-targets-for-cybercriminals-what-you-need-to-know [https://perma.cc/3JE9-3ZAS].

[170] *Avoid Payment Scams: USCIS Does Not Accept Fees by Phone or Email*, U.S. CITIZENSHIP & IMMIGR. SERVS. (Aug. 24, 2016), https://www.uscis.gov/archive/avoid-payment-scams-uscis-does-not-accept-fees-by-phone-or-email [https://perma.cc/H6HA-GYZX].

[171] *Id.*

[172] *See* Pedroza et al., *supra* note 167, at 383.

[173] *Id.*

and history prompted by the need to appear acceptable to authorities; and (3) weaponization of personal information—the harmful use of data obtained through coercion, vulnerability, or unequal power dynamics.

1. *Data Surrender*

While the digital age offers many opportunities and connections, it creates a perilous tightrope for refugees and asylum seekers. Digital technology provides access to information and communication and facilitates the distribution of essential aid to refugees and asylum seekers, but demands a constant surrender of "self" through data surrender—a steep price for basic survival.[174] Data surrender entails not only the loss of personal information but also relinquishing control over one's identity and personal narrative due to the overwhelming need for survival.[175] I refer to this as "yielding and inescapable surrender." For refugees and asylum seekers, yielding and inescapable surrender go beyond the act of giving and sharing the data. It is a complex and often compelled transaction, a desperate exchange in which agency and autonomy are surrendered for the necessities of life.[176] Unlike other individuals who navigate the digital realm with some semblance of choice and consent, refugees and asylum seekers face harsh circumstances that force them to yield to the dictates of surveillance without choice and consent.[177] They are forced into a state of inescapable surrender, driven by the imperative to ensure their survival and that of their families.[178] To them, the currency is surrendered privacy, with which they purchase the provision of food, protection, a roof over their

---

[174] *See* Amanda Alencar, *Technology Can Be Transformative for Refugees, but It Can Also Hold Them Back*, MIGRATION POL'Y INST. (July 27, 2023), https://www.migrationpolicy.org/article/digital-technology-refugees [https://perma.cc/S7BG-TFXV] (highlighting technology that enables refugees to gather information and humanitarian agencies to provide essential services).

[175] *See* Bas Verplanken & Jie Sui, *Habit and Identity: Behavioral, Cognitive, Affective, and Motivational Facets of an Integrated Self,* 10 FRONTIERS PSYCH. 1, 2 (2019) (explaining personal or self-identities, including mental representations individuals hold about themselves detailed in biographic memories, self-attributions, beliefs, motivations, recurrent thoughts, emotions, and self-perceptions).

[176] *See* Kaurin, *supra* note 15, at 2.

[177] *See* Ganslmeier, *supra* note 99 (explaining how refugees and asylum seekers often lack meaningful consent in digital surveillance, as their circumstances compel them to comply with involuntary data collection due to circumstances beyond their control).

[178] *See* Kaurin, *supra* note 15, at 2.

heads, and access to medical care. The result of this "transaction" is constant surveillance, which instills anxiety, forced loyalty, and exhaustion with the potential for even more adverse harm.

By collecting extraneous data and subjecting desperate and vulnerable individuals to constant surveillance, authorities strip refugees and asylum seekers of agency and autonomy.[179] This yielding illustrates the complex and strained techno-social landscape in which individuals are left with no choice but to relinquish their privacy rights. It creates a complex dynamic where the outcome is that "one's safety is secured at the cost of blind submission," which is a typical example of data surrender.

Refugees and asylum seekers often resign to a state of powerlessness over personal information, even when it is detrimental to their interests.[180] While their privacy needs are as valid as those of the general population, to them, the need for survival overtakes the privacy needs.[181] Though concerned about identity theft and related consequences of data breaches and misuse, they feel powerless and are unable to object or question excessive data collection. For them, yielding to demands for data collection is not an option but a necessity for survival.[182] Authorities must be sensitive to this reality while balancing privacy with national security. The effect of data surrender is a system that undermines an equitable society that gives refugees and asylum seekers meaningful control over their privacy as they seek to regularize their legal stay in the U.S.

2. *Curation of Person*

The ability to curate the personalities others observe is one of the hallmarks of privacy. Personal curation involves an individual's efforts to select personal disclosures and concealments carefully.[183]

---

[179] *Id.* at 10–13.

[180] *Id.* at 15; MOLNAR, *supra* note 21, at 141–43 (explaining how refugees and asylum seekers must choose between food and their fingerprints and highlighting their difficult tradeoff between survival and privacy).

[181] *See* Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama & Florian Schaub, *Keeping a Low Profile? Technology, Risk, and Privacy Among Undocumented Immigrants*, *in* PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1, 6 (2018).

[182] See *infra* pp. 40–49 for a discussion on weaponization.

[183] I define curation of person as a deliberate process by which an individual selects and presents specific information about themselves while intentionally concealing aspects of their true self and character. The concept is inspired by the practices of curating art in exhibitions and museums, where the curator selects the "best" items and pieces for display relative to

Curation of self-presentation may result in undue self-discipline, undue subordination, loss of self-esteem, and erasure of identity and personal historical accounts. In many respects, a curated person is a subdued individual. Highly self-conscious and even inauthentic self-curation is an understandable result of fear that information provided to others will adversely affect chances of a positive outcome. This is an everyday reality for refugees and asylum seekers awaiting immigration decisions in a surveillance state. The U.S. immigration and security agencies are deeply engaged in the surveillance of refugees and asylum seekers.[184]

The actual or perceived reality that an individual is being watched compels them to curate their actions and conform. People are prone to making some choices even when they contradict their beliefs and value systems.[185] The (in)visible immigrants' vulnerability inevitably forces them to modify their behavior and actions to appear generally desirable to the authorities at the expense of distorting their true identity.[186] Every individual is endowed with capabilities of reason and self-control, as well as strengths and weaknesses.[187] When these faculties and interests are manipulated or suppressed, it can undermine their autonomy, selfhood, and moral agency, ultimately distorting an individual's true identity.[188]

---

a theme or goal. The (in)visible immigrant carefully curates their behavior and identity to fit the expectations of those watching them. *Cf.* Lisa R. Johnston, Jacob Carlson, Cynthia Hudson-Vitale, Heidi Imker, Wendy Kozlowski, Robert Olendorf & Claire Stewart, *How Important are Data Curation Activities to Researchers? Gaps and Opportunities for Academic Libraries*, 6 J. LIBR. & SCHOLARLY COMMC'N 1, 3–5 (2018) (explaining curation as entailing the sorting and organizing of data to guarantee its accuracy, relevance, and accessibility for research applications). *See generally* Lindsay Persohn*, Curation as Methodology*, 21 QUALITATIVE RSCH. 20 (2021).

[184] Letter from Sen. Roy Wyden to Hon. Joseph V. Cuffari, Inspector Gen. of the U.S. Dep't of Homeland Sec. (Mar. 8, 2022), https://www.wyden.senate.gov/imo/media/doc/DHS%2520IG%2520ICE_HSI%2520data%2520complaint%25 [https://perma.cc/P7KX-ZCAL] (revealing that DHS illegally directed Western Union to provide transaction records of immigrants).

[185] *See, e.g.*, Roser Cañigueral & Antonia F. de C. Hamilton, *Being Watched: Effects of an Audience on Eye Gaze and Prosocial Behaviour,* 195 ACTA PSYCHOLOGICA 50, 62 (2019), https://doi.org/10.1016/j.actpsy.2019.02.002.

[186] *Id.* at 61–62.

[187] DIANA T. MEYERS, INALIENABLE RIGHTS: A DEFENSE 185 (1986).

[188] Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. 1, 9–11 (2019), https://doi.org/10.14763/2019.2.1410 (arguing that technological manipulation threatens individual autonomy by covertly shaping decision-

We are all subject to the pressures of curation of person, but these pressures are an outsized problem for refugees and asylum seekers. For instance, consider Henry A. Grunwald, an Austrian-born American who, at seventeen, migrated to the U.S. as a refugee with his family. He became a diplomat and a famous journalist, serving as managing editor of Time Magazine and editor-in-chief of Time Inc. Despite his success, Grunwald struggled with the pressures of personal curation, as vividly depicted in his essay *Home is Where You Are Happy*.[189] In this essay, he states, "[e]very immigrant leads a double life. Every immigrant has a double identity and a double vision, suspended between an old and a new home, an old and a new self."[190]

Grunwald's reflection highlights the multifaceted struggle and adaptation process the (in)visible immigrant undergoes as they try to integrate into the new American society. Grunwald's 1985 essay reflects his personal curation experience beginning in 1940 when his family arrived as refugees. It is important to note that his curation depiction is of an era with far less advanced or intrusive technology than we have today, making the current refugees' and asylum seekers' curation experience even more dire. Furthermore, he discusses dual identities and the adoption of new cultural norms while maintaining one's original cultural values, underscoring the complex reality of living between two worlds with the pressure to assimilate. His portrayal illustrates the implicit coercion that results in change, such as the struggle to learn a new language and have an accent, and pressure to adopt the new culture, such as addressing superiors by their first names.[191] These are all representations of curation of person.

The intersectional (in)visible immigrant of color faces heightened exclusion, as they are perceived as foreigners both literally and figuratively in addition to belonging to a minority group.[192] Their reality involves constant discriminatory surveillance that forces them to present a curated version of themselves frequently. They must continuously strive to conform to and perform the identity expected of them by the observing authorities while striving to stay true to their identity, culture, and preserving their

---

making and suppressing self-determination).

[189] Henry H. Grunwald, *Essay: Home is Where you are Happy*, TIME, July 8, 1985, https://time.com/archive/6704398/essay-home-is-where-you-are-happy/ [https://perma.cc/5FXE-SDAY].

[190] *Id.* at 1.

[191] *Id.*

[192] *See* Berta Esperanza Hernández-Truyol, *Natives, Newcomers and Nativism: A Human Rights Model for the Twenty-First Century,* 23 FORDHAM URB. L.J. 1075, 1075–76 (1996); Nicol Turner Lee & Caitlin Chin-Rothmann, *supra* note 148.

personal history. Intersectional immigrant curation is a lived experience of all ages. Individuals like Dr. Muntu, despite their professional backgrounds, must navigate the complexities of self-censorship and adaptation, whether at work or on the street, to avoid unwanted scrutiny.

The "good refugee" and "bad refugee" descriptions further illustrate curation of person.[193] The good refugee aims to act according to societal expectations, even when their actions are purely contrary to their values. Aiming to gain approval and credibility, refugees often mask their true selves and adopt performative, presumptive, and unquestioning conduct to meet the standards dictated by the observing authority.[194] Performative and unquestioning conduct results in a social climate that justifies excluding those unwilling and unable to meet the arbitrary expectations of authority or society. This eventually turns into an undesirable situation: ''conform and survive, or question and perish." The "good" immigrant classification as a curation mode unavoidably generates a class of those considered "bad" immigrants, undeserving of protection and asylum relief.[195]

The vulnerability of refugees and asylum seekers in the quest for survival, therefore, leads them to engage in self-curation as they strive to present themselves as good and desirable individuals.[196] This results in a constant tension between self-expressed intellectual privacy needs and self-censorship in every aspect of life.[197] In a surveillance-driven environment that disproportionately affects the most vulnerable, including asylum seekers, those surveilled painstakingly curate their actions and speech, striving to present themselves as ideal candidates deserving of positive immigration decisions and the associated immigration benefits.[198]

The extremes of curation result in real-life harm. There are well-documented cases involving asylum seekers who avoid seeking

---

[193] Sal Clark, Ashleigh Haw & Laurel Mackenzie, *The "Good Refugee" Ideal: How Discourses of Deservingness Permeate Australia's Refugee and Asylum Seeker Narratives,* 59 AUSTL. J. SOC. ISSUES 148 (2022).

[194] *Id.* at 148–52.

[195] *Id.* at 158.

[196] *See* Stephen Phillips, *Enhanced Vulnerability of Asylum Seekers in Times of Crisis*, 24 HUM. RTS. REV. 241, 241–43, 250–51 (2023) (analyzing how asylum seekers navigate predefined categories of vulnerability in their self-presentation to improve their chances of obtaining asylum or support).

[197] RICHARDS, *supra* note 8, at 6–7 (developing the concept of "intellectual privacy").

[198] David Lyon, *Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity*, 11 INT'L J. COMMC'N 824, 824–27 (2017) (examining how surveillance culture influences self-tracking and self-presentation across different social contexts).

medical treatment for themselves and their children despite the severity of their health conditions.[199] Because of misinformation and information disorder in migrant communities, many fear that seeking medical help could lead to identification and classification as a public charge, potentially affecting their immigration status. Although asylum seekers are exempt from public charge determinations, concerns over data tracking have driven many to forgo vital services, opting for isolation and vulnerability over the risk of surveillance and scrutiny.

The U.S. immigration framework had for some time aimed to facilitate the integration[200] and assimilation of immigrants within its borders while striving to maintain social cohesion and economic stability.[201] However, in many ways, curation undermines these efforts, systematically pushing refugees and asylum seekers into a precarious state, ironically imposed by the very system designed to support their transition. Even more concerning, a shift in immigration policy under the current Trump administration has heightened concerns about the integration of immigrants in the United States, as restrictive measures and enforcement priorities further complicate pathways to stability and inclusion.[202] Immigration scholar Hiroshi Motomura discusses the importance of integration, stating that "[i]n any society with an immigrant population, immigrant integration is the key to a civic solidarity that is consistent with equality and individual dignity. Without integration, the arrival of immigrants will, over time, undermine civic solidarity."[203] Motomura explains the notion of assimilation, stating that "'[a]ssimilation'—a term widely used in earlier eras—has been associated with pressure exerted by the native majority on immigrants to cut ties with their cultures, languages, or societies of

---

[199] *See* PEREIRA, ET AL., *supra* note 120, at 10–12 (detailing how immigrants' fear and mistrust of authorities leads them to avoid public assistance programs); Jan Hoffman, *Sick and Afraid, Some Immigrants Forgo Medical Care*, N.Y. TIMES (June 26, 2017), https://www.nytimes.com/2017/06/26/health/undocumented-immigrants-health-care.html [https://archive.ph/71lcR].

[200] Exec. Order No. 14,012, 86 Fed. Reg. 8277 (Feb. 5, 2021). S*ee generally* NAT'L ACADS. OF SCIS., ENG'G & MED., THE INTEGRATION OF IMMIGRANTS INTO AMERICAN SOCIETY, (Mary C. Waters & Marisa Gerstein Pineau eds., 2015), https://doi.org/10.17226/21746.

[201] *See* Muneer I. Ahmad, *Beyond Earned Citizenship*, 52 HARV. C.R.-C.L. L. REV. 257, 278–86 (2017).

[202] Exec. Order No. 14,159, 90 Fed. Reg. 1234 (Jan. 20, 2025).

[203] *See* Hiroshi Motomura, *Who Belongs? Immigration Outside the Law and the Idea of Americans in Waiting*, 2 U.C. IRVINE L. REV. 359, 365 (2012).

origin as a price of membership in the United States."[204] Both integration and assimilation, as U.S. immigration policies, are potentially inhibited by self-curation.

Curation imposes constraints on freedom of speech and movement, as individuals may choose to avoid authorities responsible for granting immigration status and benefits.[205] In this context, curation evolves into performance for an immigrant, not just as a means of personal survival but also safeguarding the well-being of their families and other vulnerable individuals connected to their data lifecycle.[206] Despite harboring concerns about diminished privacy, they refrain from voicing them due to fear of repercussions such as the denial of immigration benefits and eventual deportation.[207] Similar to data weaponization,[208] the resultant impact of curation is conformity and obedience, which limit agency, autonomy, and self-determination—critical tenets of privacy.[209] As scholar Asad suggests, the immigrants' situation resonates with Michel Foucault's idea that surveillance involves the delicate balance of risk and reward resulting from the authorities' need for power and control.[210] This results in selective engagement, which broadens the role of mainstream institutions in the lives of those concerned about state enforcement, including punishment.[211] The constant threat of deportation, denial, and reversal of immigration benefits serves as a powerful tool of curation inducement for

---

[204] *Id.* at 367.

[205] *See* David Cole, *Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens?* 25 T. JEFFERSON L. REV. 367, 377 (2003) (highlighting that the fear of deportation will permanently restrict what a foreigner says regardless of the First Amendment protection of the freedom of speech).

[206] *See* Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS (July 18, 2022), https://www.brookings.edu/articles/examining-the-intersection-of-data-privacy-and-civil-rights/ [https://perma.cc/9F5V-GKGD] (noting that for the marginalized, "the right to privacy is a matter of survival"); PEREIRA, ET AL., *supra* note 120, at 10–12 (explaining immigrants' avoidance of interaction with authorities for fear of identification).

[207] PEREIRA, ET AL., *supra* note 120, at 11–12.

[208] *See* Part II.C.3.

[209] *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980) (explaining the ideals of privacy—agency, autonomy, and self-determination).

[210] ASAD, *supra* note 9, at 11.

[211] *See* Asad L. Asad, *The Everyday Surveillance of Undocumented Immigrants*, PRINCETON UNIV. PRESS (July 26, 2023), https://press.princeton.edu/ideas/the-everyday-surveillance-of-undocumented-immigrants [https://perma.cc/S3MK-CDGE].

refugees and asylum seekers to conform by controlling their speech and conduct behavior.

The pressure to conform has affected not only the refugees and asylum seekers but also immigration activists and journalists.[212] Activists and journalists who advocate on behalf of the (in)visible immigrant, given that their freedom of speech is curtailed.[213] The targeting of journalists and activists pushes the (in)visible immigrant into a state of further undue submission and compliance. The constant monitoring, undue subordination, enforced self-discipline, and sense of inferiority create a panoptic society.[214] Ironically, many asylum seekers are forced to flee their home countries in pursuit of fundamental rights and freedoms—such as the freedom of speech protected by the First Amendment of the U.S. Constitution. Upon arrival, however, they often find those very rights constructively curtailed by the U.S. immigration surveillance regime.

The curation of a person results in the erasure of their identity and personal historical accounts. Associated with curation, the erasure of identity entails removing or suppressing certain aspects of an individual to fit into societal structures.[215] More broadly, refugees and asylees suppress their identity through systematic selectivity, which inhibits their ability to express themselves authentically.[216]

---

[212] *See* Geneva Sands & Priscilla Alvarez, *Watchdog Investigating CBP Amid Report the Agency Targeted Journalists, Activists*, CNN (March 7, 2019, 7:55 PM), https://www.cnn.com/2019/03/07/politics/inspector-general-customs-and-border-protection-tracking-journalists/index.html [https://perma.cc/8WRP-T3HF].

[213] *See* Cole, *supra* note 205, at 377 (explaining non-application of First Amendment rights to non-citizens outside the U.S).

[214] *See* Adriana C. Núñez, *Collateral Subjects: The Normalization of Surveillance for Mexican Americans on the Border*, 6(4) SOCIO. RACE & ETHNICITY 548, 555 (2020) (highlighting the strategy of compliance where individuals defined their behavior of avoiding actions that may lead them to cross paths with CBP).

[215] Erasure can be understood in literal, figurative, and metaphorical terms. I use the metaphorical and literal sense to define erasure as the loss or suppression of one's identity. I define identity as including culture, language, and religion, among other descriptions. In the literal sense, erasure can involve physical destruction, digital destruction such as burning documents or deleting digital files, forced forgetting, and memory suppression, where an individual actively tries to forget traumatic experiences. Figuratively, it can signify moving on or personal growth. Metaphorically, it means silencing history, true identity, and haunting reminders. *See* Omaiha Walajahi, *On Identity and Its Erasure,* PAUSE FOR PERSP. MENTAL HEALTH SERVS., https://hyderabadpsychologist.com/identity-series-on-identity-and-its-erasure/ [https://perma.cc/FZE7-TTCZ].

[216] *See* Guberek et al., *supra* note 181 at 6–7.

Individuals continuously construct their distinct identity and persona, moving beyond mere biographic and biometric information.[217] Identity is an inherent process of continued self-discovery and growth, shaped by experiences, culture, religion, race, nationality, and education, influencing modes of self-expression in behavior and speech.[218] This inherent uniqueness underscores the fundamental reality of the distinctiveness of every individual.[219] Accordingly, identity encompasses the ongoing activities that individuals engage in, with each action or inaction continually rebuilding and evolving their sense of self, irrespective of their physical location. Together, these ongoing activities form a unique historical and current footprint of every individual's identity.[220] Identity is intertwined with individuals' actions, self-presentation, and beliefs, which enable them to attain genuine agency and autonomy.

The constant veil of surveillance to which refugees and asylees are subjected forces them into a state of identity erasure even when they are in need.[221] Similar to curation, identity erasure suppresses freedom of speech and association. Knowing that authorities already possess abundant personal information, those surveilled choose to limit actions that could generate more data points about them.[222] For example, immigration authorities closely monitor the social media activity of asylum seekers.[223] This prompts many to avoid online

---

[217] *See* Vivian L. Vignoles, *Identity Motives*, *in* 1 HANDBOOK OF IDENTITY THEORY AND RESEARCH 403 (Seth J. Schwartz, Koen Luyckx & Vivian L. Vignoles eds., 2011).

[218] *See* Andrea Wharff, *Identity Erasure, in* THRESHOLDS 54 (Jim Tuedio & Helena Janes eds., 2009).

[219] *See* Thomas D. Williams & Jan Olof Bengtsson, *Personalism, in* STAN. ENCYC. OF PHIL. (Edward N. Zalta ed., 2022), https://plato.stanford.edu/entries/personalism/ [https://perma.cc/G44S-FUT5].

[220] *See* Verplanken & Sui, *supra* note 175, at 2 (highlighting that "personal or self-identities . . . include . . . self-attributions, beliefs, motivations, recurrent thoughts, emotions, and self-perceptions").

[221] RANDY CAPPS, MICHAEL FIX, JASON OST, JANE REARDON-ANDERSON & JEFFREY S. PASSEL, URB. INST., THE HEALTH AND WELL-BEING OF YOUNG CHILDREN OF IMMIGRANTS 24 (2004) (noting immigrants' avoidance of authorities for fear of identification, potential deportation, and adverse consequences on family members).

[222] *See* Núñez, *supra* note 214, at 553–55 (defining immigrants' behavior of avoiding actions that may lead them to cross paths with CBP).

[223] *See* Rachel Levinson-Waldman, Harsha Panduranga & Faiza Patel, *Social Media Surveillance by U.S. Government*, BRENNAN CTR. FOR JUST. (Jan. 7, 2022), https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government [https://perma.cc/5A2L-2XUY].

engagement and self-expression out of fear that their posts could negatively impact their asylum applications or expose them to additional scrutiny. They may avoid attending cultural or religious gatherings, fearing that such activities would add to their surveillance profile. Consequently, the decision to limit one's actions becomes a form of identity erasure because one's daily actions and interactions construct one's identity. It is important to note that erasure is related to curation because in both situations, individuals often avoid actions that further entrench them in surveillance.

The price of erasure of identity is very steep. It strips individuals of their agency and undermines their sense of self-worth as members of society. The surveillance tools imposed on refugees and asylum seekers profoundly affect their lives through identity erasure not only as aspiring citizens but also as members of a free society.[224] By attempting to conform through curation and identity erasure, refugees and asylees sacrifice the ideals of privacy and freedom, which are key tenets of any democratic society.

3. *Weaponization of Personal Data*

The weaponization of personal information involves using an individual's data, with or without their consent, to produce outcomes detrimental to their interests or those connected to them throughout the data lifecycle.[225] It denotes the harmful use of data obtained through coercion, vulnerability, or unequal power dynamics. The weaponization of personal information also includes the use of an

---

[224] *See* Mirian G. Martinez-Aranda, *The Impact of Immigration and Customs Enforcement's Surveillance Technology on the Well-being of the Children of Immigrants*, AM. BEHAV. SCIENTIST ONLINEFIRST 2 (Nov. 25, 2023), https://doi.org/10.1177/00027642231216538 (describing the stigmatic impact of electronic monitors on immigrants).

[225] *Cf.* Char Sample, Michael J. Jensen, Keith Scott, John McAlaney, Steve Fitchpatrick, Amanda Brockinton, David Ormrod & Amy Ormrod, *Interdisciplinary Lessons Learned While Researching Fake News*, 11 FRONTIERS PSYCH. 1, 4 (2020), https://doi.org/10.3389/fpsyg.2020.537612. The weaponization of information is enhanced in the digital world, where digital communities are created within and outside borders, simultaneously shattering hopes of privacy and instilling fear among the most vulnerable. *See also* JANNA ANDERSON & LEE RAINIE, PEW RSCH. CTR., THE FUTURE OF TRUTH AND MISINFORMATION ONLINE 11–12 (2017), https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/ [https://perma.cc/Y5V4-25KJ] (illustrating use of personal information for targeted misinformation campaigns); Flemming Splidsboel Hansen, *The Weaponization of Information,* DANISH INST. FOR INT'L STUD. (Dec. 14, 2017), https://www.diis.dk/en/research/the-weaponization-of-information [https://perma.cc/73B6-87SH].

individual's identifying information to subvert their interests, undermine their autonomy and self-determination, thereby distorting or obstructing their ability to pursue their desired goals. Information weaponization occurs when data holders leverage personal information to exclude, manipulate, and control individuals, causing harm and advancing objectives that serve external interests rather than those of the data subject.[226] Refugees' and asylum seekers' personal information has been used by both private and government entities, resulting in real-world harm against them. For example, many of them have been unlawfully tracked, detained, and deported following the personal information they willingly provided to immigration authorities.[227]

The public charge inadmissibility rules have been used to exclude and misinform refugees and asylum seekers, serving as an example of weaponizing personal information. Public charge inadmissibility hinges on whether a non-citizen will likely become primarily dependent on government support. This dependence is indicated by receiving public assistance or being institutionalized long-term at the government's expense.[228] It is important to note that refugees and asylum seekers may qualify for benefits such as the Supplemental Nutrition Assistance Program (SNAP) and Temporary Assistance for Needy Families (TANF).[229] The Trump

---

[226] *See Weaponization of Information*, *Dictionary of Populism*, EUR. CTR. FOR POPULISM STUD., https://www.populismstudies.org/Vocabulary/weaponization-of-information/ [https://perma.cc/Q48B-37QE] (exploring how personal data is weaponized to influence, control, and exploit individuals, serving external agendas); W. Lance Bennett, *The Personalization of Politics: Political Identity, Social Media, and Changing Patterns of Participation,* 644 ANNALS AM. ACAD. POL. & SOC. SCI. 20, 20–38 (2012) (analyzing how digital media personalizes political participation and influences identity formation, which may contribute to targeted influence and control in data-driven environments); TESS WILKINSON-RYAN, FOOL PROOF: HOW FEAR OF PLAYING THE SUCKER SHAPES OUR SELVES AND THE SOCIAL ORDER—AND WHAT WE CAN DO ABOUT IT 47–64, 113–62 (2023) (examining how the fear of being deceived reinforces social and economic hierarchies, contributing to the weaponization of racist and sexist biases against marginalized individuals).

[227] *See* Estefania McCarroll, *Weapons of Mass Deportation: Big Data and Automated Decision-Making Systems in Immigration Law*, 34 GEO. IMMIGR. L.J. 705, 714–16 (2020) (analyzing how automated systems and data collection facilitate the targeting, detention, and deportation of immigrants, often without judicial review or due process).

[228] Public Charge Ground of Inadmissibility, 87 Fed. Reg. 55472 (Sept. 9, 2022) (to be codified at 8 C.F.R. pts. 103, 212, 213, and 245).

[229] Field Guidance of Deportability and Inadmissibility on Public Charge Ground, 64 Fed. Reg. 28689 (proposed Mar. 26, 1999) (providing

Administration's 2019 expansion of the definition of public charge to include noncash assistance programs such as Medicaid left many asylum seekers exposed to exclusion from medical care.[230] Seeking this necessary assistance would jeopardize their eligibility for citizenship and other immigration benefits at a later stage. Any information regarding their access to this assistance would be used against them, representing a typical form of data weaponization.[231] Although the Biden Administration reversed the Trump Administration's expanded public charge regulations in 2022, misinformation and purging of access to information regarding the public charge rules still created fear, exclusion, and confusion among vulnerable refugees and asylum seekers.[232] This is a typical example of data weaponization. The fear of being deemed a public charge, despite qualifying for assistance under certain conditions, weighs heavily on refugees and asylum seekers. The resulting restrictions on essentials like food and medical care further deepen the families' vulnerability within an immigration surveillance state.

The government's technological ability to create a comprehensive digital portrait of an individual's life through various data points poses a significant risk of data weaponization for refugees and asylum seekers.[233] It also contradicts the U.S. integration framework, which is critical to civic solidarity, diversity, inclusion,

---

an exemption from public charge determinations for purposes of admission and adjustment); ESSEY WORKIE, LILLIE HINKLE & STEPHANIE HEREDIA, MIGRATION POL'Y INST., THE MISSING LINK: CONNECTING ELIGIBLE ASYLEES AND ASYLUM SEEKERS WITH BENEFITS AND SERVICES (2022), https://www.migrationpolicy.org/research/asylees-asylum-seekers-benefits [https://perma.cc/GQG4-YMAD] (supporting that refugees and asylum seekers are eligible for some federal public benefits).

[230] *See* Inadmissibility on Public Charge Grounds, 804 Fed. Reg. 41292, 41295 (Aug. 14, 2019) (to be codified at 8 C.F.R. pts. 103, 212, 213, 214, 245, and 248).

[231] RANDY CAPPS, ET AL., *supra* note 221, at 6–7, 24 (reporting that migrants with mixed families, comprised of undocumented parents and children who are U.S. citizens, avoid public assistance due to fear of deportation).

[232] Public Charge Ground of Inadmissibility, *supra* note 228, at 55473–74; *see* Drishti Pillai & Samantha Artiga, *2022 Changes to the Public Charge Inadmissibility Rule and the Implications for Health Care,* KFF (May 5, 2022), https://www.kff.org/racial-equity-and-health-policy/issue-brief/2022-changes-to-the-public-charge-inadmissibility-rule-and-the-implications-for-health-care/ [https://perma.cc/4J9X-8ART].

[233] *See* TANYA BRODER & GABRIELLE LESSARD, NAT'L IMMIGR. L. CTR., OVERVIEW OF IMMIGRATION ELIGIBILITY FOR FEDERAL PROGRAMS 11 (2024), https://www.nilc.org/issues/economic-support/overview-immeligfedprograms/ [https://perma.cc/8QDH-KXWZ].

and consistency with equality and individual dignity.[234] As explained earlier, their precarious situation affects their ability to make informed decisions and choices.[235] This results in undue conformity and obedience, stripping their agency, autonomy, and self-determination—critical dimensions of privacy. They are less likely to challenge the data collection practices for fear of jeopardizing their immigration status.

A stark illustration of data weaponization was the mandatory use of the now-discontinued CBP One(now CBP Home) app, which asylum seekers arriving at the U.S.–Mexico border were required to use to schedule appointments with immigration officers.[236] The app collected biographic, biometric, and related data and had become the sole method for immigrants at the U.S.–Mexico border to schedule appointments and ensure eligibility for asylum at the port of entry.[237] However, this mandate posed significant challenges for certain individuals, particularly those affected by factors such as race, language, digital literacy, age, or disability, thereby excluding them from the much-needed relief.[238] The app was constantly criticized as borderline racist, as its design and implementation

---

[234] *See* Exec. Order No. 14012, 86 Fed. Reg. 8277 (Feb. 5, 2021); Motomura, *supra* note 203, at 365. *See generally* NAT'L ACADS. OF SCIS., ENG'G & MED., *supra* note 200.

[235] *See* Kaurin, *supra* note 15, at 10–12.

[236] *See* AMNESTY INTERNATIONAL, *USA: Mandatory Use of CBP Application Violates the Right to Seek Asylum*, AMNESTY INT'L (May 8, 2023), https://www.amnesty.org/en/latest/news/2023/05/usa-mandatory-cbp-one-violates-right-asylum/ [https://perma.cc/6ZTE-B8YW]; *see also* Deck, *supra* note 103, at 1 (explaining how mandatory CBP One application for scheduling asylum appointments disadvantages non-English and Spanish speakers).

[237] *See CBP Home Mobile Application*, U.S. CUSTOMS & BORDER PROT. (Mar. 12, 2025), https://www.cbp.gov/about/mobile-apps-directory/cbpone [https://perma.cc/WH8D-EBC2]; *CBP One: An Overview*, AM. IMMIGR. COUNCIL (Mar. 24, 2025), https://www.americanimmigrationcouncil.org/research/cbp-one-overview [https://perma.cc/4XSV-5C2E].

[238] *See* HUM. RTS. WATCH, "WE COULDN'T WAIT": DIGITAL METERING AT THE U.S-MEXICO BORDER 44 (May 1, 2024), https://www.hrw.org/report/2024/05/01/we-couldnt-wait/digital-metering-us-mexico-border [https://perma.cc/SQT4-LS2R]; Deck, *supra* note 103 (reporting that the mandatory CBP One application for scheduling asylum appointments disadvantages non-English and Spanish speakers); *US: Digital Metering System Exposes Migrants to Harm: Asylum Turnbacks Violate Rights and Enrich Criminal Groups*, HUM. RTS. WATCH (May 1, 2024, 9:00 AM), https://www.hrw.org/news/2024/05/01/us-digital-metering-system-exposes-migrants-harm [https://perma.cc/36LR-Y9UG].

disproportionately disadvantaged immigrants of color, particularly through facial recognition.

It consistently misidentified individuals with darker skin tones, and often failed to recognize them accurately due to their complexion.[239] This led to misidentification issues, with some asylum seekers facing unjust entry bans and unfavorable asylum decisions despite having used the app as required and being lawfully present in the U.S.[240] Moreover, those who arrived at the border without a CBP One appointment and not facing certain extenuating circumstances faced an increased risk of expedited removal to Mexico or their country of origin without due process.[241]

The weaponization of personal information is evident in the current administration's immigration enforcement practices. A striking example is the case of Kilmar Abrego Garcia, an immigrant and Maryland resident who was misidentified as a member of the MS-13 gang based on his tattoos.[242] He was wrongfully deported to El Salvador, despite a court order protecting him from removal.[243] Although the administration cited his tattoos as evidence of gang affiliation, experts later established that the markings were not indicative of MS-13 membership.[244] This case not only illustrates the dangers of misidentification and overbroad classification but also highlights how immigrants' personally identifiable information can be weaponized. Such practices can lead to severe consequences like wrongful deportation and produce a broader chilling effect on speech and freedom of association, ultimately eroding privacy rights.

---

[239] SARAH DAVILA, ALEJANDRA PALACIOS & BRAD THOMPSON, UNIV. OF ILL. CHI. L., *CBP One Mobile Application: Violating Migrants' Rights to Privacy and Freedom from Discrimination* (2024), https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1034&context=whitepapers [https://perma.cc/BSR3-5EKX].

[240] AMNESTY INTERNATIONAL, *supra* note 236.

[241] *Court Allows Turnbacks of Asylum Seekers Without CBP One Appointments to Continue*, AM. IMMIGR. COUNCIL (Oct. 13, 2023), https://www.americanimmigrationcouncil.org/news/court-allows-turnbacks-asylum-seekers-without-cbp-one-appointments-continue [https://perma.cc/55CG-KQYJ].

[242] *See* Layla Ferris, *Experts Cast Doubt on Trump's Claim that Abrego Garcia's Finger Tattoo Prove MS-13 Membership,* CBS News (Apr. 23, 2025, 6:27 PM), https://www.cbsnews.com/news/trump-claim-kilmar-abrego-garcias-finger-tattoos-ms-13/ [https://perma.cc/MC3Y-VN98].

[243] *See* Susan Heavey & Ted Hesson, *Trump Administration Says Man Was Deported to El Salvador in Error,* REUTERS (Apr. 11, 2025, 4:10 PM), https://www.reuters.com/world/americas/trump-administration-says-man-deported-el-salvador-in-error-2025-04-01/ [https://archive.ph/FflLE].

[244] *See* Ferris, *supra* note 242.

Surveillance in the immigration state extends beyond refugees. It also ensnares those who advocate on their behalf. Immigration advocates and community organizers have been subjected to discriminatory profiling, targeted surveillance, and policing.[245] In many instances, their personal information has been used against them, demonstrating the effect of surveillance on both immigrant communities and their defenders. For example, in *Maria F. C. Ramirez et al. v LexisNexis Risk Solutions,* plaintiffs alleged that LexisNexis unlawfully collected, shared, and sold the personal identity and location data of immigrants, activists, and community organizers without consent.[246] They alleged that the data was being sold to private and public entities, including ICE, facilitating law enforcement targeting in violation of their privacy rights.[247] While the case was ultimately dismissed due to the plaintiffs' inability to demonstrate unfair business practices and actual damages under the Illinois Consumer Fraud and Deceptive Business Practices Act, the allegations raised in *Ramirez* underscore the broader concerns about data-driven surveillance and the legal barriers to holding private data brokers accountable.

Despite its dismissal, the *Ramirez* case highlights ICE's continued reliance on databases like LexisNexis Accurint to build dossiers on individuals for targeted for immigration enforcement.[248] Aggregated personal data sourced from multiple agencies remains central to ICE operations, exemplifying the weaponization of immigrants' personal data.[249] Law enforcement agencies rely on and exploit such commercial data sources to track, apprehend, and deport asylum seekers. Since 2015, ICE has conducted numerous facial recognition searches on state DMV databases to identify and locate

---

[245] Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.*, MIT TECH. REV. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ [https://perma.cc/DP94-9X78] (reporting that predictive data are often skewed against Black persons).

[246] 729 F. Supp. 3d 838, 849 (N.D. Ill. 2024). The motion to dismiss was granted in April 2024, with the court citing the defendant's provision of opt-out choice to consumers as one reason for dismissal. The case exemplifies the weaponization of data through data misuse.

[247] *Id.* at 845.

[248] *Id.*

[249] Victor G. Febres & Karen F. Ruiz, *The U.S. Government Buys Data for Surveillance. For Immigrants, It's a Matter of Survival*, TECH POL'Y PRESS (Apr. 18, 2024), https://www.techpolicy.press/the-us-government-buys-data-for-surveillance-for-immigrants-its-a-matter-of-survival/ [https://perma.cc/GR49-MTR8].

individuals for deportation.[250] These searches automatically verify or identify individuals from digital images or video sources, often without notice to license holders, a warrant, or other legal authorization.[251] Additionally, ICE has leveraged social media platforms to track and monitor immigrants, using online information to identify, locate, and target individuals for enforcement actions.[252]

Through real-time location tracking, personal information is weaponized as authorities restrict movement, hindering asylum seekers' ability to integrate into society and access essential services. For example, under ICE's Family Expedited Removal Management (FERM) program, asylum-seeking families are subjected to ankle monitors and curfews, severely limiting their freedom of movement, obstructing their access to healthcare, legal representation, and employment.[253] More broadly, geolocation tracking technologies used for immigration control raise significant privacy concerns as they enable continuous surveillance and control over individuals' movements.[254] Reports indicate that ICE has relied on private data brokers to collect vast amounts of personal data on immigrants, including location history, without their knowledge and consent.[255] This expansion of digital surveillance reinforces concerns about how

---

[250] *See* Aarti Shahani*, ICE Turned to DMV Driver's License Databases for Help with Facial Recognition*, NPR (July 8, 2019, 4:45 PM), https://www.npr.org/2019/07/08/739643786/ice-turned-to-dmv-drivers-license-databases-for-help-with-facial-recognition [https://perma.cc/4NBM-L35A].

[251] *See* Drew Harwell & Erin Cox, *ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers*, WASH. POST (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/ [https://archive.ph/CyG3d] (reporting that ICE conducted facial-recognition searches on millions of Maryland driver's license photos without obtaining warrants or informing license holders).

[252] *See* Max Rivlin-Nadler, *How ICE Uses Social Media to Surveil and Arrest Immigrants,* INTERCEPT (Dec. 22, 2019), https://theintercept.com/2019/12/22/ice-social-media-surveillance/ [https://perma.cc/UZQ3-8EJM].

[253] *See Policy Brief | ICE's Family Expedited Removal Management (FERM) Program Puts Families at Risk*, NAT'L IMMIGRANT JUST. CTR. (Aug. 31, 2023), https://immigrantjustice.org/research-items/policy-brief-ices-family-expedited-removal-management-ferm-program-puts-families [https://perma.cc/5R6M-B7LN].

[254] Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, AM. BAR ASS'N BUS. L. TODAY (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/ [https://perma.cc/RT4W-QP3A].

[255] *See* WANG, ET AL., *supra* note 5, at 21.

real-time tracking is systematically used and weaponized against asylum seekers under the guise of immigration enforcement.

Beyond physical restrictions, authorities also exploit and weaponize personal data to target individuals based on political ideologies, religious beliefs, and social affiliations. Even seemingly unobtrusive personal information—such as biometric identifiers (fingerprints, facial recognition scans) and behavioral indicators (social media activity, movement patterns)—can be leveraged to profile individuals and predict ideological leanings, ultimately weaponized against immigrants. Research shows that biological and behavioral markers can correlate with ideological orientations.[256] While these findings highlight the potential for predictive profiling, in the context of immigration enforcement, such data are leveraged for the surveillance and targeting of immigrants. When accessed and misused, such data enables law enforcement agencies to monitor, profile, and discourage asylum seekers from exercising their rights.[257]

Much like the phenomenon of personality curation in a surveillance state, the weaponization of personal information creates a chilling effect on free expression. As such, surveillance leads to self-censorship, discouraging individuals from expressing minority opinions.[258] This suppression of free speech instills fear, discouraging public engagement in civic discourse and participation.[259] These practices pose risks to democratic

---

[256] Woo-Young Ahn, Kenneth T. Kishida, Xiaosi Gu, Terry Lohrenz, Ann Harvey, John R. Alford, Kevin B. Smith, Gideon Yaffe, John R. Hibbing, Peter Dayan & P. Read Montague, *Nonpolitical Images Evoke Neural Predictors of Political Ideology*, 24 CURR. BIOL. 2693 (Nov. 17, 2014), https://pmc.ncbi.nlm.nih.gov/articles/PMC4245707/ [https://perma.cc/RC7T-VGWA] (explaining findings suggesting that fundamental data points, including biological data points, can play a crucial role in shaping political beliefs in previously unrecognized ways).

[257] *See* Rachel Levison-Waldman & Angel Diaz, *Social Media Surveillance by Homeland Security Investigations: Threat to Immigrant Communities and Free Expression*, BRENNAN CTR. FOR JUST. (Nov. 15, 2019), https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-homeland-security-investigations-threat [https://perma.cc/Q7T3-59UP].

[258] *See* Lyon*, supra* note 201, at 827–88 (arguing that being surveilled contributes to self-censorship); *see also* Karen Turner, *Mass Surveillance Silences Minority Opinions, According to Study*, WASH. POST (Mar. 28, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/ [https://archive.ph/PxQVR].

[259] *See generally* Suzanne Nossel, *The Fate of American Democracy Depends on Free Speech*, 153 DAEDALUS 119 (2024) (arguing that restricting free speech undermines democratic participation).

participation over time.[260] The exploitation of personal information by authorities for profiling and surveillance subjects immigrants to increased scrutiny, potentially deterring them from community participation.

Monitoring asylum seekers' movements through the ATD program while they await the hearing of their asylum cases is a form of weaponization of location data.[261] The use of facial recognition technology and ankle shackles to constantly track their location and movements in exchange for waiting for a hearing date outside of physical detention masks the reality of detention, surveillance, and control.[262] Whether physical or electronic, such detention involves intensive and constant monitoring, infringing on privacy rights and criminalizing immigration. Consequently, their pursuit of freedom from persecution is unfairly transformed into a crime, the highest form of weaponization of information.

The weaponization of personal information affects both the young and the old as exemplified by surveillance and bureaucratic hurdles, particularly children with Special Immigrant Juvenile Status (SIJS).[263] Under the SIJS program, the INA grants children, often fleeing abuse, neglect, and economic hardship, a chance to apply for special eligibility and potentially obtain lawful permanent resident status. While SIJS was designed to offer protection, the reality on the ground is one of constant surveillance, prolonged processing times, and frequent demand for additional evidence.[264] Congress intended SIJS to provide a safe and secure future for these vulnerable youth. However, they experience prolonged legal uncertainty, exploitation,

---

[260] *See* Joan Friedland, *How ICE Uses Databases and Information-Sharing to Deport Immigrants,* NAT'L IMMIGR. L. CTR. (Jan. 25, 2018), https://www.nilc.org/articles/how-ice-uses-databases-and-information-sharing-to-deport-immigrants/ [https://archive.ph/2IhlP] (discussing how ICE leverages data-sharing systems to identify and target immigrants for enforcement, raising concerns about increased scrutiny and deterrence); *see also Social Media Surveillance by Homeland Security Investigations: A Threat to Immigrant Communities and Free Expression*, BRENNAN CTR. FOR JUST. (Nov. 15, 2019), https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-homeland-security-investigations-threat [https://perma.cc/U9BZ-VYZ5] (analyzing the impact of immigration enforcement's use of social media surveillance on immigrant rights and democratic participation).

[261] *See* AM. IMMIGR. COUNCIL, BEYOND A BORDER SOLUTION: HOW TO BUILD A HUMANITARIAN PROTECTION SYSTEM THAT WON'T BREAK 15–25 (2023), https://www.americanimmigrationcouncil.org/research/beyond-border-solutions [https://perma.cc/T3ZZ-FQNR].

[262] *See* WANG, ET AL., *supra* note 5, at 4.

[263] *See* 8 U.S.C. § 1101(a)(27)(j).

[264] *See* Laila L. Hlass, Rachel Leya Davidson & Austin Kocher, *The Double Exclusion of Immigrant Youth*, 111 GEO. L.J. 1407, 1487 (2023).

discrimination, and exclusion based on age, race, and immigration status, among other intersectional factors.[265] Despite Congress mandating a 180-day adjudication period for SIJS petitions[266], delays are the order of the day, leaving them in a state of uncertainty about their future for years. These extended delays, coupled with uncertainty, have been reported to cause mental health struggles as they hinder their ability to work and pursue education.[267]

Leila Hlass and colleagues, in their comprehensive examination of the SIJS system, highlight the impact of these significant delays and label them as a form of "double exclusion," preventing children from transitioning safely into adulthood and profoundly impacting their mental health and well-being.[268] They further observe that this delay enrolls these children in a continuous surveillance system and in a form of legal violence, exacerbated by endless administrative processes and the political caprices of the time, risking further harm to these already vulnerable children.[269] Such systemic delays and bureaucratic entanglements represent a quintessential form of data weaponization with the immigration surveillance state.

The weaponization of information against refugees and asylum seekers is twofold: government and commercial weaponization. Like government agencies, commercial entities weaponize personal data through targeted advertising and manipulation, extensively mining and exploiting data to influence consumer behavior.[270] Digital technology corporations collect vast amounts of personal data, such as browsing history, location information, and social media activities, to create their profiles.[271] Participation in basic consumer activities should be devoid of surveillance and suspicion, ensuring individuals are not subject to scrutiny of their actions. However,

---

[265] *Id.* at 1486.

[266] 8 U.S.C. § 1232(d)(2).

[267] *See* Carola Suárez-Orozco & Guadalupe López Hernández, "*Waking up Every Day With The Worry": A Mixed-Methods Study of Anxiety in Undocumented Latinx College Students,* 11 FRONTIERS PSYCHIATRY 1, 7 (2020), https://doi.org/10.3389/fpsyt.2020.568167.

[268] Laila L. Hlass, Rachel Leya Davidson & Austin Kocher, *The Double Exclusion of Immigrant Youth*, 111 GEO. L.J. 1407, 1413 (2023).

[269] *Id.* at 1487.

[270] *See Protecting Migrants at Borders and Beyond*, PRIV. INT'L, https://privacyinternational.org/protecting-migrants-borders-and-beyond [https://archive.ph/WHvpP] (highlighting how inadequate data protection exposes refugees to exploitation, including through targeted advertising and manipulation).

[271] *See* Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have on You*, SECURITY.ORG (Feb. 13, 2024), https://www.security.org/resources/data-tech-companies-have/ [https://perma.cc/6RLK-NAWT].

refugees and asylum seekers often face heightened data weaponization as they are commercially exploited while at the same time eroding their fundamental freedoms. As Allen describes in her work *The Black Opticon*, African Americans and other marginalized communities face targeted digital discrimination and algorithmic bias, drawing them into inequitable pan-optic, ban-optic, and con-optic schemes.[272] This form of data weaponization disproportionately affects them, embedding biases and inequalities in decision-making processes like job hiring, insurance applications, and access to credit and housing.[273] Anyone who participates in basic consumer activities should be free from surveillance and suspicion, and there should be no fear that such activity could be used against an individual. The stakes are higher for refugees and asylum seekers, given their vulnerability in the data cycle.

D. SOCIETAL CONSEQUENCES

While significant political and social debate has centered on the number and categories of immigrants admitted to the U.S., far less attention has been paid to the long-term consequences of discriminatory and oppressive immigration enforcement policies—particularly the consequences of immigrants' surveillance. In *Unpopular Privacy: What Must We Hide?,* Allen underscored the vital role of privacy in society, highlighting it as an essential tool for achieving the goals and principles of a free and flourishing society despite public indifference or resistance.[274] Specifically, the impact of disproportionate surveillance on the (in)visible immigrant has been ignored and yet has profound implications for society.

The persistent shadow of past and present surveillance schemes by both government and private commercial entities continues exposing the (in)visible immigrant to manipulations and exploitation.[275] Surveillance effectively creates individuals who are systematically marginalized and disenfranchised.[276] This implicates broader governance and democratic processes and development as

---

[272] *See* Allen, *supra* note 8, at 907, 914.

[273] *See* Ayano, *supra* note 162, at 168–69; *see also* Matthew Desmond & Nathan Wilmers, *Do the Poor Pay More for Housing? Exploitation, Profit, and Risk in Rental Markets*, 124 AM. J. SOCIOLOGY 1090, 1115 (2019).

[274] *See* ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 108–10 (2011).

[275] TORIN MONAHAN, SURVEILLANCE IN THE TIME OF INSECURITY 71–72 (2010).

[276] VANCE PACKARD, THE NAKED SOCIETY 236–55 (1964) (explaining how over-surveillance disenfranchises and systematically marginalizes people).

individuals lack agency and are targets of political manipulation and control.[277] This continues even long after they become citizens.

Timur Kuran explains how individuals conceal their preferences under social pressure, leading to distorted representations of their norms and values to society.[278] Kuran's conception accurately depicts what becomes of the (in)visible immigrant upon the realization of intense surveillance; with a great need to conform to the watching authorities (perceived or actual), they present a curated and yielded persona in public, masking their true self.[279] Disproportionate surveillance results in concealment and self-denial as strategies to avoid societal sanctions, ultimately eroding identity and autonomy. The fear of deportation and loss of immigration benefits, including employment authorization, forces individuals into self-preservation and compels them to compromise their private beliefs, even when those beliefs do not conflict with public policy. Society loses because suppressed ideas deprive the community of diverse perspectives, stifling social and cultural growth.

The surveillance of the (in)visible immigrant not only undermines their rights to privacy but also impedes the free and open participation of immigrant families in societal life. The constant fear of family separation through deportation looms large, discouraging meaningful engagement and silencing their presence in public spaces like schools, churches, cultural exchange events, and social services.[280] A family is a fundamental unit and building block of the entire society.[281] The long-term impact of sustained surveillance of immigrant families is the erosion of spaces for dialogue and exchange of ideas—processes vital for democracy. The ultimate result of surveillance is an erosion of trust, discouraging civic engagement and participation in social and political activities,

---

[277] *See generally* WILLIAM G. STAPLES, EVERYDAY SURVEILLANCE: VIGILANCE AND VISIBILITY IN POSTMODERN LIFE (2d ed. 2014).

[278] *See* TIMUR KURAN, PRIVATE TRUTHS, PUBLIC LIES: THE SOCIAL CONSEQUENCES OF PREFERENCE FALSIFICATION 22–50 (1997).

[279] *See supra* Section II. C, pp. 325–326 (discussion of yielding in relation to data surrender).

[280] *See* Randy Capps, Marc R. Rosenblum, Cristina Rodríguez & Muzaffar Chishti, *Delegation and Divergence: A Study of 287(g) State and Local Immigration Enforcement*, Migration Pol'y Inst. (Jan. 2011), https://www.migrationpolicy.org/research/delegation-and-divergence-287g-state-and-local-immigration-enforcement [https://archive.ph/r4xn5] (noting that immigration raids and deportations foster fear and mistrust of public institutions, reducing immigrant participation in community services and activities).

[281] *See generally* CARLE C. ZIMMERMAN, FAMILY AND CIVILIZATION (1947).

thereby destabilizing democracy.[282] This suppression of diverse voices and experiences leads to homogenized discourse that does not reflect the actual needs and aspirations of any civil and democratic society.[283]

Addressing the privacy needs of the (in)visible immigrant requires deliberate and sustained efforts that foster their agency and full participation in society. This must be accompanied by robust accountability measures and clear frameworks to ensure that digital technologies are used responsibly and that immigration enforcement authorities operate within the limits of the law.

III. PROTECTING THE (IN)VISIBLE IMMIGRANT

Immigration has long been a polarizing political subject in the U.S. Yet, there is a glaring lack of public discourse on the broader implications of data surveillance in immigration policy debates.[284] Mainly, the issue with discriminatory surveillance of refugees and asylum seekers in immigration enforcement lies in the lack of adequate oversight and accountability for their privacy.[285] Immigration matters are often overshadowed by the politics of the day and national security concerns, which tend to eclipse an immigrant's human and legal rights. Consequently, vulnerabilities arising from automation, lapses in data security, and the potential misuse of immigration surveillance systems have long been overlooked, especially as refugees and asylum seekers are perceived as "foreigners" or "others" undeserving of equal legal protection.[286] For example, in 2022, ICE experienced a data breach that exposed the personal information of over six thousand asylum seekers, subjecting them to the risk of privacy violations such as online fraud

---

[282] *See* BRENNAN CTR. FOR JUST., *supra* note 259 (analyzing the impact of immigration enforcement's use of social media surveillance on immigrant rights and democratic participation); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW (2007).

[283] *See* AMY E. LERMAN & VESLA M. WEAVER, ARRESTING CITIZENSHIP: THE DEMOCRATIC CONSEQUENCES OF AMERICAN CRIME CONTROL 199–202 (2014) (active participation in political processes is a cornerstone of a healthy democracy); Megan Brenan, *Immigration Named Top U.S. Problem for Third Straight Month*, GALLUP (Apr. 30, 2024), https://news.gallup.com/poll/644570/immigration-named-top-problem-third-straight-month.aspx# [https://perma.cc/5SUM-3N9D] (explaining that "immigration has been the most politically polarizing issue mentioned in past 25 years").

[284] BRENNAN CTR. FOR JUST., *supra* note 257.

[285] *See* WANG, ET AL., *supra* note 5, at 4.

[286] Hiroshi Motomura, *The Rights of Others: Legal Claims and Immigration Outside the Law*, 59 DUKE L.J. 1723, 1783–86 (2010).

and impersonation.[287] Without careful refinement of data collection laws, regulations, policies, and practices specifically designed to protect the (in)visible immigrant, data will continue to be used as a tool of disproportionate surveillance by both the government and private entities.

A. PRIVACY AS A HUMAN RIGHT

Privacy is a fundamental human right essential to preserving every individual's agency, autonomy, and self-determination—a principle that should extend to the (in)visible immigrant under the human rights framework of citizenship status.

The Universal Declaration of Human Rights (UDHR), adopted by the United Nations General Assembly in 1948, recognizes privacy as a universal and fundamental human right.[288] The U.S played a pivotal role in drafting and advocating for the adoption of the UDHR, embedding its principles into the foundation of modern human rights.[289] Although the UDHR is not a binding treaty, it has significantly influenced international human rights norms and should serve as a valuable reference in advancing, including privacy.

The UDHR principles have informed international covenants, most notably the International Covenant on Civil and Political Rights (ICCPR), which was adopted in 1966 and ratified by the U.S. in 1992.[290] The ICCPR enshrines the essential rights and freedoms inherent to any democratic society, including the right to privacy, and should guide the evolution of domestic privacy rights protection for all.

---

[287] Hamed Aleaziz, *ICE Releases Thousands of Migrants Affected by Data Breach*, L.A. TIMES (Jan. 19, 2023), https://www.latimes.com/world-nation/story/2023-01-19/ice-leak-personal-information-immigrants-asylum# [https://perma.cc/J7KG-K2LU].

[288] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948) [hereinafter UDHR] ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."); *see also* Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right,* 14 HUM. RTS. L. REV. 441, 441–43 (2014) (tracing the development of the right to privacy as a human right emanating from the UDHR).

[289] Harold Hongju Koh, *Why U.S. Leadership Matters for the Global Defense, Protection and Promotion of Human Rights*, FOREIGN SERV. J. (June 2020), https://afsa.org/why-us-leadership-matters-global-defense-protection-and-promotion-human-rights [https://perma.cc/2WHP-QMRT].

[290] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976); *see* 138 CONG. REC. 8068–71 (1992) (ratifying the ICCPR).

Article 17 of the ICCPR adopts verbatim the language of the UDHR in providing for the right to privacy, affirming that no one shall be subjected to unlawful or arbitrary interference with their privacy, family, home, or correspondence.[291] While the U.S. ratified the ICCPR with reservations, understandings, and declarations (RUDS) and declared it non-self-executing, it notably did not include a specific reservation regarding the right to privacy.[292] Despite the limitations on enforceability, the ICCPR adoption of the UDHR's privacy framework establishes a global benchmark for fundamental rights and freedoms, reinforcing privacy as an essential human right alongside other core protections. Thus, aligning U.S. policies with the ICCPR's privacy protections would provide crucial safeguards for refugees and asylum seekers, ensuring their rights are upheld in accordance with established international standards.[293]

The U.S. Constitution provides that treaties, together with the Constitution and federal statutes, constitute "the supreme law of the Land."[294] The exception is that if a treaty contradicts the Constitution, the Constitution takes precedence, as established by

---

[291] ICCPR, art. 17." No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[292] *See* 138 CONG. REC. 8068–71 (1992) (ratifying the ICCPR with U.S. reservations, understandings and declarations (RUDs)); William A. Schabas, *Invalid Reservations to the International Covenant on Civil and Political Rights: Is the United States Still a Party?* 21 BROOK. J. INT'L. L. 277, 280–85 (1995) (analyzing the legal implications of the RUDs to the ICCPR). Congress declared the ICCPR non self-executing, meaning it does not create directly enforceable rights in domestic courts without implementing legislation. This principle was reaffirmed in *Medellín v. Texas,* 552 U.S. 491 (2008), where the Supreme Court ruled that ratified non self-executing treaties do not create enforceable domestic execution rights unless Congress enacts implementing legislation. The U.S. has historically appeared cautious in ratifying international human rights. To date, it has only ratified three of the nine core human rights treaties and only after significant delays: the International Covenant on Civil and Political Rights (ICCPR), adopted in 1966 and ratified by Congress in 1992, the International Convention on the Elimination of All Forms of Racial Discrimination (CERD), adopted in 1965 and ratified in 1994, and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT), adopted in 1984 and ratified in 1994.

[293] Timothy E. Lynch, *The ICCPR, Non-Self-Execution, and DACA Recipients' Right to Remain in the United States*, 34 GEO. IMMIGR. L.J. 323, 345–47 (2020) (discussing the ICCPR's privacy protections and its potential role in shaping U.S. policies on immigrant data collection and surveillance).

[294] U.S. CONST. art. VI.

Reid v. Covert.[295] In the absence of conflicting domestic law, international customary law is also binding on the U.S. [296] Therefore, the U.S. authorities and Courts have to understand and interpret domestic statutes in a manner consistent with international obligations whenever possible.[297] International legal instruments are essential in protecting individual autonomy and attendant civil rights.[298] They complement national efforts by providing additional frameworks for monitoring and enforcing civil and human rights protections.[299]

Given the UDHR and the ICCPR's clear recognition of privacy as a fundamental human right, U.S. immigration authorities should uphold this protection for all individuals under their jurisdiction. This obligation extends to safeguarding the privacy of the (in)visible immigrant.

U.S. refugee and asylum laws are deeply rooted in international legal frameworks. In 1968, the U.S. acceded to the 1976 U.N. Protocol Related to the Status of Refugees, incorporating the 1951 United Nations Convention Relating to the Status of Refugees. In addition, international human rights instruments use inclusive language—terms like "all" and "everyone"—to ensure that no one is discriminated against based on culture, religion, nationality, race, language, or immigrant status.[300] As marginalized and vulnerable

---

[295] *See* Reid v. Covert, 354 U.S. 1, 16–17 (1957); Boos v. Barry, 485 U.S. 312, 324 (1988) (stating that "it is well-established that 'no agreement with a foreign nation can confer power on the Congress, or on any other branch of Government, which is free from the restraints of the Constitution.'") (quoting *Reid*, 354 U.S. at 16 (plurality opinion)); Am. Ins. Ass'n v. Garamendi, 539 U.S. 396, 416 n.9 (2003) (stating that the power of a treaty to preempt state law is "[s]ubject . . . to the Constitution's guarantees of individual rights").

[296] The Paquete Habana, 175 U.S. 677, 700 (1990) ("International law is part of our law, and must be ascertained and administered by the courts of justice of appropriate jurisdiction, as often as questions of right depending upon it are duly presented for their determination.").

[297] *See* Murray v. Schooner Charming Betsy, 6 U.S. 64, 118 (1804) ("[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains.").

[298] *See* Jaunius Gumbis, Vytaute Bacianskaite & Jurgita Randakeviciute, *Do Human Rights Guarantee Autonomy?* 62 CUADERNOS CONSTITUCIONALES DE LA CÁTEDRA FADRIQUE FURIÓ CERIOL 77, 91 (2008) (arguing that each state is internationally obliged to ensure the protection of human rights); Louis Henkin, *The Universality of the Concept of Human Rights*, 506 ANNALS AM. ACAD. POL. & SOC. SCI. 10, 11 (1989).

[299] Liza J. Laplante, *Bringing Effective Remedies Home: The Inter-American Human Rights System, Reparations, and the Duty of Prevention*, 22 NETH. Q. HUM. RTS. 347, 357 (2004).

[300] UDHR, art. 1 ("All human beings are born free and equal in dignity

individuals, refugees and asylum seekers are protected under the 1951 Refugee Convention[301] and the Declaration on the Rights of Persons Belonging to National or Ethnic, Religious, and Linguistic Minorities.[302] Additionally, the preamble to the Declaration states that it aims to promote effective human rights implementation for minorities, inspired by Article 27 of the ICCPR.[303] It applies to all individuals, not just citizens, emphasizing the obligation of nations to protect these rights for everyone under their jurisdiction.

Many international legal instruments protect civil and human rights and ensure equal protection for all individuals, and they would serve in the protection of privacy as a human right. The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) is also an international instrument for which one can advocate for the protection of immigrants, including refugees and asylum seekers. This convention defines discrimination as any exclusion based on race, color, descent, or national or ethnic origin that impairs human rights.[304] With the recognition of privacy as a fundamental human right, the exclusionary surveillance targeting refugees and asylum seekers with their intersectional identities should be considered a violation of the ICERD. By recognizing such technology-enabled exclusions as discriminatory, the ICERD protects the rights of refugees and asylees who often belong to racially marginalized groups.

With the increased use of digital technology and the heightened risk of privacy violations, the United Nations General Assembly adopted the resolution The Right to Privacy in the Digital Age in 2013.[305] This resolution underscores the importance of protecting privacy in the increasingly digitized world. In 2014, the American Civil Liberties Union (ACLU) recommended updating General Comment 16 to address the digital economy's data collection practices.[306]

---

and rights."); ICCPR art. 1 ("All peoples have the right of self-determination.").

[301] Convention Relating to the Status of Refugees art. 1, July 28, 1951, 189 U.N.T.S. 137, as modified by Protocol Relating to the Status of Refugees, Jan. 31, 1967, 606 U.N.T.S. 267.

[302] GA Res. 47/135, Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities (Dec. 18, 1992).

[303] ICCPR, Art. 27.

[304] International Convention on the Elimination of All Forms of Racial Discrimination art. 1(1), Dec. 21, 1965, S. Exec. Doc. C, 95-2 (1978); S. Treaty Doc. 95-18; 660 U.N.T.S. 195, 212.

[305] G.A. Res. 68/167, International Convention on the Elimination of All Forms of Racial Discrimination (Dec. 18, 2013).

[306] *See* ACLU, INFORMATIONAL PRIVACY IN THE DIGITAL AGE, A PROPOSAL TO UPDATE GENERAL COMMENT 16 (RIGHT TO PRIVACY) TO THE

As technology advances, these international frameworks can significantly enhance the privacy of all humans.[307] The rapid development of AI and machine learning as applied to automated decision-making in immigration presents new and complex challenges, heightening the urgency for more robust legal protections, particularly for vulnerable populations, including refugees and asylum seekers.[308] It should be noted that I do not seek to assert a unique or privileged position for the data protection of refugees or asylum seekers. However, we must recognize and ensure human dignity through the protection of privacy—a fundamental human right not restricted to any given country's citizens or individuals with exclusive standing. This approach will ensure the upholding of the principles of non-discrimination and equal protection, recognizing every person's intrinsic human dignity and equality, regardless of their nationality or social standing.

A human rights approach to privacy, grounded in international legal instruments, requires legal recognition and understanding within the context of the U.S.'s domestic outlook. Additionally, it necessitates a careful balance between national security interests and individual privacy protections. Navigating this delicate intersection is essential in the effort to safeguard citizens' safety while addressing the unique privacy vulnerabilities of refugees and asylum seekers.

1. *The Domestic Outlook of Privacy as a Human Right*

Privacy as a human right is a crucial normative foundation for advancing positive law and public policy. In *Griswold v. Connecticut*, the Supreme Court linked privacy ideals to constitutional liberties of speech, association, religion, education, and intimate conduct.[309] Moreover, privacy ideals have recently been linked to civil rights in the United States.[310] Privacy is notoriously rich in meaning yet devoid of an agreed-upon, uniform definition.[311]

INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (2015).

[307] *See* Diggelmann & Cleis, *supra* note 288, at 448 (explaining that privacy gained recognition as an international human right through global agreements and conventions, eventually becoming a guaranteed principle within various nations' national constitutions and statutes).

[308] MOLNAR, *supra* note 21, at 91–115.

[309] Griswold v. Connecticut, 381 U.S. 479, 483–86 (1965).

[310] *See* Allen & Muhawe, *supra* note 19, at 12–26 (documenting the emergence of privacy as a civil right and civil rights protectant).

[311] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477 (2006) (noting that the concept of privacy is in disarray, that no one can definitively articulate what it truly means); *see also* Woodrow Hartzog, *What is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1677 (2021) (observing that privacy has always evaded precise

It is noteworthy that despite the numerous attempted definitions over time, shared understandings of its value associate privacy with norms that fundamentally protect and advance valuable ideals of agency, autonomy, and self-determination.[312] The absence of these ideals would risk undercutting the possibility of human flourishing, thereby making privacy rights particularly important.[313]

Understanding privacy from the human rights perspective and acknowledging its ideals provides context for addressing digital discriminatory practices against the (in)visible immigrant.[314] Personal data has frequently been leveraged to exclude immigrants from accessing opportunities, including education, and to target them for redlining, ultimately resulting in discrimination.[315] These practices affect access to housing, jobs, health care, insurance, and education opportunities.[316] The invitation to recognize privacy ideals from a human rights perspective highlights the apparent shortcomings of the U.S.'s neoliberal or market-driven approach to data protection, which prioritizes corporate interests at the expense of marginalized communities.[317] The human rights approach to

---

meaning); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (defining privacy as "the right to be let alone"); IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 11 (1975) (defining privacy as the process by which individuals or groups negotiate boundaries through letting others in or keeping them out). *See generally* BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984) (defining privacy as electing whether to decline access to one's person, to avoid observation by others, or to hold back information about oneself in certain situations).

[312] *See* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 35–45 (1988); *cf.* Anita L. Allen, *Privacy, Critical Definition, and Racial Justice*, *in* OXFORD HANDBOOK OF APPLIED PHILOSOPHY OF LANGUAGE 349, 351–56 (Luvell Anderson & Ernie Lepore eds., 2024) (identifying problems "defining" privacy in a politicized contemporary context).

[313] *See* LESLIE P. FRANCIS & JOHN G. FRANCIS, PRIVACY: WHAT EVERYONE NEEDS TO KNOW 2 (2017).

[314] *See* EUBANKS, *supra* note 8, at 28–34, 112–26.

[315] *See* SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 1 (2018) (arguing that algorithms enforce oppressive social relationships and create new racial profiling methods termed "technological redlining").

[316] EUBANKS, *supra* note 8, at 51, 78–83, 116–20.

[317] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 9 (2015); *see* BRIDGES, *supra* note 8, at 65–68, 73, 85–86 (detailing how needy families must permit unconstitutional state intrusions to receive social welfare benefits).

privacy offers a panacea to such commercial exploitation. Beyond ensuring the balance of corporate interests and the individual's human rights interests, this framework would also serve in curtailing government surveillance against the marginalized with adequate oversight.

Given the overdependence on automation in critical decision-making, the social cost of ignoring the ideals of privacy as viewed from a human rights perspective risks a continued state of "automated inequality."[318] These inequalities manifest in the form of information privacy violations and the ensuing harms of racial discrimination, misinformation, and targeted manipulations that disproportionately harm marginalized communities.[319] Recognizing ideals from a human rights perspective is crucial, especially given the outdated federal data privacy statutes that fail to protect the civil and human rights of the marginalized, including refugees and asylum seekers.[320] Federal statutes designed to prevent unfair treatment and discrimination against the marginalized need to be aligned with the modern digital technology landscape and law enforcement practices.[321] The current data privacy laws not only fail to protect refugees and asylum seekers but also citizens, as they do not adequately address their privacy needs.

Protecting privacy as a fundamental human right significantly benefits refugees and asylum seekers through the existing international human rights implementation framework.[322] Human rights instruments elevate domestic expectations for government compliance.[323] The human rights compliance framework has the

---

[318] *See* EUBANKS, *supra* note 8, at 78–83, 116–20.

[319] *See* Chao, et al., *supra* note 22, at 11–15.

[320] *See* Donohue, *supra* note 18, at 408 (noting that some U.S. privacy law is obsolete in the context of new and emerging technology). Some of the existing privacy laws include the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2523, 2701–2710, 3121 (comprising the Wiretap Act, the Stored Communication Act, and the Pen Register Act); the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681; and the Genetic Information Nondiscrimination Act of 2008 (GINA), 42 U.S.C. § 2000ff et seq.

[321] *See* Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241 (codified as amended in scattered sections of 42 U.S.C.); Equal Credit Opportunity Act of 1974, Pub. L. No. 93-495, 88 Stat. 1521 (codified as amended at 15 U.S.C. § 1691–1691f); Fair Housing Act of 1968, Pub. L. No. 90-284, 82 Stat. 81 (codified as amended at 42 U.S.C. §§ 3601–3619, 3631).

[322] Cosette D. Creamer & Beth A. Simmons, *The Proof is in the Process: Self-Reporting Under International Human Rights Treaties*, 114 AM. J. INT'L L. 1, 36–37 (2020); BETH A. SIMMONS, MOBILIZING FOR HUMAN RIGHTS: INTERNATIONAL LAW IN DOMESTIC POLITICS 4–5 (2009).

[323] Geoffrey P.R. Wallace, *International Law and Public Attitudes*

potential to overcome the over-politicization of immigration debates, ensuring that individual rights are protected regardless of citizenship status. In the U.S., immigration is a sensitive, highly politicized, and contested issue.[324] Consequently, there is minimal interest and pressure on legislators to pass privacy protection legislation that benefits them. The likelihood of passing privacy protection legislation with refugees and asylum seekers in mind is overshadowed by the political undertones and discomfort surrounding immigration debates, making such reforms appear out of reach. The existing contention around immigration as a general matter, coupled with the absence of a voting bloc advocating for legislative change, pushes privacy protection for refugees and asylum seekers to rank lower on the legislative agenda. This is despite the fact that privacy is a fundamental human right worthy of protection regardless of citizenship status.

The near-universal ratification of international instruments, including those affirming privacy as a human right, should serve as a reference point for domestic understanding and policies.[325] Framing privacy as a fundamental human right based on international treaties may help build consensus and shape perceptions of universally acceptable treatment of individuals' privacy interests, regardless of their citizenship status. Furthermore, human rights' formal and universally acceptable nature enhances their influence on public appreciation and normative aspirations.[326] Therefore, recognizing privacy as a fundamental human right of refugees and asylum seekers helps overcome the politically charged and biased perspectives on immigration issues in the U.S.

The domestic recognition of privacy as a human right is nuanced, as DHS and its immigration agencies must balance privacy rights with national security interests while processing immigration and asylum claims. This complex interplay between safeguarding the

---

Toward Torture: An Experimental Study, 67 INT'L ORG. 105, 105–06, 111 (2013).

[324] *See* Jessica Bolter, *Immigration Has Been a Defining, Often Contentious, Element Throughout U.S. History*, MIGRATION POL'Y INST. (Jan. 6, 2022), https://www.migrationpolicy.org/article/immigration-shaped-united-states-history [https://archive.ph/7l1JR]; Lawrence H. Yang, Maureen A. Eger & Bruce G. Link, *The Human Cost of Politicizing Immigration: Migration Stigma, US Politics, and Health*, 332 J. AM. MED. ASS'N 619 (2024), doi:10.1001/jama.2024.11126.

[325] Creamer & Simmons, *supra* note 322, at 37.

[326] *See* Burns H. Weston, *The Universality of Human Rights in a Multicultured World: Toward Respectful Decision-Making*, *in* THE FUTURE OF INTERNATIONAL HUMAN RIGHTS 65 (Burns H. Weston & Stephen P. Marks eds.,1999) (pointing to the universality and broad acceptance of human rights).

nation and respecting individual privacy rights sets the stage for a deeper examination of the tension between privacy and security.

2. *Privacy versus National Security*

National security concerns have long been cited as the primary justification for extensive data collection efforts aimed at protecting citizens.[327] This would likely pose a challenge to the framework of privacy as a human right. While national security is undeniably important, it must be balanced with privacy, a fundamental human right. Additionally, while national security is key, it is important to recognize that the benefits of privacy extend beyond an individual, fostering broader societal well-being and democratic engagement.

Discretionary power exercised in national security measures, particularly in data collection, has often been abused, with arbitrary data collection from immigrants without transparency or accountability. A prime example is the lack of transparency in handling data collected by the CBP One app, both during its operation and after its functionalities were discontinued by the Trump administration on January 20, 2025, which raises serious questions. This opacity heightens the risk that such data could be misused to the detriment of individuals, including for deportation. Further exacerbating these concerns, ICE agents have sought sensitive personal information from unlikely sources, such as abortion clinics, elementary schools, and utility companies.[328] This excessive and indiscriminate data collection, justified under the banner of national security, has led to the misuse of innocuous personal information, resulting in surveillance, exclusion, discrimination, detention, and deportation.[329]

---

[327] *See* JIMMY GURULE, GEOFFREY CORN, ERIC JENSEN & PETER MARGULIES, NATIONAL SECURITY LAW: PRINCIPLES AND POLICY 196 (2015).

[328] Dhruv Mehrotra, *ICE Is Grabbing Data from Schools and Abortion Clinics*, WIRED (Apr. 3, 2023, 7:00 AM), https://www.wired.com/story/ice-1509-custom-summons/ [https://perma.cc/8AGX-3ULG].

[329] Jize Jiang & Edna Erez, *Immigrants as Symbolic Assailants: Crimmigration and Its Discontents*, 28 INT'L CRIM. JUST. REV. 5, 11 (2017); MUSKAN MOMIN, ALICE MIN & NIKO MARCICH, AM. BAR ASS'N COMM'N ON IMMIGR., ELECTRONIC MONITORING OF MIGRANTS: PUNITIVE NOT PRUDENT 3–6 (2024), https://www.americanbar.org/content/dam/aba/administrative/immigration/electronic-monitoring-report-2024-02-21.pdf [https://archive.ph/7OpK4] (observing that immigrants are subjected to surveillance from arrival until either deported, granted permanent residency and beyond).

A common justification for extraneous and invasive data collection in the name of national security is the oft-repeated line that "if one has nothing to hide, they have nothing to fear."[330] This is a dangerously reductive argument when applied to refugees and asylum seekers. While individuals who pose legitimate threats to national security warrant scrutiny, a broad and indiscriminate application of surveillance where every immigrant is considered a security risk undermines privacy. Privacy is not merely about concealing wrongdoing; it is foundational to human dignity and self-determination regardless of citizenship status.[331] The danger is that treating every immigrant as a potential security threat effectively criminalizes their existence, legitimizes excessive data collection and surveillance, and erodes their fundamental human rights.

National security concerns are often cited as justification for exclusions, restricting and delaying citizenship and immigration benefits such as family reunification.[332] This results in unintended consequences, especially harm to children. For instance, certain national security programs, including the Controlled Application Review and Resolution Program (CARRP), have resulted in long delays and denial of citizenship and other immigration benefits for individuals from Muslim-majority countries without adequate explanation and transparency.[333] The program has been criticized for its overbroad criteria, which can place individuals under suspicion based on unsubstantiated connections to national security concerns.[334]

National security has long been invoked as a rationale for the surveillance, targeting, and exclusion of immigrant communities throughout U.S history.[335] During the Palmer raids of 1919–1920, the

---

[330] *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 21–24, 66–70 (2011) (explaining the notion- "nothing to hide no fear" and the improper use of national security).

[331] ALLEN, UNEASY ACCESS, *supra* note 312, at 35–48.

[332] *See* Katherine Yon Ebright, *The Alien Enemies Act*, BRENNAN CTR FOR JUST. (Oct. 10, 2024), https://www.brennancenter.org/our-work/policy-solutions/alien-enemies-act [https://perma.cc/7AG8-VGDQ] (discussing the use of national security concerns to justify exclusions and restrictions on immigrants).

[333] ACLU, DELAY AND DENY: HOW THE U.S. GOVERNMENT CONDEMNS ASPIRING AMERICANS TO IMMIGRATION PURGATORY (July 10, 2024), https://www.aclu.org/documents/delay-and-deny [https://perma.cc/E9MC-9G9Y]; Edward Alden, *National Security and U.S. Immigration Policy*, 1 ST. JOHN'S J. INT'L & COMPAR. L. 19 (2010).

[334] ACLU, *supra* note 306 at 11–13.

[335] *See* MOMIN, ET AL., *supra* note 328, at 3–5; *see also* Alden, *supra* note 332 at 20–29 (explaining how, since the September 11 attacks, national security arguments have been used to expand immigration enforcement and

U.S. government engaged in widespread targeting and deportation of Russian and Eastern European immigrants.[336] During World War II, census data was misused to identify and detain Japanese Americans.[337] This resulted in *Korematsu*, where the Supreme Court upheld Executive Order 9066, an exclusionary order that allowed the forced internment of Japanese Americans during the war.[338] The Court ultimately ruled against Korematsu, finding that national security interests outweighed individual rights during wartime and in national emergencies.[339] This precedent continues to symbolize the dangers of unchecked government power against those perceived as threats to national security, with immigrants often becoming the first victims of this amorphous notion—one that can be stretched to mean almost anything.

Decades after *Korematsu*, the ruling in *Trump v. Hawaii* reflected the continued struggle to balance national security concerns with individual rights.[340] In 2017, President Trump's "travel ban" restricted applications and travel from Muslim-majority countries, North Korea, certain Venezuelan officials, and the United States Refugee Admission Program (USRAP), citing national security reasons.[341] The ban was challenged in *Trump v. Hawaii,* where the Supreme Court upheld it, with Chief Justice John G. Roberts affirming that the president had broad discretion under the INA to restrict entry of non-citizens for national security reasons.[342] In her dissent, Justice Sonia Sotomayor compared the decision to *Korematsu,* warning that the Court was repeating past mistakes by sanctioning discrimination under the banner of national security.[343]

While Chief Justice Roberts in his majority opinion stated that *Korematsu* was "gravely wrong the day it was decided" and had no place under the Constitution,[344] which creates a question of whether

---

restrict entry for all immigrants).

[336] Harlan Grant Cohen, *The (Un)favorable Judgment of History: Deportation Hearings, the Palmer Raids, and the Meaning of History*, 78 N.Y.U. L. Rev. 1431, 1436, 1458 (2023).

[337] Lori Aratani, *Secret Use of Census Info Helped Send Japanese Americans to Internment Camps in WWII,* WASH. POST. (Apr. 3, 2018), https://www.washingtonpost.com/news/retropolis/wp/2018/04/03/secret-use-of-census-info-helped-send-japanese-americans-to-internment-camps-in-wwii/ [https://archive.ph/9aCiH].

[338] 323 U.S. 214, 223 (1944); Exec. Order No. 9066, 7 Fed. Reg. 1407 (Feb. 25, 1942).

[340] 585 U.S. 667 (2018).

[341] Proclamation No. 9645, 82 Fed. Reg. 45161 (Sept. 24, 2017).

[342] 585 U.S. 667 (2018).

[343] *Id.* at 754 (Sotomayor, J., dissenting).

[344] *Id.* at 710.

this constituted a formal overruling. Peter Margulies has criticized the Court's ruling and observed that upholding President Trump's 2017 travel ban orders, without considering the INA and its statutory context, armed the executive branch with a "loaded weapon" for further executive branch abuses in the name of national security.[345]

Post-9/11, the U.S. government intensified surveillance of Muslim, Arab, and South Asian communities using the PATRIOT Act of 2001, a continuation of the discriminatory practices under the national security justification.[346] These practices inevitably resulted in disproportionate violations against these communities, including citizens.

The courts have often supported these facially unfair and absurd discriminatory and exclusionary measures at the expense of the vulnerable in society. In 1943, the Supreme Court's unanimous decision in *Hirabayashi v. United States* upheld a dusk-to-dawn curfew imposed on Japanese Americans, paving the way for broader injustices like mass internment, surveillance, and exclusion of migrant and other minority communities, weeks before the implementation of the mass removal orders of *Korematsu*.[347] These were targeted, extreme exclusionary measures that are manifesting in the current administration.

As the ACLU stated, "[T]he legitimate concern of the government with national security does not give it the right to know anything it may want to know about anyone. . . Americans are accustomed to a government of law, not of men and not of discretion."[348] Therefore, balancing the government's national security interests with human rights is imperative.

The privacy-as-human-right approach aligns with the traditional principles of political thought that security encompasses fundamental rights, mental well-being, and the absence of danger envisioned in a civil state where comprehensive security means equality.[349] This approach ensures that national security measures do not compromise essential human rights and maintains security and accountability.

---

[345] *See* Peter Margulies, *The Travel Ban Decision, Administrative Law, and Judicial Method: Taking Statutory Context Seriously*, 33 GEO. IMMIGR. L.J. 159, 160, 163 (2019) (arguing that *Hawaii* granted excessive deference to the executive branch, enabling abuses through an isolated reading of the INA).

[346] Pub. L. No. 107-56, 115 Stat. 272 (2001). *See generally* Khaled A. Beydoun, *Acting Muslim*, 53 HARV. C.R.-C.L. L. REV. 1, 30–31 (2017).

[347] 320 U.S. 81, 92 (1943).

[348] *See* PACKARD, *supra* note 276, at 123.

[349] *See* FRÉDÉRIC GROS, THE SECURITY PRINCIPLE: FROM SERENITY TO REGULATION 75–78 (2019).

B. THE RIGHT TO DATA DELETION

One effective approach to protecting the privacy rights of vulnerable populations is establishing the right to data deletion upon attainment of citizenship, ensuring that data retention does not extend beyond what is necessary to determine refugee or asylum status and the naturalization process.

The right to data deletion will not require reinventing the wheel, as it aligns naturally with the U.S.'s existing immigration-to-citizenship framework. It would fit within the existing immigration framework, albeit with modifications and adaptations. Foreign-born individuals who become U.S. citizens must fulfill various requirements, such as being a lawful permanent resident for a period ranging from three to five years.[350] They must demonstrate good moral character[351] and pass a civics and English language examination.[352] The rigorous pathway to naturalization, coupled with taking an oath of allegiance, demonstrates an individual's commitment to U.S. values.[353] This rigorous process justifies supporting the right to data deletion, as it effectively balances national security with privacy interests.

Allowing individuals to regain control over their personal information through data deletion would advance the protection of their dignity and enable them to shape their personal narratives and history as they integrate and rebuild their lives in new communities. Upon the grant of citizenship, individuals gain rights and responsibilities, such as the right to vote,[354] the right to hold federal office (except the presidency),[355] and access to federal benefits and programs.[356] Similarly, they should be granted automatic data deletion within the immigration framework.[357]

The right to data deletion should be adopted as a privacy-based "right against data retention." This is grounded in a solid moral foundation proposed by Anita Allen, in *Dredging Up the Past: Lifelogging, Memory, and Surveillance*, wherein she underscores the

---

[350] 8 U.S.C. § 1430(a)–(b).

[351] 8 C.F.R. § 316.10(b) (2025).

[352] 8 U.S.C. § 1423.

[353] *See* 8 U.S.C. § 1427 (detailing the requirements for naturalization); 8 U.S.C. § 1448 (prescribing the Oath of Allegiance).

[354] 52 U.S.C. § 10101(a)(1).

[355] 8 U.S.C. § 1427. This provision confers citizenship, which implicitly includes the right to hold public office except the presidency. See U.S. CONST. art. II, § 1, cl. 5, on qualifications for the President.

[356] 8 U.S.C. § 1611.

[357] Moreover, the Fair Information Practice Principles (FIPPs) include the principle that data should be deleted when the purposes for which it was collected have expired.

importance of allowing individuals to distance themselves from their past misfortunes, asserting a "need to be safe from memory."[358] She emphasizes that such safety from memory creates a necessary balance that benefits both individuals and society.[359] In this way, the right to data deletion for data held by immigration authorities and their private contractors would grant individuals greater control over their sensitive information, enhancing dignity and self-determination.

The right to data deletion benefits society by fostering a freer and inclusive polity where individuals are liberated from the burden of past information held by authorities, ultimately contributing to increased social cohesion and trust and encouraging civic engagement. This is particularly significant given the wealth of personal information refugees and asylum seekers must disclose about themselves and their families. The information they surrender includes details of survival through war, persecution, torture, rape, and other traumatic experiences. They should be afforded the right to have these pieces erased once they attain citizenship. Ensuring that this sensitive information is not held indefinitely restores their dignity, self-worth, personal agency, and self-determination, helping them rebuild their lives in new communities.

The right to data deletion closely parallels the legal concept of expungement. Expungement entails destroying or sealing criminal records from court systems or police divisions.[360] Like expungement, which enables formerly incarcerated individuals to reintegrate into society by erasing certain records, the right to data deletion would allow refugees and asylum seekers a path to rebuild their lives without the burden of past traumatic records.[361] Most states in the U.S. provide juveniles with the right to request expungement, enabling them to have their conviction records sealed.[362] Although

---

[358] Anita L. Allen, *Dredging Up the Past: Lifelogging, Memory, and Surveillance,* 75 U. CHI. L. REV. 47, 57 (2008).

[359] *Id.* at 47.

[360] *See What is "Expungement?",* AM. BAR ASS'N (Nov. 20, 2018), https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-_expungement-/ [https://archive.ph/3jRuI].

[361] *See generally* MARGARET COLGATE LOVE, COLLATERAL CONSEQUENCES RES. CTR., THE MANY ROADS FROM REENTRY TO REINTEGRATION: A NATIONAL SURVEY OF LAWS RESTORING RIGHTS AND OPPORTUNITIES AFTER ARREST OR CONVICTION (2022), https://ccresourcecenter.org/wp-content/uploads/2022/08/MRFRTR_8.24.22.pdf [https://perma.cc/LX9S-VFDR].

[362] *See* J.J Prescott & Sonja B. Starr, *Expungement of Criminal Convictions: An Empirical Study*, 133 HARV. L. REV. 2460, 2483, 2502 (2020).

refugees and asylum seekers are not criminals, both groups face barriers due to their past information, such as exclusion from employment and housing.[363] Expungement laws and proceedings have been widely adopted across the country as a dignified means of facilitating the reentry of formerly incarcerated individuals into society.[364] These laws allow formerly incarcerated individuals to have their criminal records sealed or set aside, improving their chances of reintegration, obtaining employment, securing housing, accessing other social services, and other opportunities.[365] Similarly, recognizing the right to data deletion upon attainment of citizenship fosters integration, allowing refugees and asylum seekers to rebuild their lives free from their past burdens and systemic surveillance records.

A right to data deletion for refugees and asylum seekers would not be unprecedented in the U.S. The California Consumer Privacy Act (CCPA) already grants California residents the right to request that businesses delete their personal information, illustrating that such protections are achievable within the existing legal framework.[366]

The U.S. Video Privacy Protection Act (VPPA) is a valuable model for structuring a right to data deletion for refugees and asylum seekers. The VPPA mandates video service providers to delete personally identifiable information about the consumer's rental or purchases "as soon as practicable," but no later than one year after

---

[363] *See generally* Suchismita Bhattacharjee & Chie Noyori Corbett, *Housing Condition and Preferences of Refugee Immigrants in Dallas, TX*, 4 WELLBEING, SPACE & SOC'Y 100150 (2023), https://doi.org/10.1016/j.wss.2023.100150.

[364] *See generally* Restoration of Rights Project, *50-State Comparison: Expungement, Sealing & Other Record Relief*, COLLATERAL CONSEQUENCES RES. CTR., https://ccresourcecenter.org/state-restoration-profiles/50-state-comparisonjudicial-expungement-sealing-and-set-aside-2-2/ [https://perma.cc/BY68-R2KB] (last updated July 2024) (providing a comprehensive analysis of state laws on expungement, sealing, and record relief).

[365] *See* JOSHUA GAINES, THE COUNCIL OF STATE GOV'TS JUST. CTR., BEYOND CONFIDENTIALITY: MODERNIZING CRIMINAL RECORD CLEARANCE POLICIES IN THE DIGITAL AGE 1–2 (2023), https://csgjusticecenter.org/publications/beyond-confidentiality-modernizing-criminal-record-clearance-policies-in-the-digital-age-2/ [https://perma.cc/8S88-GVJF] (discussing how expungement and sealing laws support reintegration by reducing barriers).

[366] CAL. CIV. CODE § 1798.130(a)(2)(A); *see* Reece Hirsch & Kristin M. Hadgis, *INSIGHT: California's New, GDPR-Like Privacy Law Is a Game-Changer*, BL (July 11, 2018), https://www.bloomberglaw.com/bloomberglawnews/bloomberg-law-news/X6Q3B7MC000000 [https://perma.cc/P3NF-7XTV].

the data is no longer necessary for its intended purpose.[367] This provision enforces clear data retention limits, requiring deletion once information is no longer needed for business purposes. It allows exceptions, such as data retention, if a consumer requests access or a court order requires it.[368] A similar framework could be adopted for refugees and asylum seekers, establishing firm but flexible retention limits that prevent the indefinite storage of sensitive data while allowing specific exceptions and legal obligations. By following the VVPA's approach, policymakers could effectively address concerns about excessive data retention, offering protection for vulnerable individuals within the data cycle while maintaining essential national security and immigration administrative functions.

The Children's Online Privacy Protection Act (COPPA) regulations grant parents the right to delete data collected from their children, especially when the data is no longer necessary for the purpose it was initially collected.[369] Similarly, refugees and asylees should be afforded a comparable right to have their sensitive data after the grant of citizenship. This would help them rebuild their lives without the weight of their past.

This right to data deletion is in some respects akin to the European Union's right to be forgotten under the General Data Protection Regulation (GDPR), which, like this proposal, is grounded in the values of dignity. The GDPR grants individuals the right to have their data erased from databases under certain conditions, such as when the data is no longer necessary for the original purpose for which it was collected, when consent has been withdrawn, or when there are other legal grounds for erasure.[370] Although the right to be forgotten does not have a universally agreed-upon definition, it is generally understood as an individual's right to

---

[367] 18 U.S.C. § 2710(e).

[368] *Id.*

[369] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4(d)(3) (2021) ("[A] parent can review or have deleted the child's personal information and refuse to permit further collection or use of the child's information and state the procedures for doing so."); *id*. § 312.10 ("An operator of a Web site or online service shall retain personal information collected online from a child for only as long as reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.").

[370] Regulation (EU) 2016/679, art. 17 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 43–44.

request the removal of personal information from internet searches, databases, and other directories.[371]

However, the proposed right to data deletion is distinct from the right to be forgotten. The right to be forgotten is largely grounded in the idea of protecting individual privacy and controlling the dissemination of personal information that may be private or damaging when it appears on internet searches and public directories. On the other hand, the right to data deletion for refugees and asylees is primarily an anti-data retention principle. That is for information held by immigration and related authorities and their privacy contractors. To this extent, the proposed right to data deletion does not follow the traditional EU-style right to be forgotten as it emphasizes permanent data removal rather than obscurity.

The right to be forgotten in many ways does not require the deletion of data; instead, it is largely understood as a right to obscurity.[372] Under this right, the data remains intact but is removed from public visibility in search results as the original/primary data does not have to be deleted.[373] Specifically, search engines are obliged to de-link third-party web pages when the information is deemed "inadequate, irrelevant, or excessive."[374]

In contrast, the proposed right to data deletion for refugees and asylees prioritizes permanent erasure, addressing their unique vulnerabilities within the data lifecycle. Unlike the right to be forgotten, which merely obscures data, the right to data deletion would ensure that sensitive information is entirely removed, allowing individuals to regain control over their personal histories represented in their data as held by immigration authorities. By eliminating past records, the right to data deletion supports dignity, security, and a fresh start, offering protection beyond what the right to be forgotten may provide.

The GDPR's right to be forgotten does not apply to security-related data, as processing for state security purposes falls outside

---

[371] *See* Meg Leta Ambrose, *It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten*, 16 STAN. TECH. L. REV. 369, 375 (2013); Michael J. Kelly & David Satola, *The Right to be Forgotten*, 2017 U. ILL. L. REV. 1, 3 (2017); Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 90–91 (2012); Giancarlo F. Frosio, *The Right to Be Forgotten: Much Ado About Nothing*, 15 COLO. TECH. L.J. 307, 307–15 (2017) (discussing the different views on the right to be forgotten).

[372] Evans Selinger & Woodrow Hartzog, *Google Can't Forget You, but It Should Make You Hard to Find*, WIRED (May 20, 2014, 3:33 PM), https://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/ [https://perma.cc/CL9K-XHE9].

[373] Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 1019 (2023).

[374] *Id.*

the regulation's scope.[375] This suggests that an EU-style right to be forgotten may not be applicable in the immigration context, as national security is often cited to justify extensive data collection and prolonged retention periods for refugees and asylees. Therefore, the right to data deletion is designed to cover information exempted by the GDPR's right to be forgotten provision, providing a more comprehensive privacy safeguard. This modification and adaptation approach offers complete protection for privacy for information that the GDPR carves out.

Despite its benefits, the right to data deletion could encounter challenges similar to those faced by the right to be forgotten in the U.S., particularly under the First Amendment, which safeguards the public's right to know.[376] In *Cox Broadcasting v. Cohn*, the Supreme Court ruled in favor of a reporter who disclosed a deceased rape victim's name, determining that the public's right to know outweighed privacy concerns.[377] The Court held that "[e]ven the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information already appears on the public record."[378] This case, like others, suggests that the right to be forgotten and, in this circumstance, the proposed right to data deletion may be in tension with First Amendment principles.[379]

While making a case for the right to be forgotten, Eric Posner argues that the First Amendment can accommodate and coexist with privacy interests, drawing parallels between the right to be forgotten and historical barriers that once limited access to personal information.[380] This approach advances compelling privacy interests without unduly restricting free speech or access to information about ordinary individuals. Building on this idea, in the case of refugees and asylees, the public interest in accessing details of their traumatic histories and related personal information is minimal when compared to the pressing need for data deletion, which stands to

---

[375] Regulation (EU) 2016/679, recital 16, art. 2(2)(a), 2016 O.J. (L 119) 3, 32.

[376] *See* Chelsea E. Carbone, *To Be or Not to Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age*, 22 VA. J. SOC. POL'Y & L. 525, 555 (2015).

[377] 420 U.S. 469 (1975).

[378] *Id.* at 469.

[379] I conceptualize the right to data deletion as embodying some features of the right to be forgotten. For other cases on the First Amendment in this context, see, e.g., Florida Star v. B.J.F., 491 U.S. 524 (1989); Smith v. Daily Mail Pub. Co., 443 U.S. 97 (1979).

[380] Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014, 4:37 PM), https://slate.com/news-and-politics/2014/05/the-european-right-to-be-forgotten-is-just-what-the-internet-needs.html [https://perma.cc/TQ6U-U6EZ].

ensure their dignity, agency, security, self-determination, and protection as vulnerable individuals.

C. INDEPENDENT DATA PROTECTION AGENCY

To effectively safeguard the privacy rights of refugees and asylum seekers, data privacy reforms must be tailored to address their unique vulnerability and challenges throughout the data lifecycle. As a highly marginalized population, they are exposed to risks from commercial entities and immigration agencies, such as online profiling and algorithmic discrimination.[381] These challenges place them at a greater risk of privacy violations, making it crucial to establish protective frameworks designed explicitly for their circumstance. To ensure the enforcement of such frameworks, I propose the establishment of an Independent Data Protection Agency (IDPA) with a mandate of protecting privacy rights for all individuals within the U.S. Among its key functions, the IDPA should include a specialized office or unit focused on protecting the privacy rights of immigrants, particularly refugees and asylum seekers. The foundation for the functions of the IDPA should be based on the consideration of privacy as a fundamental human right.

There is an opportunity to adopt the IDPA. Rep. Cathy McMorris Rodgers (R-Wash.) and Sen. Maria Cantwell (D-Wash.) proposed the American Privacy Rights Act (APRA) last Congress with the aim of establishing a comprehensive baseline of U.S. consumer data protection.[382] The APRA bill builds upon the groundwork laid by the American Data Privacy and Protection Act (ADPPA) of 2022, which ultimately failed to be passed in Congress.[383] With the APRA pending consideration, Congress needs to include the IDPA as it aims to protect and enforce not only immigrants' privacy rights but also citizens' privacy. This is even more paramount as the civil rights protection provisions initially included in the bill have since been removed.[384] Above, the IDPA would be handy in protecting the

---

[381] *See* Johnson, *supra* note 115; Katie Kelly, *Enforcing Stereotypes: The Self-Fulfilling Prophecies of U.S. Immigration Enforcement*, 66 UCLA L. REV. DISCOURSE 36, 40 (2018) (examining the race-restrictive immigration system); Lai & Tanner, *supra* note 206 (noting that for "the marginalized group, the right to privacy is a matter of survival").

[382] *See* APRA, *supra* note 24.

[383] American Data Privacy Protection Act (ADPPA), H.R. 8152, 117th Cong. (2022).

[384] *See* Eric Null, *CDT and Allies Call on Congress to Restore Civil Rights Protections to* APRA, CTR. FOR DEMOCRACY & TECH. (June 25, 2024), https://cdt.org/insights/cdt-and-allies-call-on-congress-to-restore-civil-rights-protections-to-apra/ [https://perma.cc/9GD8-QA5A].

privacy rights of marginalized communities while upholding the human rights perspective.

The APRA proposes to empower the Federal Trade Commission (FTC) with the authority to enforce it, but more is needed to address and protect marginalized communities' specific privacy interests. The FTC's enforcement authority stems from Section 5 of the FTC Act, which prohibits unfair or deceptive trade acts or practices.[385] Refugees' and asylum seekers' interactions with immigration authorities are not commercial and or trade practices and in effect would not be addressed by the FTC. While the FTC would be crucial in the realm of commercial surveillance, it is often hampered by limited resources, leading to the selective enforcement of complaints.[386] With such an existent issue of a lack of resources, additional complaints from refugees and asylum seekers would not rank high in the FTC's priorities. Therefore, the proposed IDPA would fill the gap by addressing immigrants' privacy concerns.

The proposal herein follows the footsteps of previously proposed interventions. I propose modifications to previous efforts by primarily advocating for an intervention geared towards protecting the privacy rights of refugees and asylum seekers as a uniquely vulnerable population in the data lifecycle. In 2021, Sen. Kirsten Gillibrand (D-N.Y.) and Sen. Sherrod Brown (D-Ohio) introduced the Data Protection Act of 2021, which proposed the creation of a Federal Data Protection Agency (DPA).[387] Allen analyzed this bill in her work *The Black Opticon*, discussing its potential to advance what she defines as the African American Online Equity Agenda (AAOEA).[388] She acknowledges that the then-proposed bill with a provision creating the DPA was a step in the right direction for protecting against privacy harms and discrimination against African Americans.[389] I follow this route, but with the addition of the creation of a specialized unit or office that specifically attends to immigrants' privacy protection.

The proposed immigrants' unit under the IDPA would ensure transparency in the selection and supervision of contractors conducting surveillance on behalf of the immigration authorities.[390]

---

[385] 15 U.S.C. § 45(a).

[386] *See* David A. Hyman & William E. Kovacic, *Why Who Does What Matters: Governmental Design and Agency Performance*, 82 GEO. WASH. L. REV. 1446, 1474, 1484 (2014) (arguing that agencies are charged with many responsibilities and yet with frail resources that affect their performances).

[387] Data Protection Act of 2021, S. 2134, 117th Cong. (2021).

[388] Allen, *supra* note 8, at 928.

[389] *Id.* at 949–56.

[390] *See* Alex Heuer, *St. Louis asylum seekers demand end to abuse and monitoring by ICE contractor*, NPR ST. LOUIS (Apr. 24, 2023, 4:54 PM),

DHS has an internal privacy oversight framework that includes the Privacy Office, established under the Office of Civil Rights and Civil Liberties(CRCL), along with the Privacy and Civil Liberties Oversight Board (PCLOB), and officer training protocols, all designed to safeguard privacy.[391] While these mechanisms are intended to protect privacy for all individuals, privacy rights for immigrants, particularly refugees and asylum seekers, are often violated without accountability and meaningful protection from these offices. In 2020, the Biometrics Subcommittee of the Homeland Security Advisory Council released a report on privacy violations.[392] The Subcommittee proposed establishing a Biometric Oversight and Coordination Council (BOCC) led by the DHS.[393] The proposed IDPA is along these lines, and I support the BOCC-like approach but with adjustments and modifications toward adopting and establishing an independent privacy unit under the proposed IDPA. This unit should have no DHS affiliation to avoid a conflict of interest. The proposed IDPA would be ideal in this circumstance. Additionally, DHS is already burdened with multiple immigration matters and related duties, making it challenging to effectively address privacy-related issues relating to immigrants.

The proposed immigrants' privacy unit under the IDPA would be mandated to monitor the collection, use, analysis, and retention of immigrants' data held by both immigration authorities and commercial entities. It would also be responsible for monitoring immigration programs that are heavily reliant on digital surveillance. For example, it would address privacy violations within the ATD

---

https://www.stlpr.org/show/st-louis-on-the-air/2023-04-24/st-louis-asylum-seekers-demand-end-to-abuse-and-monitoring-by-ice-contractor [https://perma.cc/KVL3-QKED]; *see also* David Yaffe-Bellany, *"It's humiliating": Released immigrants describe life with ankle monitors*, TEX. TRIB. (Aug. 10, 2018, 12:00 AM), https://www.texastribune.org/2018/08/10/humiliating-released-immigrants-describe-life-ankle-monitors/ [https://perma.cc/R5QW-2E59].

[391] *See* 6 U.S.C. § 345; 6 U.S.C. § 142 (establishing the DHS Privacy Officer to oversee privacy compliance and protections); 42 U.S.C. § 2000ee (creating the Privacy and Civil Liberties Oversight Board to ensure executive actions respect privacy and civil liberties); U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM NO. 2008-01 at 4 (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf [https://perma.cc/Q6X3-DYWL] (outlining officer training protocols for privacy protection); U.S. CUSTOMS & BORDER PROT., DIRECTIVE NO. 2120-010A: PRIVACY POLICY, COMPLIANCE, AND IMPLEMENTATION (June 29, 2022).

[392] *See* U.S. DEP'T OF HOMELAND SEC. ADVISORY COUNCIL, FINAL REPORT OF THE BIOMETRICS SUBCOMMITTEE (Nov. 12, 2020).

[393] *Id.* at 2.

program, which relies on technologies such as ankle monitors and the now-discontinued CBP One app, both of which have location tracking capabilities.[394] These programs would be closely and independently monitored to ensure refugees' and asylum seekers' privacy.

Additionally, the IDPA would monitor the actions of commercial entities often contracted by immigration authorities to ensure proper and accountable handling of immigrants' data and adherence to stringent privacy standards.[395] Key enforcement duties of the IDPA would also include assessing privacy violation claims, granting relief and injunctions, and imposing fines against privacy-violating entities. The fines collected would be used to fund the administration of the IDPA to ensure its independence, sustainability, and operational efficiency.

Furthermore, the establishment of an immigrant's privacy unit under the IDPA would be a crucial step forward in rooting out algorithmic biases embedded in technologies deployed by immigration authorities and their contractors. The unit would act as a specialized section with authority to conduct human rights and civil rights impact assessments before these technologies are deployed. Technologies with potential algorithmic biases and discriminatory outcomes would be identified prior to deployment.

The IDPA, which would be a federal agency, is crucial for safeguarding individuals' privacy rights—an essential component of any functioning democracy, particularly in the modern digital era. However, I acknowledge that such an initiative may face opposition in the current political environment, which is largely influenced by major tech stakeholders that are opposed to federal agency regulation. Notably, Elon Musk has been associated with efforts to dismantle federal oversight agencies, such as the Consumer Financial Protection Bureau.[396] Moreover, recent Supreme Court

---

[394] *See* Wiener, *supra* note 128 (noting misuse of the ATD program); *Government Documents Reveal Information about the Development of the CBP One App*, AM. IMMIGR. COUNCIL (Feb. 28, 2023), https://www.americanimmigrationcouncil.org/foia/government-documents-reveal-information-about-development-cbp-one-app [https://perma.cc/3SH7-994U] (noting privacy violations via the CBP One app).

[395] *See* ELEC. PRIV. INFO. CTR., STATEMENT TO THE SENATE COMMERCE COMMITTEE: THE NEED FOR FEDERAL DATA PROTECTION LEGISLATION (2020), https://epic.org/wpcontent/uploads/testimony/congress/EPIC-SCOMEFederalPrivacyLegislation-Sept2020.pdf [https://perma.cc/239X-6YBX].

[396] *See* Bobby Allyn, *Elon Musk's DOGE Takes Aim at Agency That Had Plans of Regulating X,* NPR (Feb. 12, 2025, 5:00 AM)

rulings have significantly threatened the power of key federal agencies, including the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC).[397]

These decisions have emboldened corporations to question the purposes, structures, procedures, and constitutionality of agencies. Notably, Meta Platforms, Inc. (formerly Facebook) and X Corp. (formerly Twitter) are now challenging the FTC, CFPB, and other agencies under these precedents, further testing the limits of regulatory enforcement.[398]

While these decisions have raised concerns about the constitutional viability of federal agencies, they should not dissuade efforts to advocate for privacy protections through the proposed IDPA, which remains essential in an era of increasing digital surveillance and data exploitation. Despite challenges to agency power and constitutionality, particularly those raised by profit-oriented corporations, this should not reduce the need for privacy protection championed by the proposed IDPA. It should not be surprising that big tech corporations like Meta and X Corp. are leading the fight against regulatory and oversight agencies. Consumer protection and individual rights, including privacy rights, must remain paramount. Refugees' and asylum seekers' privacy rights should take precedence over profit. The establishment of the IDPA would be crucial for safeguarding individual privacy rights, a core necessity for any democracy, especially in today's digital age.

CONCLUSION

Refugees and asylum seekers striving to enter and reside safely in the United States are highly visible to data-collecting entities, yet "invisible" to the nation's privacy protection laws. They are vulnerable candidates for the massive data collection schemes by both government and commercial entities, subjecting them to

---

https://www.npr.org/2025/02/12/nx-s1-5293382/x-elon-musk-doge-cfpb [https://perma.cc/LX64-77NF].

[397] *See* Seila Law LLC v. Consumer Fin. Prot. Bureau, 591 U.S. 197, 205 (2020) (holding that the CFPB's structure violated the separation of powers because its single director was not removable by the President); Axon Enter., Inc. v. Fed. Trade Comm'n, 598 U.S. 175, 185 (2023) (holding that district courts have jurisdiction to hear constitutional challenges to the structure of the FTC and SEC before agency proceedings conclude, thereby limiting agency authority).

[398] *See* Tonya Riley & Katie Arcieri, *Meta Lawsuit a 'Serious Attack' on FTC Enforcement Authority*, BL (Dec. 1, 2023, 5:05 AM), https://news.bloomberglaw.com/privacy-and-data-security/meta-lawsuit-a-serious-attack-on-ftc-enforcement-authority [https://perma.cc/7PJR-65WU].

surveillance, discrimination, and commercial exploitation. It is vital to safeguard the (in)visible immigrant's privacy because the protection of privacy is integral to upholding human dignity in any democratic society. Privacy and related data protection measures advance their agency, autonomy, and self-determination. As explored herein, data surrender results in the yielding of excessive personal information in exchange for safety and necessities of life and services, stripping them of their agency. Constant surveillance forces them to curate their behavior and identity to fit authorities' expectations, resulting in a loss of self-esteem and subdued individuality, inhibiting their ability to express their true self. Additionally, personal data can be weaponized against them, leading to discrimination, targeted surveillance, and exclusion, undermining their efforts to fully integrate into society.

This Article invites lawmakers to consider bold policies in the face of striking realities. Contemplating novel policies is fully warranted. Looking ahead, the challenges faced by the (in)visible immigrant raise urgent and profound questions not only about the future of privacy for immigrants, but also about the broader contours of governance and national identity in the digital age. These concerns extend beyond immigrant populations and increasingly affect the rights and freedoms of citizens as well. As technologies evolve and datafication intensifies, the legal system must grapple with the normative implications of who is seen, remembered, or erased. Protecting the privacy of refugees and asylum seekers is not merely about safeguarding personal information. It is about affirming their humanity, acknowledging their dignity, and reimagining democratic inclusion in an era of pervasive digital surveillance that threatens every facet of life.