The Role of ICTs in the Maintenance and Reproduction of Digital Border Assemblages

Lubna Razaq
Dept of Human Centered Design Engineering
University of Washington
Seattle, Washington, USA
lubnar@uw.edu

Sucheta Ghoshal
Human Centered Design and Engineering
University of Washington
Seattle, Washington, USA
sghoshal@uw.edu

Abstract

In this paper, we extend the Digital Border Assemblages framework (DBA) by locating the role of ICTs in enabling means of racialized control at geographical boundaries or borders. Applying a critical-interpretive approach, we identify key features of DBA that contribute to such racial formations. We analyze three case studies of border technologies deployed at and beyond physical sites of border control: electronic device inspections, electronic location monitoring, and restricted transactions in financial technologies. Although a framework of DBA exists in the current paradigm of border studies, we argue that a close examination of the entanglements between borders and ICTs offers us key insights into how migrant bodies are subjected to racialized control at/by the border. Implications for HCI researchers include studying the experiences of those impacted by this assemblage and developing methods inspired by the legal field for studying these obscure systems.

CCS Concepts

• **Human-centered computing → HCI theory, concepts and models**; • **Social and professional topics → Governmental surveillance**; *Race and ethnicity*.

Keywords

migration, surveillance, ICTs, digital border assemblages, case studies, digital borders, race and privacy

ACM Reference Format:
Lubna Razaq and Sucheta Ghoshal. 2025. The Role of ICTs in the Maintenance and Reproduction of Digital Border Assemblages. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3706598.3713261

1 Introduction

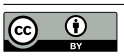
Western political discourse has centered on curtailing what policymakers frame as the 'threat' of immigrants. This focus has driven governments to steadily increase investment in border control, surveillance personnel, carceral facilities, and technologies over the years [28], a trend experts expect to continue into the foreseeable future [25, 90]. By labeling migrants as illegals, criminals, and terrorists—a threat to both the economy and security—policymakers have criminalized migration and militarized borders through police and surveillance technologies [127]. Lawmakers continue to push for greater investment in border technologies, emphasizing the critical role of technology and private companies in securing borders [25]

Research in HCI has examined how ICTs aid in integrating migrant populations including asylum seekers, immigrants, and refugees [7, 23, 24, 33, 45, 50, 77, 102, 119, 132]. These studies address topics such as language learning, digital literacy [91], access to technology, safety, gender issues [102], emotional barriers, and the fears and anxieties experienced by migrant families and laborers in accessing and using ICTs. They also examine co-designing with, rather than for, these populations [40], as well as the privacy challenges and practices of migrant communities in their use of ICTs [11, 42, 114, 119].

Our paper shifts the focus from the use of ICTs by migrant populations for integration to the use of ICTs by the state for social ordering, sorting, and mobility control, both within and beyond its borders. The purpose of this paper, therefore, is to extend the Digital Border Assemblage (DBA) framework proposed by the border studies scholars Chouliaraki and Georgiou [22], as outlined in §1.1. We expand on the existing understanding of the DBA framework by identifying a concrete set of features within this framework, analyzing the role of ICTs in creating or enabling these features, and discussing the resulting implications for HCI (see §6). We address the overarching research question: *How can HCI designers and researchers begin to understand the role ICTs play in the ongoing racialization of migrant bodies caused by border assemblages?*

Inspired by the paradigm of critical-interpretive research, our work consists of three stages. In the first stage, we reviewed the literature on critical border studies to develop conceptual foundations on the history and current state of border technologies, their artifacts, their entanglement with race, and the historical role of race in border practices. In the second stage, we developed three case studies on the use of ICTs in bordering namely: electronic device inspections at borders, electronic ankle monitoring, and financial remittance transactions. In the final stage of our work, adopting a critical-interpretive approach, we applied a critical analytical lens to the empirical evidence collected through these case studies.

Based on our analysis, we identify several key features of Digital Border Assemblages (DBA). These include racial and information profiling, discriminatory practices, making racial subjects legible to the state, obscurity, the expansion of bordering sites, the erosion of social relations, racialized surveillance through data extractions, and the self-enforcement of borders. These features lead to new



CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713261

forms of racialized control over marginalized and migrant bodies, even after they have crossed physical border sites.

We argue that the features of Digital Border Assemblage (DBA) are enabled by ICTs, specifically enabling new modes of racialized control at/by the border. Our findings also reveal that bordering sites have expanded spatially and temporally to include migrant bodies, families, communities, traveler devices, data, online activities, digital relationships, and financial transactions. By surveilling migrants, immigrants, and racialized citizens through ICTs, community, and familial relations are weaponized and extracted as data by the authorities. Location monitoring and device inspection policies force data extraction and self-disclosure. Furthermore, individuals enforce borders on themselves to avoid the adverse consequences of ICT-enabled surveillance.

Finally, we recommend that the HCI research community respond by interrogating the role of DBA and adopting methods inspired by legal studies to address its obscurity. This includes identifying and studying new sites of bordering and underrepresented narratives, foregrounding race and relationality in discussions of privacy and migration, and exploring how migration, citizenship, and activism are performed within the evolving context of DBA.

In this work, we make the following contributions. First, we extend the existing concept of DBA (§1.1) by offering a concrete DBA framework (§6.1) with a well-defined set of characteristics, establishing clear connections to ICT and HCI. By introducing these features, we add significant specificity to the framework and establish clear points of connection for HCI research. Second, we address the race question more directly by centering race and racialization in the digital border discourse, supported by empirical evidence. Third, we offer clear implications (§6.2), as well as actionable points and avenues of inquiry, for HCI towards researching DBAs.

1.1 The Concept of Digital Border Assemblage

Nail [76] summarizes Deleuze & Guattari's concept of *assemblage* as follows: assemblage consists of heterogeneous elements including knowledge, signs, practices, people, institutions, materials, etc. However, they get their particular meaning because of the elements of connection to each other or when they come together. Assemblages are political, and to understand them, we need to understand how they work and the processes that shape them. Assemblages are never total or homogeneous. All assemblages are always undergoing some kind of adaptation or change [76, p.34-35].

Sohn [116] argues that the term *border assemblages* best describes the ontological multidimensionality of borders as suggested by terms like *multiplicity of borders* i.e. borders mean different things to different people, and borders are everywhere. Border assemblages consist of machinic assemblages of bodies performing the material role and collective assemblages of enunciation performing an expressive role. The material role at an actual border is performed by a variety of elements such as physical infrastructure, policing procedures, tools (passports and visas, biometric devices), surveillance technologies with their data, algorithms and machines (scanners and cameras), resources (time, money, energy), networks and the physical or virtual locations at which bordering practices are carried out. The expressive role is performed by legislation defining border regimes, rituals, and symbols (flags) referring to a given territorial identity.

Chouliaraki & Georgiou [22, chp.1] build on Sohn's analysis [116] of machinic and enunciation assemblages in the border assemblages to describe the *Digital Border Assemblages* as consisting of techno-symbolic infrastructures of the territorial border (technologies doing the sorting work) and the platformed narratives of the symbolic border (images, and narratives circulated on social media legitimating some migrations over others) to position migrants on an elastic, adaptable yet persistent boundary of inside/outside stabilizing power relations on ground and in language. The symbolic and territorial have different empirical realities and methods for studying them, but they always exist in mutual reference to one another. Sohn [116] suggests that instead of questioning what a border is, we should trace how various elements of border assemblages connect and disconnect, unfold, and become borders.

2 Related Works in HCI, CSCW, Critical Computing

In this section, we review relevant literature in refugee & migration studies and surveillance & privacy within the fields of HCI, CSCW, and Critical Computing.

2.1 Refugee Studies & Migration in HCI

HCI and adjacent disciplines have been interested in ICTs' role in the migration and movement of people across nation-states. ICTs such as smartphones support migrants, refugees, and asylum seekers to access information, communication with personal and relational networks, access to financial and educational services, and navigation among other things. In this regard, HCI scholars [33, 77, 119] studied smartphones and social media usage practices of asylees before and during migration, their practices for information and decision-making with challenges in the truthfulness of information, surveillance by governments in country of origin resulting in restricted phone use. Other works have focused on the role of ICTs in integrating and resettling refugees, asylum seekers and migrants in host countries [7, 23, 24, 45, 50, 102, 132] assessing both practical and emotional aspects of migrants relationship with and through the devices to their social circle at home and host countries as they stay connected to families and start new lives by accessing government services through phones. Since the focus of these works is on the use of phones for seeking information via social media or personal networks before, during, and after migration they briefly hint at the threats to participants' safety. However, these concerns are geared towards threats to safety due to identity theft, viruses, or financial loss [102], or perceptions of threat to safety due to (unspecified) external attacks [24]. Only participants from authoritarian regimes showed awareness about the potential use of phones for surveillance by home country governments. For example, Dekker et al. [33] discuss the fear of government surveillance among Syrian refugees during migration due to the use of phones. However, they do not go beyond a brief mention of the protective strategies and limited understanding of how this surveillance might take place via ICTs. Overall, this body of work focused on using ICTs to integrate incoming refugees, the challenges faced, and the design opportunities identified. Moreover, there is a focus on the

adoption and use of ICTs and related services by what appears to be the migrants' own willingness. We add to the discussion of ICTs in migration by highlighting technologies that might be imposed on these groups by the state, sometimes without their knowledge, and the surveillance of migrant groups by host governments via ICTs. We add to migration literature in HCI by shifting the focus from the use of ICTs, either for everyday use or specifically designed, for migration, integration, and resettlement of migrant communities to their use for surveillance, mobility, and social hierarchical control of migrants and racialized minorities by nation-states, particularly the US. We add to the discussion on HCI and migration the concept of digital borders which emphasizes the existence of borders as a site beyond physical spaces to digital spaces.

Previous works highlighted the use of technologies such as biometrics for profiling migrant groups [9], the focus has now shifted to the use of ICTs for surveillance [63] and profiling which we expand upon through our case studies. Existing works discuss migrants' dependence on personal social networks for information due to information precarity and misinformation during migration indicating relationality in information seeking. Through a focus on the use of ICTs in bordering and surveillance, we show that the use of ICTs in DBA targets relationships and communities of racial subjects threatening relational networks of migrant groups.

2.2 Privacy and Surveillance

Within HCI and security, the intersection of privacy and migration is gaining interest [1], yet research in this area remains limited [11, 42, 114, 119]. Existing studies have explored smartphone privacy perceptions among migrants at different stages of their migration journey. Simko et al. [114] examined the privacy practices of refugees resettled in the US, finding a greater reliance on technology than expected, which heightened the importance of computer security. While Simko et al. focused on post-resettlement privacy practices, Steinbrink et al. [119] investigated asylum seekers' perceptions of privacy during migration, identifying key challenges, consequences, and adaptation strategies.

Although these works adopt a temporal perspective on migration, we expand the scope by incorporating the concept of bordering sites from critical studies. We demonstrate how ICTs not only extend these sites but also reshape the contexts in which privacy becomes a critical concern. Furthermore, while prior research has primarily examined privacy at the individual level, our case studies highlight the need for a relational perspective — one that accounts for governments' surveillance of racialized migrant groups.

These studies also explored migrants' understanding of government surveillance. Steinbrink et al. [119] found that participants who had fled government persecution developed more sophisticated mental models of privacy. However, all participants recognized privacy risks posed by both state and non-state actors, as well as the potential consequences for their safety and asylum status. To mitigate these risks, migrants employed various strategies, including maintaining anonymity, modifying phone usage and communication patterns, and in some cases, forgoing phones altogether.

Design recommendations emerging from this work include anonymity-on-demand features in communication apps, browser-enabled communication with easy history erasure, and lockdown modes to conceal sensitive information in the event of phone seizures. Guberek et al. [42] further examined privacy practices among undocumented workers in the US, revealing a gap between their offline safety precautions and their online behaviors. Their study also found that many migrants lacked understanding of state surveillance mechanisms, leaving them more vulnerable to digital risks.

Technology can also have negative consequences for refugees. Aarunasalam et al. [11] examined how toxic content and online harassment influence the privacy practices of refugees, who often rely on social media for resettlement. To shield themselves from online abuse, they adopt strategies such as selective blocking and removing landmarks from photos. While these privacy measures —such as omitting personally identifiable information — help protect refugees, they can also hinder family reunification. Similarly, Forti [35] argued that although smartphones facilitate resettlement, they also function as surveillance tools. European governments, for instance, have shown interest in using digital traces — such as social media profiles and location data —for identity verification and security checks, turning smartphones into control mechanisms.

Building on Forti's concerns, we expand the notion of surveillance in migration — examining who conducts it, when, where, why, and on whom. Using critical border studies, we highlight racialized surveillance as a fundamental aspect of border management. We argue that HCI researchers should adopt a racial perspective on privacy, not only in technologies explicitly designed for border control but also in everyday digital tools integrated into the Digital Border Assemblages (DBA). While existing HCI literature has largely focused on migrant and asylum seeker privacy, using critical border and race studies we draw attention to the surveillance of racial others in migration and travel including both citizens and noncitizens, not just at physical ports of entry but also within the state and across digital spaces and technologies of everyday use.

Race is a central theme in critical border studies. Race underpins the logic of mobility management across borders and associated government surveillance as discussed in section 4, therefore, we review the discussion on Race and Privacy within HCI. The notion of surveillance as racialized was introduced by Simone Browne. In her book Dark Matters: The Surveillance of Blackness [18], she argued that the assessment of surveillance is incomplete without a view of race. Although terms like the *surveillance society* might indicate a total homogenized existence of surveillance, they overlook the nuanced, *discreet and varying ways in which surveillance operates*. Surveillance was not something created by the creation of technologies. It has always been a fact of black life. Browne defines **racialized surveillance** as enactments that *...reify boundaries along racial lines, thereby reifying race, and where the outcome of this is often discriminatory and violent treatment of those who are negatively racialized by such surveillance.*

Racialized surveillance is a technology of social control where surveillance practices, policies, and performances concern the production of norms about race and exercise a *power to define what is in or out of place* [18, p.16]. However, a review of privacy and security literature by Sannon and Forte [104] with a focus on marginalized populations to ascertain gaps in the field shows that privacy research in HCI on marginalization focuses on individuals and identities; physical spaces and communities; online spaces, tools, and

communities; or marginalization, in general. Although 82% of the papers focused on marginalization based on individual identities such as LGBTQ, victims of sexual assault, and disability, only a few focused on race, ethnicity, or immigration status as a source of marginalization. Sannon and Forte [104] concluded that the discussion on privacy and race is lacking in HCI. Even when race is an inextricable factor in marginalization, it does not take center.

However, legal studies have discussed the link between race and privacy. Matt Reichel [97] argues that privacy as a right is distributed unevenly across racial and class lines. They argue that the privacy architecture that users interact with is not neutral but reflects societal prejudices and power asymmetries which requires more than a legalistic approach. Using the example of better encryption of expensive smartphone devices, they argue that wealth and class divide determine how privacy is distributed across groups. We add to the discussion of racial distribution of privacy and extend it to the field of HCI. Through case studies (4.2) and extension of the DBA framework (6), we demonstrate practical examples of the racial distribution of privacy.

Reichel [97] differentiates between a conventional and critical approach to privacy [36] where the conventional approach does not consider the sociological divisions determining privacy invasions. It is worth noting that Sannon & Forte's [104] review showed that only six HCI papers and none of the privacy papers applied a critical lens. Our work addresses this gap by taking a critical-interpretevist approach to study and extend the DBA framework by introducing the use of ICTs in bordering and surveillance as a new avenue of HCI research.

Racialized groups disproportionately face privacy risks. Razaq et al. [96] referred to these risks as digital manifestations of border imperialism. Similarly, Owens et al. [87] examined the surveillance of families of incarcerated individuals, noting how these practices disproportionately impact Black communities but without centering race in their analysis. We extend this discussion by advocating a relational view of privacy, focusing on the networks and communities targeted by racialized surveillance.

Research has also explored the chilling effects of government surveillance on behavior. Penney [89] found that awareness of surveillance deters legal activities due to fear of unfavorable legal consequences. Stoycheff et al. [120] reported similar deterrents among Muslims in the U.S., including reduced political participation and disclosure of religious identities. We build on these findings to emphasize how racialized surveillance extends beyond borders, affecting both citizens and non-citizens within digital and physical spaces.

3 Methods

Using a critical-interpretivist approach to answer the overarching research question: *How can HCI designers and researchers begin to understand the role ICTs play in the ongoing racialization of migrant bodies caused by border assemblages?* In that, we review relevant scholarship around border studies, critical race studies, and surveillance studies to generate a comprehensive understanding of what constitutes borders and racialization of migrant bodies at/by the border, and ultimately how these themes shape the framework of digital border assemblages (DBA). This review of critical scholarship works as a lens through which we analyze three case studies to identify the role of ICTs in enabling and extending DBA. In this section, we explain the three parts of our work: a review of critical theory to ground our analysis; empirical evidence in the form of case studies; and our interpretive work toward identifying the role of ICTs in evolving the DBAs framework.

3.1 Review of Relevant Literature in Critical Theory

We take inspiration from Orlikowski and Baroudi's [86] description of critical research philosophy to guide our work. Critical research is concerned with critiquing existing social systems. It maintains that social reality is constituted historically. Systems or things exist in relation to the totality of which they are a part and not in isolation. It aims to highlight the systems of domination and how it limits humans from reaching their potential. Mark & Klien [72] suggest that critical research data collection and analysis be grounded in core concepts and ideas from critical theorists. Therefore, as the first part of our work, we ground our work in the history of border technologies and artifacts and their entanglement with race through a review of the critical border studies literature and the history of race in bordering. We conducted a review to analyze literature in critical border studies [48, 88, 99, 126, 127], bordering technology [22, 63, 125], datafication by state [108, 115], surveillance and racialized surveillance [18, 43, 59], critical race studies [52, 95] to understand key concepts in border studies and migration, the role of race and racialization in bordering, role of surveillance technologies in border imperialism.

3.2 Case Studies, Data Sources, and Data Analysis

Our empirical evidence consists of three case studies demonstrating the use of ICTs in bordering regimens. These case studies have been selected where ICTs are used in controlling the movement of individuals or money, making decisions about entry into the country is dependent on their usage patterns, contingent on the inspection of ICTs at the border or use of ICTs for monitoring as a condition for release. They represent the experiences of US citizens, asylum seekers, migrants, and communities of color with ICTs either specifically designed for movement control, surveillance, and bordering or implicated into the larger border assemblage. The sites of case studies vary from physical border crossings into the US, to bodies of the migrants, devices of US citizens, migrants and asylum seekers, and the movement of money. The types of data sources used for the case studies are summarized in Table 1.

Documents analyzed for **Case Study 1** include the CBP Directive on Border Search of Electronic Devices [93], Privacy Impact Assessment Report of border search of electronic devices [79], CBP statistics on annual number of device inspections (upto FY 2017) [94], reports from legal advocacy group Muslim Advocates on US citizens of South Asians, Arabs and Middle Eastern origin, of varying age, gender, ethnicity, mostly Muslims, being targeted disproportionately with border device inspections and documenting their experiences [4], news articles [105, 122] and books [69, chp.8] reporting similar experiences, audit reports on the CBP's

Case Study	Data Sources
Electronic Device Inspection	CBP Directive and statistics, Privacy Impact Assessment Report, DHS audit report, legal advocacy group reports, news articles, legal commentary and scholarly articles, forensic testing reports
Location Surveillance and Ankle Monitors	Program overview by ICE and American Bar Association, statistics from ICE and TRAC, investigative journalism and news articles, legal advocacy reports, FOIA data, peer reviewed publications in law
Anti-Terrorism Laws and Financial Technologies	Critical studies literature, Peer reviewed publications in HCI and law, legal advocacy group reports, news articles, public office correspondence

Table 1: Case Studies and corresponding data sources

management of searches of electronic devices at ports of entry by DHS Office of Inspector General [82], scholarship and commentary by legal experts on fourth amendment rights and privacy intrusions resulting from border inspections of electronic devices [39, 74], reports providing travelers with guidelines for protecting their data at the US border [107] and forensic tool testing reports for forensic investigation softwares by the Computer Forensics Tool Testing (CFTT) program [1] [81].

The data sources analyzed for **Case Study 2** include an overview of ATD program by ICE [47] and American Bar Association [84], news articles [37, 113, 123] reporting impact of ATD on immigrant individuals, families and communities, ATD statistics from ICE [46] and TRAC [121], investigative journalism article [16] and legal advocacy group Mijente's reports on the collection and retention of data by ICE based on analysis of documents obtained through FOIA lawsuits [67], report on experiences of individuals enrolled in the ATD program [66] and recommendations and legal scholarship on ankle monitors as digital cages [111].

The sources referred to for **Case Study 3** include peer-reviewed publications in the fields of law [13, 117] and HCI [100], critical scholarship [52, 95, 126], US Senator's letter [83], legal advocacy group report [34] and news articles discussing racial profiling [64, 112] and government mass surveillance [6] of financial transactions.

[1]The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology (NIST) Special Programs Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense's Cyber Crime Center, the U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, as well as the DHS Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications. Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT website (http://www.cftt.nist.gov/).

It is worth highlighting that the method for studying-up opaque government systems part of the border assemblages. Nader [73] suggests that researchers study up the organizations, institutions, and governments that affect the society at large and not just focus on the peoples, tribes, societies, and communities. *Studying-up* refers to understanding the processes through which power is exercised by studying the upper and middle ends of the social power structure. Access is challenging in studying up as elite institutions may not allow researchers to observe them. Researchers can use eclectic methods such as studying public-facing documents, memoirs, interviews, etc [73]. Border studies scholars, legal advocates, and migrant justice groups have adopted Freedom of Information Requests (FOIAs) to glean into the inner workings of organizations, their tools, practices, systems, policies, statistics of border management, and control. Reports issued by legal advocacy and migrant justice groups uncover border assemblages through Freedom of Information Act (FOIA) requests [12, 67]. These include requesting and analyzing training documents, procurement requests detailing system requirements and features for border surveillance and management technologies, statistics on operations, internal policies, etc. Another data source is reports containing the experiences of people targeted through these practices and technologies. We, therefore, selected our case studies based on the level of details available and coverage of each case in literature, popular media, and advocacy reports.

3.3 Extending the Digital Border Assemblages Framework

For the last part of our work, while adopting the critical-interpretivist approach, we applied a critical analytical lens to the empirical evidence we collected in our case studies. The empirical evidence demonstrated the current use of ICTs in/for bordering. We followed that with a critical interpretation of the empirical evidence by connecting it to the broader critical theoretical frameworks reviewed in our literature review on critical border and race studies [92]. Identifying such systems aims to initiate social change or transformation at an individual, societal, and theoretical level [72]. While the interpretive approach seeks to study the social world, the critical

approach aims to understand and critique systems of domination that shape and constrain the social world of the participants. We aim to create consciousness around restrictive conditions of status-co to initiate change in social relations and practices to eliminate the bases of domination [86]. The result of this work is the extended DBA Framework that we present in section 6. In this section, we extend the DBA framework suggested by Chouliaraki and Georgiou [22] to locate both the evolution enabled and novelty achieved by the function of ICTs in border assemblage.

4 Conceptual Foundation: Understanding Racialization at/by the Border

This section provides an overview of the conceptual foundations of borders from critical border studies (§4.1) and discusses the role of race in the history of border control formation and the development of border technologies (§4.2).

4.1 Understanding Borders

Borders are traditionally perceived as fixed cartographic lines inscribed in geography to regulate migration and movement, symbolizing state sovereignty, security, and citizenship [99]. However, scholars in critical border studies challenge this notion, advocating for a more fluid and networked understanding of borders, one that is diffused, vacillating, and dislocated. They conceptualize borders as productive regimes that both emerge from and reinforce racialized social relations, further shaped by gender, sexuality, class, ability, and nationality [127, p.78].

Beyond physical demarcations, scholars have examined borders as techniques of control that privilege nation-states. They argue for a more capacious understanding beyond the physical borders to include technological spaces, politics, discourses, and so on. Johnson et al. [48] invite scholars to rethink borders in terms of place (of enactment or materialization), performance (of border work), perspective (of those performing border work), and politics of border work. Rumford introduced the concept of borderwork to refer to *envisioning, constructing, maintaining and erasing borders*[101] and argues that borders have generalized in society as a whole and border work is being performed not only by the state but also by ordinary citizens and organizations through 'rebordering' and 'debordering'. Critical Border Studies scholars Parker and Williams et al. [88] state that *border lines are not only found at territorially identifiable sites such as ports, airports, and other traditional 'border crossings'*. Instead, they are increasingly ephemeral and/or impalpable: electronic, invisible, and located in zones that defy straightforwardly territorial logic. Borders should be thought of in terms of epistemology, spatial-temporality, and ontology, networked, dislocated, and as experiences. The epistemology of border thinking requires theorizing borders as experiences of what it means to exist as a migrant [88].

Walia [126] extends this critique with the concept of border imperialism, emphasizing that borders are artificial and deeply political tools of colonization and othering. Border imperialism refers to the structural production and maintenance of displacement and migration-related violence and precarity [127, p.2]. It operates through four key strategies: exclusion, territorial diffusion, commodified inclusion, and discursive control [127, p.77-92]. In particular, territorial diffusion allows borders to be externalized beyond national territories or internalized within them. Internalization means that a border's function persists beyond the point of physical crossing and it can be enforced anywhere within the nation-state [127, p.84]. Meanwhile, exclusion manifests through walls, detention centers, and deportation regimes, actively containing and expelling migrants.

Foucault introduced the concept of Governmentality, or the 'conduct of conduct,' which has influenced various domains, including migration. Governmentality describes how governments guide individuals toward certain behaviors. Foucault framed government not only as state management but also as a matter of self-regulation [53]. It operates through both disciplinary power and control mechanisms. While disciplinary power enforces direct consequences, control mechanisms subtly steer people toward desirable behaviors while discouraging undesirable ones [53].

Walter [129, p.5] encourages migration researchers to apply mid-range concepts, such as antipolicy (e.g., anti-trafficking, anti-terrorism, anti-poverty), to link Foucault's ideas on Governmentality with migration governance. Antipolicies, often led by state or civil society organizations, seek to combat perceived threats by polarizing public discourse and urging people to take sides [109]. By racializing Muslims as terrorists and Latinos as criminals, these antipolicies enforce migration control through both overt disciplinary power and covert governmentality. We argue that many state policies and practices around migration and bordering cultivate **internalized self-governmentality** —the regulation of one's behavior to align with state expectations—among racialized migrants, immigrants, and citizens, as explored in case studies §4.2 and §6.1.

By examining how border studies scholars problematize the concept of borders as dynamic sites of enactment - where border work both enforces and resists migration control through internalization and externalization - we can adopt a more expansive perspective. This enables a deeper exploration of ICT-enabled bordering practices, whether through surveillance (§6.1.5) or self-enactment (§6.1.8), and their implications for Human-Computer Interaction (HCI) (§6.2).

4.2 Understanding Racial Formations at/by the border

In this section, we examine the intersection of *bordering technologies* and *racialized mobility management*. We argue that these technologies are deeply entangled with social control along racial lines. Legal scholar Achiume [2] analyzes race and racial justice within the liberal democratic legal discourse and international borders, asserting that *borders are inherently racialized*. They privilege *whiteness* in migration and mobility, reinforcing racial disparities under the guise of neutrality. Achiume conceptualizes race as a *border infrastructure* — a structuring force that dictates the enforcement of territorial and political boundaries.

Historically and in the present, U.S. border policies, technologies, and practices have racialized and controlled groups such as *Black [18], Arab, Muslim [8, 75], and Latinx [32, 56] communities*. As we demonstrate in our case studies §4.2, the *narrative tropes, operational mechanisms, and artifacts* involved in racial othering differ, yet the

outcome remains the same: the regulation of mobility and the assertion of social control. From their inception, border technologies have been designed to control the movement of racialized populations—both across national boundaries and within urban spaces. Winner [130] argues that understanding the politics of technological artifacts requires analyzing their broader socio-political contexts. Following this framework, it is crucial to examine the historical foundations of bordering technologies and the underlying logics that sustain modern bordering regimes. Contemporary border and immigration controls are rooted in *anti-Black violence, imperial expansion, and Indigenous elimination* [127]. The history of border enforcement is inextricably tied to the racialized surveillance and policing of the Black movement.

Borders are argued to be a site of exception. Both Jason de Leon [32, p.27] and Puar [95] build on *Agamben's state of exception—the process whereby sovereign authorities declare emergencies to suspend the legal protections afforded to individuals while simultaneously unleashing the power of the state upon them* [5]—to explain the exceptional treatment of and violence against Latinos [32, 56] and Muslims [8, 75] at borders. In the context of ICTs, such an exception curtails privacy rights at borders. In section 6, we argue that this privacy exception, combined with a racialized exercise of policies at borders, leads to *racialized surveillance and invasion of privacy.*

Anti-Black logics, originally designed to regulate and punish Black mobility, remain central to modern border controls, which use surveillant assemblages[2] [43] to classify, monitor, and contain *undesirable* populations. As hierarchical mechanisms of social control, borders enforce the subjugation of racialized immigrant bodies—dictating who belongs and under what conditions.

Browne [18], in *Dark Matters: On the Surveillance of Blackness*, traces the genealogy of border surveillance to historical techniques of *Black movement control.* The Book of Negroes, a register of freed slaves used during the transatlantic slave trade, functioned as one of the earliest government-issued migration documents—explicitly linking *corporeal markers to state-regulated mobility.* Similarly, branding enslaved people's bodies served as an early form of *biometric identification*, ensuring they remained visible and controllable within the system of racial capitalism.

The *Lantern Laws* provide another historical example of racialized mobility control. These laws required enslaved individuals to carry *supervisory devices* (lanterns) when moving at night, making them permanently *illuminated, locatable, and surveilled* [18, p.78]. Such measures framed Black, Indigenous, and mixed-race people as *security threats* requiring continuous monitoring. As Browne notes, these laws established a *panoptic framework* - a form of racialized surveillance that produced knowledge about Black bodies, regulating their presence within urban spaces [18, p.79].

In his book, *The Land of Open Graves*, Jason de Leon [32] shares the experiences of migrants crossing the Sonoran desert at the U.S.-Mexico border. He contrasts the technology used by the nation-state to surveil migrants with the artifacts and tools migrants use to *subvert and resist* that surveillance, highlighting the massive technological disparity. He argues that despite billions spent on surveillance, border technologies are *ineffective in stopping migration.* Instead, they heighten the dangers faced by migrants who remain highly motivated to seek better lives and reunite with their families.

Narratives are central in not only shaping national identity and constructing racialized *others* [10] but also creating justification for the use of technology in bordering. First, border discourse criminalizes migration, casting migrants as *illegals, terrorists, and criminals* [127, p.78]. This framing justifies detention, deportation, and incarceration while *dehumanizing migrants as threats to be deterred, managed, and contained.* Second, technology is positioned as a solution to problems of *criminality, terrorism, and illegality,* reinforcing state security logic. By emphasizing values such as *national security, futurity, and innovation*, governments invest in border surveillance technologies, extending carceral and policing infrastructures to racialized populations both within and beyond state borders.

Several scholars, including Iván Chaar López, Jason de Leon, and Melissa Villa-Nicholas, have examined the racialized logic embedded in border technologies along the U.S.-Mexico border.

In *Cybernetic Borders*, López [56] argues that mobility management has already been transformed into an informational problem, governed by drones, sensors, and cameras. The cybernetic border framework integrates data-driven technologies to enforce national boundaries, yet race remains the primary criterion for categorizing, surveilling, and managing bodies. These surveillance systems encode racial biases, using algorithms to determine inclusion or exclusion based on racialized assumptions. By framing migrants from Latin America and the Muslim world as security threats, cybernetic borders justify violence against marginalized communities and entrench racialized exclusion.

Villa-Nicholas [125] extends this argument, showing how information technologies expand the U.S.-Mexico border beyond its geographic limits. Through data integration from government and private sources, surveillance infrastructures create a nationwide digital border. Silicon Valley firms collaborate with the U.S. government, making data a key form of capital in border enforcement.

The U.S.-Mexico border has become a testing ground for surveillance technologies, including predictive analytics, facial recognition, biometrics, sensor networks, and automated decision-making systems [9, 62, 71, 118]. Migrants serve both as test subjects and data sources, further entrenching the racialized logic of digital border enforcement.

Building on these historical precedents, we examine how *ICTs integrate into contemporary bordering regimes.* Through case studies on *electronic location monitoring, device inspections, and financial technology* §4.2, we explore how digital border assemblages (DBAs) extend these surveillance practices. By embedding racialized logic into *data-driven technologies*, ICTs make racialized subjects hypervisible, reinforcing state control over their mobility.

5 Case Studies

This section presents three case studies from the United States that illustrate different dimensions of digital border assemblages. Each case study examines specific tactics employed within these assemblages, highlighting how information and communication technologies (ICTs) enhance their operation. These tactics are later

[2]Surveillant assemblages consist of people, corporations, government contractors, states, agencies and are used by governments - both democratic and authoritarian - to surveil their citizens extensively [58] to maintain social order, prevent terrorism, and distribute welfare.

analyzed in relation to the conceptual foundations outlined in Section 4 to identify key characteristics of digital border assemblages, as articulated in Section 6.1.

5.1 Case Study 1: Electronic Device Inspections at Borders

The U.S. Customs and Border Protection (CBP) is responsible for enforcing immigration laws at and near the borders of the United States. The agency has the authority to inspect all merchandise and individuals crossing the U.S. border, whether inbound or outbound, to uphold immigration, customs, and other federal statutes. According to CBP, these searches help *detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography, as well as reveal information about financial and commercial crimes* and assess the intentions behind an individual's visit [93].

As part of these inspections, electronic devices are examined[3]. Notably, *neither a warrant nor reasonable suspicion* is required, meaning any international traveler entering the U.S. can be subjected to such searches. Statistics indicate that electronic device searches increased significantly from 19,020 in FY 2016 to 30,200 in FY 2017, marking a 58% rise, along with a subsequent increase in privacy complaints regarding these searches [105].

Device inspection as forced data extraction and disclosure: As per CBP directive, border searches of electronic devices *will include an examination of only the information that is resident upon the device and accessible through the device's operating system or other software, tools, or applications.* Officers are prohibited from intentionally using the device to access information exclusively stored remotely. To prevent unintentional access to cloud-stored data, officers must ensure that the device is disconnected from the internet and avoid taking any actions that could alter its contents.

There are two types of inspections of electronic devices, categorized by the method of search and whether suspicion is required for an officer to search: *basic or manual search* and *advanced or forensic search* [93].

A **basic search** involves a manual search of the device by an officer in front of the passenger with or without suspicion. A Privacy Impact Assessment (PIA) report suggests that such a search *may reveal information resident upon the device and would ordinarily be visible by scrolling through the phone manually (including contact lists, call logs, calendar entries, text messages, pictures, videos, and audio files).* Unlike advanced search, it does not include connecting the devices to external equipment for review. Officers searching are required to document the interaction, including a record of any electronic devices that were searched [79].

Forensic or advanced search refers to the process in which a border patrol officer connects a device to external equipment *through wired or wireless means, not simply to access the device, but to meticulously review, copy, and/or analyze its contents* in cases where there is *reasonable suspicion or a national security concern.* Factors that may establish reasonable suspicion include *the presence of a relevant national security-related lookout, in conjunction with other articulable factors, or the identification of an individual on a government-operated and vetted terrorist watch list.* Test reports for forensic software tools utilized for these inspections [81] indicate that forensic device inspections can extract various types of data, such as contact lists, messages, call logs, text, and multimedia messages, as well as data files, including audio, images, videos, and even deleted files corresponding to all of the aforementioned. Additionally, internet activity data, encompassing visited websites, bookmarks, emails, location data like GPS coordinates and geo-tagged information, and social media data can also be retrieved. Although the specifics of social media data are not disclosed, anecdotal evidence from travelers suggests that border agents may manually scrutinize the social media profiles of passengers, including posts and lists of friends.

Despite the prohibition on officers connecting devices to the internet during searches and accessing cloud data, an audit report evaluating the management of electronic device searches at Ports of Entry reveals several violations of policy. Specifically, the report highlights instances where officers failed to: i) disconnect the device from the internet during searches, and ii) promptly remove the data from the thumb drive before connecting it to the Automated Targeting System (ATS)[4] for analysis [82]. This failure to delete data copied from travelers poses a risk of unintended disclosures in the event of theft [17].

Obscurity: While searches must generally be conducted in the presence of the individual whose information is being examined, exceptions apply. Border patrol officers are instructed to prevent the individual from observing the search, particularly if it might disclose law enforcement techniques or compromise operational considerations [93]. Legal reports concerning border inspections of electronic devices often highlight violations of Fourth Amendment rights[5] experienced by U.S. citizens and permanent residents. These reports stem from grievances filed by affected travelers for infringing upon their rights, predominantly representing U.S. citizens, who may face delays but are not outright barred from entry. In contrast, non-citizen travelers may be denied entry to the U.S. and risk deportation for non-compliance. Unfortunately, the experiences of non-citizen travelers often go unreported and remain largely invisible to the legal system. Furthermore, statistics on electronic device inspections at the border do not indicate the ethnicity, national origin, gender, race, religion, or immigration status of travelers selected for searches, rendering the process opaque [12, 106].

Discriminatory practices and creating state legibility: The PIA report on the border search of electronic devices [79] highlights significant legal concerns surrounding the inspection of digital devices. Although border patrol is authorized to inspect merchandise at borders, the inspection of electronic devices stands apart from traditional searches of physical goods. This distinction arises from the vast amounts of personal data stored on digital devices.

[3]As per the Directive on Electronic Device Inspections [93], an electronic device is defined as any device that may contain information in an electronic or digital form, including computers, tablets, disks, drives, tapes, mobile phones, communication devices, cameras, and music and media players.

[4]The Automated Targeting System (ATS), a decision support tool that assesses traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data through risk-based scenarios and assessments. [80]

[5]The Fourth Amendment to the U.S. Constitution guarantees individuals the "right . . . to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government.

Legal scholars contend that digital searches pose a heightened threat to individual privacy. According to their analysis, *the particular mechanics of digital searches and the frequency with which personal information is stored on electronic devices makes the discovery of private information highly likely* [74, p.152]. Moreover, searches of cell phones and computers reveal not just current files but also browsing histories and deleted files. Many users are often unaware of the extent of data retained in their devices' memory, making it difficult to prevent the unintended disclosure of sensitive information. Moreover, potential access to cloud-stored data further complicates matters, as it allows the government to obtain information that was never physically transported across the border [74].

Racial profiling: While statistics indicate that fewer than 1% of travelers are subjected to device searches [94], legal advocacy groups report that Muslim travelers are disproportionately targeted. Multiple civil rights organizations have documented cases of religion- and ethnicity-based profiling, raising constitutional concerns [31, 110].

Targeting Communities and Belonging: Travelers subjected to device searches have reported interrogations about their religious practices, political views, charitable donations, and community ties, particularly targeting Muslim Americans [31, 110]. The advocacy group Muslim Advocates highlights these concerns in its report *Unreasonable Intrusions: Investigating the Politics, Faith & Finances of Americans Returning Home* [4]:

> Law-abiding Muslim, Arab, and South Asian Americans returning home after overseas travel have experienced widespread, systematic, and profound privacy intrusions by federal agents at the nation's borders and airports. CBP agents have questioned individuals about their political beliefs, religious practices, and the charities they support. Agents have also sought to review and copy business cards, credit cards, and data on laptops, digital cameras, and cell phones. The interrogations and searches are taking place without evidence or even suspicion that the travelers have engaged in wrongdoing, and investigated various First Amendment-protected activities, including religious beliefs and political speech, as a pre-condition for allowing them to re-enter their own country and return home.

Enacting borders through self-governmentality: Travelers have reported altering their behavior in response to these searches. Some avoid carrying politically sensitive books or electronic devices with personal communications (e.g. correspondence of religious leaders with community members), fearing that electronic device inspections may expose confidential information. Legal scholars warn that border searches of digital devices can *reveal intimate details about how individuals think, research, and engage with their communities in ways that paper documents cannot* [4]. This has significant implications for free speech, privacy, and the unrestricted exchange of ideas —fundamental democratic values that such searches may inadvertently suppress.

5.2 Case Study 2: Location Surveillance and Ankle Monitors as *Digital Cages*

The criminalization of migration is starkly illustrated through policing practices like electronic location monitoring under the Alternatives to Detention (ATD) program implemented by Immigration and Customs Enforcement (ICE). This agency is tasked with enforcing U.S. immigration laws both within the country and at its borders, alongside conducting detention and removal operations. According to the American Bar Association, the United States has expansive authority to detain various migrants and asylum seekers while they navigate legal proceedings. Although these detentions are classified as *civil*, individuals are often housed in criminal detention centers, a practice widely regarded as inhumane [84].

In response to these conditions, ICE established the ATD program, which facilitates the conditional release of non-citizens who are not detained. This initiative represents the largest electronic monitoring program among U.S. law enforcement agencies [65]. As stated by ICE, the ATD programs are designed to ensure adherence to release conditions and to provide essential case management services for non-detained non-citizens. The program includes the Intensive Supervision Appearance Program (ISAP), which employs a combination of case management and technological tools to promote compliance with release conditions while individuals remain on ICE's non-detained docket [47].

ISAP incorporates various monitoring technologies, including ankle monitors, the SMARTLink app, and telephonic check-ins. Participants may be subjected to a blend of these surveillance methods. A brief overview of each technology is provided below:

GPS monitoring mandates that participants wear an ankle monitor for 24/7 location tracking. Since 2023, both ICE and BI have introduced wristwatches into the program as an additional option. Participants must keep their monitors charged to avoid alerts about low battery levels and notifications about leaving designated zones, typically conveyed through beeps and announcements. However, the technology can be glitchy, causing frustration and added stress. Lawyers and asylum seekers have reported instances in which participants have experienced shocks, burns from overheating, or medical issues due to the tight fit of ankle monitors. The *SMARTLink App* is either installed on participants' smartphones or on a device loaned by the government. It requires users to take selfies or call their ISAP case manager when prompted by the app. Many participants report difficulty complying with these prompts due to app glitches or poor connectivity. The fear of incarceration for failing to respond heightens the stress and disrupts their daily lives. In addition, *Telephonic Check-ins* require participants to call their ISAP case managers. ISAP uses voice forensics to verify the identity of callers, imposing further pressure on participants.

State Legibility, Expanding Borders, and Targeting Relationships & Communities: Electronic monitoring through alternatives to detention (ATD) contributes to the expansion of detention both spatially and temporally. Journalists, legal experts, and migrant justice organizations have documented a disturbing increase in the detention rates of migrants, alongside a rise in the number of individuals subjected to electronic surveillance, despite the intended purpose of ATD [37]. Rather than serving as a viable alternative to detention,

these electronic monitoring tools effectively become *de facto detention*, infringing on all aspects of individuals' lives, including their ability to shop for groceries, participate in recreational activities, fulfill family obligations, and secure stable employment or housing [123].

The imposition of ankle monitors often requires at least one parent in the migrant family to wear the device. Although typically associated with individuals on parole for criminal offenses, the use of ankle monitors on migrants suggests a presumption of criminality in the public's perception. This stigma can lead to social ostracism, mental distress, and isolation for the monitored individuals and their children [124]. Participants have reported losing their jobs due to the monitors alarming unexpectedly during work hours [84, 123].

In terms of duration, electronic monitoring frequently extends beyond the period of formal detention [46, 84]. While there was previously a trend of increased monitoring through the SMARTLink app, the situation has recently shifted, showing a decline in its usage compared to ankle monitors [121].

Spatially and relationally, electronic location surveillance is highly intrusive to privacy. It monitors frequent locations, time spent at each location, and movement patterns of individuals. It is used to surveil entire communities. Migrants often rely on their diaspora to access employment opportunities and housing. However, ICE's use of location data from electronic location monitoring to conduct raids and detain, monitor, or deport more migrant workers puts entire communities at risk [113], therefore, isolating the migrants.

Obscurity: An investigative journalism report on BI, a subsidiary of Geo Inc., which manages the electronic monitoring of immigrants using ankle monitors, tracking apps, and case management services, indicates that inadequate technology and overworked BI personnel negatively impact participants in the ISAP program [16, 67]. The report raises significant concerns regarding the lack of transparency surrounding intensive data collection on migrants' lives and movements over extended periods through the ISAP program. Access to this data is not restricted solely to ICE; numerous organizations and employees can view it. Moreover, the duration for which critical private data are stored on migrants continues even after they exit the program, raising concerns about the potential for a nonprofit organization to sell these data to data brokers [ibid.]. In particular, BI also supplied incarceration data to ICE through contracts with data brokers in sanctuary states, data that would otherwise be unavailable to ICE.

Data Extraction: Another report examines data acquired through FOIA requests to assess the extent of data collected on migrants and their applications [67]. This report concluded that the ISAP program is collecting extensive amounts of information[6] regarding migrants, their families and their communities. Moreover, the actual data collection and retention practices contradict the information provided in FOIA documents. Sensitive data on migrants and their relationships are collected and stored for up to 75 years. Legal scholars and migrant justice organizations argue that ankle monitors function as *digital cages, a "violence of invisibility"* that must be eliminated [111].

[6]As reported by Mijente, Just Futures Law, and Community Justice Exchange Fact Sheet [67], the following types of data are collected through ankle shackles and the SMARTLink app: Personally Identifying Information (address, email address, phone number, birth date, social security number, visa, passport number, employment information, education information, financial information, religious affiliation, race, gender, etc.); Biometric and body/health data (facial images, voice prints, weight, height, tattoos, scars, medical information, disabilities, pregnancy and births, etc.); Geolocation data; Phone numbers of close contacts; Immigration court records; Vehicle and driver data (e.g., license plate number, driver's license number, vehicle registration number); Community surveillance data (e.g., information about someone's home, neighborhood or community ties)

5.3 Case Study 3: Anti-Terrorism Laws and Financial Technologies

According to legal scholar Reem Bahdi [13], *the War against Terrorism takes the form of a vast and complex array of laws, regulations, policies, and practices that cut across contexts like the criminal law, tax law, financial regulations, employment, intelligence services, and airport security.* Digital payments are another area where racial profiling has become prominent since 9/11. Social payment software, like Venmo or Paypal, is a unique information system that merges the often separated worlds of personal finance and online communities [3, 21]. The underlying financial technology of international or domestic remittance systems controls the flow of funds across borders and is another site for the manifestation of border imperialism.

Discriminatory practices: Regulations such as *anti-terrorism financing* used to control the flow of funds to countries, entities, and individuals [100] adversely affect individuals, social groups, and communities [117]. Rohanifar [100] studied the effects of harsh regulatory requirements on financial institutions in Bangladesh due to the increased compliance burden resulting from the association of terrorism financing with Muslim countries, as well as the amplified consequences of minor incidents, such as the closure of entire banks for inspection after one *suspicious* transaction. Kumar argues that racism against Muslims in the US has been legitimized through the charge of *material support for terrorism*, which criminalizes a wide array of financial transactions, including donations to charitable organizations and antiwar protests [52, p.148]. Following the post-9/11 shutdown of almost all Muslim charitable organizations in the US and the freezing of their assets *to allegedly prevent the flow of money to terrorists*, the US government equated the Islamic charitable giving of Zakat, a key pillar of the Islamic faith, with aiding the enemies of the nation-state [ibid].

Racial & informational profiling and digital discrimination: Profiling takes place due to discretionary decision-making under vague policies [13]. One such example is the use of Counter Financing of Terrorism (CFT) lists that include the names of people and organizations deemed suspicious of terrorism, predominantly Muslim names [41]. Transactions made to such individuals or organizations are considered as 'material support for terrorists' that results in harsh convictions [52, p.149]. However, financial institutions are instructed not just to block transactions or freeze assets for people on the list, but also for people whose names resemble those on the list thus profiling Muslim names [13]. Individuals whose transactions or assets are blocked or frozen are asked to provide proof of innocence. Moreover, key payment platforms in the US, such as Venmo and PayPal, have demonstrated the racialized treatment of transactions by deeming transactions with Arabic or Persian words and descriptors, added by users in the social features of these applications, as *risky* [64, 112].

Targeting relationships & communities: Attack on diasporic financial ties to home countries extends to immigrant communities in general. While the movement of migrants from the rest of the world to the West is discouraged and controlled, the free movement of capital is ensured under border imperialism. The limitations of migrant movement and the concurrent freedom of capital across borders is a defining element of border imperialism [126]. Puar [95, p.149] states:

> The militarization of urban space is largely accomplished by clamping down on the routine circuits of diasporic connectivity: air travel, financial remittances to families back home, contributions to homeland charities, political organizations, and foundations, and communication networks. This situation mandates a unilateral nationalism. To be a unilateral citizen of the nation-state means foregoing diasporic subjectivity as part of multiple communities across continents while maintaining transnational identities and relationships. The privilege of transnational identification — the ability to sustain political and economic ties to places of belonging and social reproduction that are not American and are not fully subject to U.S. sovereignty - has been the first casualty of the War on Terror [95, p.149].

This is further evidenced by the indiscriminate surveillance of the financial transactions of immigrant communities on a mass scale through subpoenas to Money Transfer Operators (MTOs) with no legal justification [6, 34]. As per the records obtained and analyzed by the American Civil Liberties Union (ACLU) through FOIA requests, as of 2021, the Transaction Record Analysis Center (TRAC) had access to 145 million records of financial transactions shared by MTOs from the U.S. to various countries, and this number is suspected to be growing. TRAC is a non-profit record-holding entity accessed by 600 local, state, and federal law enforcement agencies and field offices in the US [34]. ACLU argues that these subpoenas were illegal and that such mass surveillance practices disproportionately harm immigrant communities that are unbanked and rely on MTOs to send money to their families in their home countries. Thus, bordering regimes and discriminatory lists prohibit the flow of money across countries, targeting relationships and creating isolation for immigrant communities and their families.

6 Extending the Concept of Digital Border Assemblages: Features and Implications

In this section, we extend the concept of digital border assemblages (DBAs) suggested by [22], as explained in §1.1. This concept in its current articulation provides a starting point for thinking about the digital in the context of border assemblages. We extend it toward a more concrete framework by identifying key features of the DBA and elaborating on how ICTs are used, resulting in an evolved set of dynamics, sites, and capabilities, with race at its center. We ground our understanding in the racial formations at the border and the entanglement between racial and social control of mobility and the development of technology for bordering. We then use this understanding to analyze our case studies, resulting in features of DBA in §6.1 and implications for HCI in §6.2.

In what follows, we identify and expand on the following features of DBA: racial and informational profiling (§6.1.1), discriminatory practices (§6.1.2), making racialized subjects legible (§6.1.3), obscurity (§6.1.4), expanding borders (§6.1.5), attack on social relations (§6.1.6), racialized surveillance through forced disclosures (§6.1.7), and enacting borders through self-governmentality (§6.1.8). This has implications for HCI research in interrogating digital border assemblage, developing new methods with/inspired by legal studies to uncover and interrogate border assemblages that continue to reproduce racialized forms of control of migrant bodies §6.2.

6.1 Identifying the features of Digital Border Assemblages

In this section, we map our conceptual foundation onto the case studies to identify various features of DB and highlight the ways in which ICTs enable and perpetuate racialized control of migrant subjects of the state.

6.1.1 Racial and informational profiling. Racial profiling involves separating a subsection of the population based on specific criteria that correlate to risk, subjecting them to special scrutiny to prevent violence or crime [13]. Airports use racialized surveillance through ocular and informational profiling [95]. In ocular profiling, features like afros, beards, turbans, and headscarves are deemed dangerous when worn by people of color, leading to intrusive physical (pat-downs, luggage inspections) and digital (device scans, x-rays) checks. Epidermalization refers to the imposition of race on the body [18, p.7], where bodily markers impede security clearance [18, p.138].

Informational profiling digitizes the body through biometrics and scanners, with data stored in databases, preemptive screenings, and trusted traveler programs. Puar [95, p.197-202] compares the panopticon and informational profiling and argues that they are both *biopolitical*[7] control models[54]. While the panopticon[8] isolated racialized bodies, informational profiling accuses individuals before they form a subject, dispersing control through multiple sites of anxiety. Both models produce the terrorist and patriot in one body, reinforcing discrimination against certain citizens. Profiling leads to discriminatory practices, as discussed in section 6.1.2.

In our case studies, we observe privacy intrusions based on racial profiling and surveillance of people and capital crossing borders. In Case Study 1, racial profiling of Muslims exposes them to disproportionate device searches at borders. Basic searches might rely on ocular profiling, but forensic searches often involve informational profiling, e.g. name in a list that triggers a search. In Case Study 2, profiling people crossing the U.S.- Mexico border as *illegals* or criminals at flight risk justifies location tracking via ankle monitors and apps. In Case Study 3, the use of Counter-Terrorism Financing laws and databases to profile names and transactions involving Muslims or migrant communities of color indicates informational

[7] Biopower, a concept developed by Michel Foucault, refers to a form of power that takes life itself as its target. It operates through two modes: anatamopolitics, which governs individual bodies, and biopolitics, which regulates entire populations. By claiming to manage or protect life, biopower intensifies control through precise regulations while remaining resistant to criticism. [128, p.145]

[8] The concept of the panopticon in surveillance describes how individuals internalize discipline due to the fear of constant observation by an authority, leading them to regulate their own behavior[18, p.33-35].

racial profiling based on religion, race, ethnicity, and country of origin.

Although not part of our case studies, ICTs are increasingly used to create informational profiles that preemptively identify individuals as a *threat* based on ideological differences, preventing entry to the nation-state [69] or controlling them if already within the state [103]. Informational profiling extends the U.S. surveillance globally through practices like *extreme vetting* and *preclearance*, classifying visa applicants and travelers before they arrive in the U.S. Profiles are created using big data from online sources such as social media, apps, locations, search and travel histories, relationships, religion, and shopping, forming a global caste system that allows some (e.g., U.S., Europe, Australia) to travel freely while restricting others [68].

6.1.2 Discriminatory practices. Border assemblages involve practices that create and maintain borders, shaping reality through repetition [38, p.23-33]. Border policies are often enacted discriminatorily at airports, giving officials discretion in deciding outcomes on the use of bordering technologies like passports, trusted traveler programs, and scanners [18][9]. For example, trusted traveler programs, while offering privileged access, can be applied discriminatorily [110], and rely on mutual trust, which may be absent for those deemed dangerous by the state [18].

Racial profiling and ICTs intersect in DBA through discriminatory practices. Border agents and financial institutions discriminate in enforcing policies like device inspections (Case Study 1) and counter-financing terrorism (Case Study 3). While privacy is not guaranteed at the border [78], these practices disproportionately target certain racial groups, enabling data collection that hampers mobility §6.1.7, informs technology development [125], and leads to social isolation by surveilling relationships §6.1.6, limiting research, free speech, and belonging through internalized borders §6.1.8.

6.1.3 Making racialized subjects legible. The state's goal of making certain bodies more legible is central to statecraft, particularly in border and mobility management. Over time, with increasing datafication, the techniques for achieving legibility have become more sophisticated, though the motivation remains the same — *appropriation, control, and manipulation* [108, p.77].

In border assemblages, racial categories like *criminals, terrorists, and illegals* are framed as threats [127], whose lives must be *documented* through increased surveillance, data extraction, and panoptic sorting [18]. The synoptic view available to border control institutions allows them to command and control movement [56] not only at borders but across the nation-state for certain racialized groups. This ongoing project of legibility leads to expanding bordering sites resulting in oppressive discriminatory interventions [108][10]. Increased legibility continues to result in detentions and deportations of racialized immigrants, refugees, and asylum seekers [63, 95].

DBA creates legibility of racial others through databases and lists that target individuals based on race, ethnicity, or nationality, enabling increased surveillance and control. These lists function as a form of panoptic sorting, a discriminatory tool that categorizes individuals by race, gender, or neighborhood, ignoring the complexities that define them [19]. In our case studies, racialized surveillance occurs at two levels: First, at the data collection stage, where migrants, asylum seekers, and Muslim travelers are specifically targeted for privacy-invasive inspections that extract personal data (Case Studies 1 and 2) [57]. Second, through the discriminatory assembly of data, such as the creation of lists based on ethnicity, nationality, and religion. For instance, the Counter Financing of Terrorism (CFT) lists focus on individuals with Muslim names, applying restrictions to others with similar identifiers, thus profiling Muslims disproportionately [41] (Case Study 2). This discriminatory data collection and assembly exacerbate racial profiling and surveillance, reinforcing the marginalization of targeted groups.

We argue that the border's technological apparatus creates state legibility around racialized others, whether migrants or citizens. The cybernetic border converts physical border management into an informational and technological issue, making the racial other legible (see §4). Case studies show that ICTs enable a more granular level of legibility, monitoring thoughts, behaviors, financial transactions, and relationships, internalizing borders into every aspect of the racial subject's life.

6.1.4 Obscurity and the techno-legal nature of exploration. Borders serve as tools of state violence, obscured by bureaucratic delays and denials, as explored through studying-up [73] (see §3.2). One example of this is the National Immigration Justice Center, through FOIA requests, gained access to documentation like lists of detention facilities and ICE inspection reports. However, Hernandez [44] argues that border management is obscured in several ways: 1) delays in FOIA fulfillment, leading to lawsuits by legal firms; 2) spatial obscurity of detention practices by establishing such centers in remote areas out of sight of people; 3) for-profit corporations, which are exempt from FOIA and resist transparency laws.

Delays in FOIA requests keep border practices like data extraction hidden (Case Study 3), with private companies blurring the line between technologies of everyday use and bordering technologies [61, 70]. Unlike government bodies, private companies are not required to disclose information, and regulatory loopholes allow governments to access private data without a warrant [20].

For travelers and migrants, the use of ICTs in DBAs limit the disclosure of policies, data storage practices(Case Study 2), and statistics on affected individuals (Case Study 1). As demonstrated in Case Study 1, device inspections targeting Muslim U.S. citizens were revealed through advocacy reports. At the data level, ICE's claims about data storage and access contradict actual practices (Case Study 2). Uncovering and resisting DBAs requires expertise in technology, law, privacy, civil rights, and legal procedures to access relevant information.

6.1.5 Borders as site of exception and expanding sites. As discussed in section 4, borders are sites of exception, marked by exceptional violence [32] and privacy exemptions [78]. These exceptions are applied to certain racial groups deemed a threat to the nation, justifying their over-surveillance. Building on critical border studies that view borders as networked, invisible, and located in non-traditional spaces [48, 88], we highlight new sites of bordering enabled by

[9]Browne [18] cites cases where black travelers with valid passports were deemed untrustworthy and required additional biometric proof of identity.

[10]Scott [108] cites the creation of a list of Jewish people in Nazi-occupied Amsterdam, which led to their deportation, demonstrating how state legibility can have deadly outcomes

ICTs. These include the sites of migrant bodies (Case Study 2), families and communities, traveler devices, data, online activities and communications, digital relationships (Case Study 1), and financial support for families globally (Case Study 3). Through ICTs and associated data, both the scope and duration of surveillance and bordering are expanding. The range of behaviors and information scrutinized to grant mobility is growing. Borders are increasingly becoming digital, amplified by the online surveillance dragnet [125]. As these bordering sites expand, privacy exceptions extend to new areas, leading to the surveillance of all aspects of a racialized person's life.

6.1.6 Attacking relational ties/social isolation. As shown in the case studies, digital surveillance through ICTs targets relationships within communities of color and migrant groups by scrutinizing their networks as a condition for entry. This includes extracting data from devices (Case Study 1), tracking location (Case Study 2), and monitoring financial transactions (Case Study 3). In Case Study 1, authorities questioned Muslim travelers about their networks, profiled those traveling to Muslim-majority countries, and copied data from devices. Case study 3 reveals the surveillance of remittance transfers, while case study 2 shows location tracking through ankle monitors for asylum seekers (case study 2) violates civil rights. Location is also tracked by purchasing location data from data brokers for Muslim prayer apps [29, 30]. Social media profiles of visa applicants are also monitored [49]. All these practices present surveillance of relational ties and might be used to deport and detain migrant community members (Case Study 2) or to file criminal charges using financial data (Case Study 3). Racialized surveillance targets entire communities, violating privacy by treating them as threats by association. This can force individuals to isolate themselves or be isolated, enacting borders through self-governmentality, as discussed in §6.1.8.

6.1.7 Racialized surveillance in the form of data extraction and forced self-disclosures. Borders and migrant bodies are increasingly sites of datafication, where individuals are transformed into sources of raw data for surveillance systems [125]. Lippert [55] argues that *liberal governmentality* operates by asserting authority from a distance through the symbolic power of the law, fostering self-discipline through the potential for scrutiny of the specified legal authorities' actions. However, Browne [18] critiques this approach, noting that racialized subjects lack the privilege of voluntary participation and are often forced into compliance.

As Case Studies 1 and 2 demonstrate, racialized migrants are compelled to disclose private information to gain entry into the US, forming the foundation of surveillance technologies [125]. These case studies show how self-disclosure is coerced through various means—forced disclosures at the border (Case Study 1), data collection through ankle monitors (Case Study 2), and hidden monitoring of financial transactions (Case Study 3). Other examples include the collection of social media handles and email addresses for visa applicants [26], and tracking the routes taken by undocumented migrants to exploit their vulnerability.

Privacy exceptions at the border [78], such as border patrol's authority to inspect electronic devices, suspend the privacy rights of all travelers. However, discriminatory application of such laws (Case Study 1) can result in a racialized distribution of privacy [97]. Furthermore, practices of location tracking through ankle monitors (Case Study 2) or purchasing data from data brokers internalize borders across the country, revealing personal information about tracked individuals, such as health, religious beliefs, ethnicity, political opinions, socio-economic status, and social activities [15].

6.1.8 Borders enacted through self-governmentality. Technology's role in border assemblages complicates both the *site* of bordering and the *entity* performing it. Some ICTs designed for widespread use (e.g. electronic devices, social media, search engines etc.) get incorporated into DBAs due to practices (Case Study 1 and 3) like *extreme vetting* or *pre-vetting* [68, 96]. While others designed specifically for migrant populations (e.g., refugeeTech, asylum application apps) might have components of surveillance for movement control and tracking built into them (Case Study 2) [51, 63]. Both types of ICTs bifurcate people into different strata with marginal benefits compared to the associated cost [63].

Incorporating a wide range of data streams into bordering and surveillance regimes can lead to *information panics*[11] and self-policing, resulting in secondary effects such as epistemic consequences. Users may limit their mobility in physical and digital spaces (Case Studies 1 and 2), enforcing digital borders on themselves due to internalized governmentality [63, 96]. This highlights the need for public understanding of how data and technologies are used in border assemblages, raising questions about transparency.

6.2 Implications for HCI: Interrogating role of ICTs in digital border assemblages

In this section, we further suggest how HCI researchers can begin to understand their role in interrogating the digital border assemblages. In connecting back to existing domains within HCI that are encountering borders and migration in other ways, we identify how these lines of work can engage in further examination of the role of ICTs in enabling DBAs.

6.2.1 Studying DBAs. We argue that although migration scholarship in HCI has focused on studying and designing technologies for the integration and settlement of refugees, migrants, and asylum seekers in host countries, including through participatory design (see §1.1), there is a need to expand the research agenda to examine ICTs' role in DBAs. This paper demonstrates the key features of DBAs, highlighting that HCI research can no longer be limited to developing technologies for integration. Researchers must also understand how technology is used for bordering, how technologies specifically designed for this purpose operate, and how everyday technologies—such as social media, payment systems, communications, and location tracking—are incorporated into DBAs through obscurity and legal loopholes.

As discussed in §6.1.4, **DBAs are opaque, and combating this obscurity requires collaboration with legal scholars**. There is a practice gap in HCI necessary to detect, uncover, and understand

[11] Mahmoudi [63] cites the case study of the LinkNYC kiosks across NYC where asylees and migrants can seek information through free Wi-Fi and language services which were previously mediated through people. However, the kiosks are equipped with surveillance technologies like cameras, Bluetooth sensors and pick up on a wide range of device-related information including browser type, time zone settings and language which can be detrimental to the immigrants and asylees using these kiosks. This has led to getting information from word of mouth and avoiding using kiosks which he refers to as information panics.

DBAs. This underscores the need for cross-disciplinary collaboration, as understanding DBAs and their consequences is impossible without legal expertise. This gap also highlights the challenge for HCI researchers: social computing technologies operate within this space, yet remain largely unexamined. For HCI researchers to identify which groups are affected by DBAs, these structures must first be identified. The obscurity of DBAs raises further questions about users' awareness of their impact. If these systems are so difficult to study, how can users be aware of them and protect themselves?

The narratives surrounding border technologies often focus on documenting 'illegal' migrants or Muslim 'terrorist' suspects, collecting data to predict potential threats, thereby justifying technologies like the SMARTLink app and ankle monitors, as well as practices such as device inspections at ports of entry. These practices violate the privacy and rights of both racialized citizens and non-citizens. However, the experiences of migrants, asylum seekers, and citizens targeted by ICTs in DBAs are poorly understood, with most insights coming from case reports by legal advocacy groups. This presents an opportunity for the HCI community to explore.

Orlikowski [85, p.9] argues that technology use is not a fixed choice from a predefined set of possibilities, but a situated process of enactment that may invent new patterns of use. She distinguishes between technologies as artifacts and technologies-in-practice, noting that the intended affordances of technology may differ from how it is used in practice. As discussed in §6.1.8, users impacted by DBAs might engage in self-governmentality, altering their technology use patterns to protect themselves from the harms of racialized surveillance. They may resist using technologies designed for widespread use if these technologies perpetuate racialized surveillance and neoliberal imperialistic agendas. Such technologies should be considered, specified, and designed with a focus on the potential harms and benefits for those lower in the matrix of domination, ensuring their voices are represented in the design process [27]. Furthermore, HCI researchers need to broaden their understanding of migration by considering the expanded sites of bordering, as demonstrated in our work.

6.2.2 Foregrounding race and relationality in privacy and migration. Borders inherently function as a system of racialized mobility management. Through case studies (§4.2) and a review of critical literature (§4), we have shown that border assemblages combine racial narratives and technological artifacts designed to surveil racial 'Others,' such as Blacks, Latinos/ex, Muslims, and Arabs. However, a review of HCI literature on migration (§2.1) and privacy (§2.2) reveals a lack of attention to race, even when it is central. In §6.1, we demonstrated how ICTs in DBAs perpetuate racialized surveillance through practices like racial profiling (§6.1.1), discriminatory practices (§6.1.2), and forced data extraction (§6.1.7). Matt Reichel [97] argues that privacy is unequally distributed across racial and class lines, with marginalized groups, particularly people of color, being denied equitable access to privacy. He warns that focusing solely on privacy rights can legitimize targeted surveillance over mass surveillance, reinforcing racial profiling. We propose that HCI, privacy, and migration research adopt a critical approach to privacy in migration, focusing on racial differences.

DBAs surveil not only individuals but also their networks of relationships, putting the privacy of families, groups, and communities at risk 6.1.6. Privacy scholars emphasize the **relational nature of privacy** [14, 60, 98], which considers social relationships and contextual factors, rather than focusing solely on individual control over personal data. Privacy evolves through interactions with others and is embedded in cultural and social contexts [14]. However, work on privacy in migrant communities is limited, mainly focusing on individual privacy (§1.1). Previous HCI migration studies highlight the role of smartphones in maintaining relationships across migration, focusing on information-seeking before, during, and after migration, taking an *asset-based approach*[131][12] to ICTs' role in migration 2.2. We propose a *relational approach*[13] to migration and privacy research, focusing on communities and groups to assess the material and psychological harms of surveillance on migrant and racialized communities. This approach should consider how the management of locations, activities, and mobility affects not only individuals but also those they are connected to.

6.2.3 Performing migration, citizenship, and activism in an evolving DBAs. Performing *borderwork* [101] involves engaging with the legal, technological, and bureaucratic processes that define borders and citizenship. People often discover they are subject to additional scrutiny, restricted access to travel, or inclusion in surveillance databases through personal experiences at borders, communication with legal advocacy groups, or transparency mechanisms like FOIA requests. Once aware, individuals must engage in various forms of *borderwork* to resist or escape these systems. This involves a combination of legal challenges, such as filing lawsuits or appeals, utilizing administrative reviews, and leveraging legal networks; transparency efforts through accessing data or uncovering discriminatory practices; and collective action, including grassroots organizing and advocacy campaigns. The work to exit these systems requires strategic navigation of opaque governmental and technological systems, resistance against systemic profiling, and coordinated efforts to challenge the policies and corporate structures underpinning DBAs. We suggest that HCI researchers study this multi-layered resistance both at an individual by those affected and at a collective level by advocacy groups and activists to understand the borderwork involved in subverting oppressive effects of DBAs.

7 Conclusion

Border studies scholars Chouliaraki & Georgiou [22] presented the concept of digital border assemblages. Although this concept offers an invitation to understand more closely the role of the digital in border assemblages that continue to govern migrant subjects of the state, the current discourse does not explore the role of ICTs beyond their role in the platformed narratives of the symbolic border. We expand on the existing understanding of DBA by locating the role of ICTs and identifying key features through which they perform racialized control, thus concretizing the concept of DBA toward a framework. Applying a critical-interpretive approach involving

[12] An asset-based approach to technology design focuses on leveraging existing strengths, resources, and capabilities—rather than emphasizing gaps or problems—to create innovative and inclusive technological solutions. This approach recognizes and builds upon the assets of users, communities, and organizations to design technology that is empowering, sustainable, and aligned with their needs. [131]

[13] A relational approach to technology design focuses on the relationships between people, technology, and their environments. An asset-based approach and a relational approach are distinct but can overlap in some ways.

relevant literature in critical border studies, HCI and migration, surveillance, and border technology, we develop a conceptual foundation that helps us understand racial formations at/by the border. Then, through a synthesis of three case studies on the use of ICTs for bordering, we determine how ICTs enable key features of DBA, further illustrating that a close examination of the role of ICTs in DBA helps us get a more concrete understanding of border assemblages. Although existing knowledge of DBAs considers technologies specifically designed for the border as part of the material infrastructure determining mobility, we also assess technologies of the border and everyday use that are implicated in the DBAs for decisions on migration and mobility. This has implications for HCI researchers in uncovering and interrogating DBAs by developing appropriate methods that facilitate this interrogation.

Acknowledgments

This paper is based on work supported by the National Science Foundation under Grant No. 2310515. We thank Hannah Lucal for her help in developing case studies. The authors also thank Ishtiaque Ahmed (CS Department, University of Toronto), Kate Starbird (Dept of Human-Centered Design & Engineering, University of Washington), and Richard Anderson (Paul G Allen School of Computer Science & Engineering, University of Washington) for their feedback on this work during its early stages. Finally, we extend our gratitude to the scholars, advocacy organizations, and migrant justice activists whose work forms the foundation of our case studies.

References

[1] Ruba Abu-Salma, Reem Talhouk, Jose Such, Claudia Aradau, Francesca Meloni, Shijing He, Syed Ishtiaque Ahmed, Cansu Ekmekcioglu, Dina Sabie, Rikke Bjerg Jensen, Jessica McClearn, Anne Weibert, Max Krüger, Faheem Hussain, and Rehema Baguma. 2023. Diverse Migration Journeys and Security Practices: Engaging with Longitudinal Perspectives of Migration and (Digital) Security. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–7. doi:10.1145/3544549.3573800

[2] E Tendayi Achiume. 2021. Racial borders. *Geo. LJ* 110 (2021), 445.

[3] Amelia Acker and Dhiraj Murthy. 2020. What is Venmo? A descriptive analysis of social features in the mobile payment platform. *Telematics and Informatics* 52 (Sept. 2020), 101429. doi:10.1016/j.tele.2020.101429

[4] Muslim Advocates. 2009. Unreasonable Intrusions: Investigating the Politics, Faith & Finances of Americans Returning Home. https://muslimadvocates.org/advocacy/report-unreasonable-intrusions-investigating-the-politics-faith-finances-of-americans-returning-home/.

[5] Giorgio Agamben. 2008. *State of exception*. University of Chicago press, Chicago, IL.

[6] Hamed Aleaziz. 2022. Immigrants sue ICE for spying on their financial records. https://www.latimes.com/world-nation/story/2022-12-12/immigrants-ice-lawsuit-spying-money-orders Section: World & Nation.

[7] Amanda Alencar. 2018. Refugee integration and social media: A local and experiential perspective. *Information, Communication & Society* 21, 11 (2018), 1588–1603.

[8] Sabrina Alimahomed-Wilson. 2019. When the FBI knocks: Racialized state surveillance of Muslims. *Critical Sociology* 45, 6 (2019), 871–887.

[9] Louise Amoore. 2006. Biometric borders: Governing mobilities in the war on terror. *Political geography* 25, 3 (2006), 336–351.

[10] Benedict Anderson. 2008. Imagined Communities: Reflections on the origin and spread of nationalism. In *The New Social Theory Reader* (2 ed.). Routledge.

[11] Arjun Arunasalam, Habiba Farrukh, Eliz Tekcan, and Z. Berkay Celik. 2024. Understanding the Security and Privacy Implications of Online Toxic Content on Refugees. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 4373–4390. https://www.usenix.org/conference/usenixsecurity24/presentation/arunasalam

[12] Knight First Amendment Institute at Columbia University. 2024. Knight Institute v. DHS | Knight First Amendment Institute. https://knightcolumbia.org/cases/knight-institute-v-dhs-device-searches

[13] Reem Bahdi. 2003. No Exit: Racial Profiling and Canada's War against Terrorism. *Osgoode Hall Law Journal* 41, 2 (April 2003), 293–317. doi:10.60082/2817-5069.1413

[14] Sara Bannerman. 2019. Relational privacy and the networked governance of the self. *Information, Communication & Society* 22, 14 (2019), 2187–2202.

[15] Benjamin Baron and Mirco Musolesi. 2020. Where you go matters: A study on the privacy implications of continuous location tracking. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 4 (2020), 1–32.

[16] Johana Bhuiyan. 2022. Poor tech, opaque rules, exhausted staff: inside the private company surveilling US immigrants. https://www.theguardian.com/us-news/2022/mar/07/us-immigration-surveillance-ice-bi-isap.

[17] Aaron Boyd. 2018. CBP Officers Aren't Deleting Data After Warrantless Device Searches, IG Says - Nextgov/FCW. https://www.nextgov.com/cybersecurity/2018/12/cbp-officers-arent-deleting-data-after-warrantless-device-searches-ig-says/153425/

[18] Simone Browne. 2015. *Dark Matters: On the Surveillance of Blackness*. Duke University Press, Durham, NC.

[19] John Edward Campbell and Matt Carlson. 2002. Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media* 46, 4 (Dec. 2002), 586–606. doi:10.1207/s15506878jobem4604_6

[20] Isabelle Canaan. 2021. A Fourth Amendment Loophole?: An Exploration of Privacy and Protection through the Muslim Pro Case. *HRLR Online* 6 (2021), 95.

[21] Monica Caraway, Daniel A. Epstein, and Sean A. Munson. 2017. Friends Don't Need Receipts: The Curious Case of Social Awareness Streams in the Mobile Payment App Venmo. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 1–17. doi:10.1145/3134663

[22] Lilie Chouliaraki and Myria Georgiou. 2019. The digital border: Mobility beyond territorial and symbolic divides. *European Journal of Communication* 34, 6 (Dec. 2019), 594–605. doi:10.1177/0267323119886147 Publisher: SAGE Publications Ltd.

[23] Lizzie Coles-Kemp and Rikke Bjerg Jensen. 2019. Accessing a new land: Designing for a social conceptualisation of access. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Glasgow, Scotland, 1–12.

[24] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. 2018. In a new land: mobile phones, amplified pressures and reduced capabilities. In *Proceedings of the 2018 chi conference on human factors in computing systems*. Association for Computing Machinery, Montreal, Canada, 1–13.

[25] Republican Homeland Security Committee. 2024. Chairmen Higgins, Bishop Open Joint Hearing: Border Security Technologies "Play a Critical Role" In Countering Threats, Mass Illegal Immigration. https://homeland.house.gov/2024/07/09/chairmen-higgins-bishop-open-joint-hearing-border-security-technologies-play-a-critical-role-in-countering-threats-mass-illegal-immigration/.

[26] Saira Hussain and Sophia Cope. 2024. EFF to D.C. Circuit: The U.S. Government's Forced Disclosure of Visa Applicants' Social Media Identifiers Harms Free Speech and Privacy. https://www.eff.org/deeplinks/2024/02/eff-dc-circuit-us-governments-forced-disclosure-visa-applicants-social-media

[27] Sasha Costanza-Chock. 2020. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, Cambridge, MA, USA.

[28] American Immigration Council. 2024. The Cost of Immigration Enforcement and Border Security. https://www.americanimmigrationcouncil.org/research/the-cost-of-immigration-enforcement-and-border-security.

[29] Joseph Cox. 2020. How the U.S. Military Buys Location Data from Ordinary Apps. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[30] Joseph Cox. 2021. Leaked Location Data Shows Another Muslim Prayer App Tracking Users. https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first.

[31] Kevin Monahan Cynthia McFadden; E.D.Cauchi, William M. Arkin. 2017. American citizens: U.S. border agents can search your cellphone. https://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746.

[32] Jason De León. 2015. *The land of open graves: Living and dying on the migrant trail*. Vol. 36. Univ of California Press.

[33] Rianne Dekker, Godfried Engbersen, Jeanine Klaver, and Hanna Vonk. 2018. Smart refugees: How Syrian asylum migrants use social media information in migration decision-making. *Social Media+ Society* 4, 1 (2018), 2056305118764439.

[34] Fikayo Walter-Johnson and Nathan Freed Wessler. 2023. How the Arizona Attorney General Created a Secretive, Illegal Surveillance Program to Sweep up Millions of Our Financial Records | ACLU. https://www.aclu.org/news/privacy-technology/how-the-arizona-attorney-general-created-a-secretive-illegal-surveillance-program

[35] Mirko Forti. 2020. Migrants and refugees in the cyberspace environment: privacy concerns in the European approach. *European Journal of Privacy Law & Technology* 2 (2020), 241.

[36] Christian Fuchs. 2013. Critique of the political economy of web 2.0 surveillance. In *Internet and Surveillance*. Routledge, United Kingdom, 31–70.

[37] Setareh Ghandehari. 2022. Number of Immigrants Under Punitive Surveillance Quadrupled on Biden's Watch. https://truthout.org/articles/number-of-immigrants-under-punitive-surveillance-quadrupled-on-bidens-watch/.

[38] Damon Golsorkhi, Linda Rouleau, David Seidl, and Eero Vaara. 2010. *Cambridge Handbook of Strategy as Practice*. Cambridge University Press. Google-Books-ID: Rx87NnaK03wC.

[39] Ashley N Gomez. 2020. Over the Border, Under What Law: The Circuit Split over Searches of Electronic Devices on the Border. *Ariz. St. LJ* 52 (2020), 279.

[40] Ricardo Gomez, Ivette Bayo, Philip Reed, Cherry Wang, and Marisol Silva. 2013. Fearless Cards: A Low-Tech Solution to Help Overcome Emotional Barriers to ICT Adoption Among Marginalized Populations. *The Electronic Journal of Information Systems in Developing Countries* 56, 1 (2013), 1–15.

[41] Government of Canada. 2024. Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. https://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-360/page-1.html#h-672920

[42] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile?: Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–15. doi:10.1145/3173574.3173688

[43] Kevin D. Haggerty and Richard V. Ericson. 2000. The surveillant assemblage. *The British Journal of Sociology* 51, 4 (2000), 605–622. doi:10.1080/00071310020015280

[44] David Hernandez. 2013. Detained in obscurity: The US immigrant detention regime. *NACLA Report on the Americas* 46, 3 (2013), 58–63.

[45] Joey Chiao-Yin Hsiao and Tawanna R Dillahunt. 2018. Technology to support immigrant access to social capital and adaptation to a new country. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–21.

[46] Immigration and Customs Enforcement. 2023. Detention Management. https://www.ice.gov/detain/detention-management.

[47] Immigration and Customs Enforcement. 2024. Alternatives to Detention. https://www.ice.gov/features/atd.

[48] Corey Johnson, Reece Jones, Anssi Paasi, Louise Amoore, Alison Mountz, Mark Salter, and Chris Rumford. 2011. Interventions on rethinking 'the border' in border studies. *Political Geography* 30, 2 (Feb. 2011), 61–69. doi:10.1016/j.polgeo.2011.01.002

[49] Amy L. Peck Joseph J. Lazzarotti. 2024. Privacy Issues of U.S. Collection of Social Media Information from Visa Applicants. https://natlawreview.com/article/privacy-issues-us-collection-social-media-information-visa-applicants.

[50] Katja Kaufmann. 2018. Navigating a new life: Syrian refugees and their smartphones in Vienna. *Information, Communication & Society* 21, 6 (2018), 882–898.

[51] Austin Kocher. 2023. Glitches in the Digitization of Asylum: How CBP One Turns Migrants' Smartphones into Mobile Borders. *Societies* 13, 6 (June 2023), 149. doi:10.3390/soc13060149 Number: 6 Publisher: Multidisciplinary Digital Publishing Institute.

[52] Deepa Kumar. 2012. *Islamophobia and the Politics of Empire*. Haymarket Books, Chicago, IL, USA.

[53] Thomas Lemke. 2002. Foucault, Governmentality, and Critique. *Rethinking Marxism* 14, 3 (2002), 49–64. doi:10.1080/089356902101242288 Publisher: Routledge _eprint: https://doi.org/10.1080/089356902101242288.

[54] Thomas Lemke. 2010. Beyond Foucault: From biopolitics to the government of life. In *Governmentality*. Routledge, 173–192.

[55] Randy Lippert. 2009. Signs of the Surveillant Assemblage: Privacy Regulation, Urban CCTV, and Governmentality. *Social & Legal Studies* 18, 4 (Dec. 2009), 505–522. doi:10.1177/0964663909345096 Publisher: SAGE Publications Ltd.

[56] Iván Chaar López. 2024. *The Cybernetic Border: Drones, Technology, and Intrusion*. Duke University Press.

[57] David Lyon. 2003. *Surveillance After September 11*. Polity, Cambridge, UK.

[58] David Lyon. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society* 1, 2 (2014), 2053951714541861.

[59] David Lyon and Centre for International Governance. 2019. *State and Surveillance*. Technical Report. Centre for International Governance Innovation. 21–25 pages. https://www.jstor.org/stable/resrep26129.6

[60] Yuanye Ma. 2019. Relational privacy: Where the East and the West could meet. *Proceedings of the Association for Information Science and Technology* 56, 1 (2019), 196–205.

[61] Dave Maas. 2024. Hundreds of Tech Companies Want to Cash In on Homeland Security Funding. Here's Who They Are and What They're Selling. | Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/06/hundreds-tech-companies-want-cash-border-security-funding-heres-who-they-are-and

[62] Mirca Madianou. 2019. The biometric assemblage: Surveillance, experimentation, profit, and the measuring of refugee bodies. *Television & New Media* 20, 6 (2019), 581–599.

[63] Matthew Mahmoudi. 2021. *Race & Mobility in the Digital Periphery: New Urban Frontiers of Migration Control*. Ph. D. Dissertation. University of Cambridge.

[64] Aaron Mak. 2020. Why You Can Venmo for "Cocaine" or "Bomb" but Not a "Cubano Sandwich". https://slate.com/technology/2020/02/paypal-venmo-iran-syria-sanctions-crime-detection-system.html.

[65] Zane McNeill. 2023. New ICE Program Subjects Asylum Seekers to GPS Monitoring and Curfew. https://truthout.org/articles/new-ice-program-subjects-asylum-seekers-to-gps-monitoring-and-curfew/.

[66] Mijente. 2022. *Tracked and Trapped: Experiences from ICE Digital Prisons*. Technical Report. Mijente. https://notechforice.com/digitalprisons/

[67] Mijente, Just Futures Law, and Community Justice Exchange. 2022. *ICE FOIA Lawsuit: Fact Sheet*. Technical Report. Mijente.

[68] David Miller. 2013. Border Regimes and Human Rights. *The Law & Ethics of Human Rights* 7, 1 (Aug. 2013), 1–23. doi:10.1515/lehr-2013-0001 Publisher: De Gruyter Section: Law & Ethics of Human Rights.

[69] Todd Miller. 2019. *Empire of borders: The expansion of the US border around the world*. Verso Books, New York.

[70] Diego Naranjo Molnar, Petra. 2020. The Privatization of Migration Control. https://www.cigionline.org/articles/privatization-migration-control/

[71] Petra Molnar. 2020. Technological testing grounds: Migration management experiments and reflections from the ground up.

[72] Michael D Myers and Heinz K Klein. 2011. A set of principles for conducting critical research in information systems. *MIS quarterly* (2011), 17–36.

[73] Laura Nader. 2018. Chapter 1. Up the Anthropologist: Perspectives Gained From Studying Up. In *The Unwritten Rules of Academia*. Berghahn Books, New York, Oxford, 12–32.

[74] Sid Nadkarni. 2013. Let's Have a Look, Shall We: A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices. *UCLA Law Review* 61 (2013), 146. https://heinonline.org/HOL/Page?handle=hein.journals/uclalr61&id=144&div=&collection=

[75] Baljt Nagra and Paula Maurutto. 2016. Crossing borders and managing racialized identities: Experiences of security and surveillance among young Canadian Muslims. *Canadian Journal of Sociology* 41, 2 (2016), 165–194.

[76] Thomas Nail. 2017. What is an Assemblage? *SubStance* 46, 1 (2017), 21–37. https://www.jstor.org/stable/26451291 Publisher: University of Wisconsin Press.

[77] Sarah Nikkhah, Andrew D Miller, and Alyson L Young. 2018. Telegram as an immigration management tool. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*. Association of Computing Machinery, New Jersey, USA, 345–348.

[78] Laura Nowell. 2018. Privacy at the border: Applying the border search exception to digital searches at the united states border. *Fed. Comm. LJ* 71 (2018), 85.

[79] Office of Field Operations U.S. Customs and Border Protection. 2018. Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices. https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf#page=5.67

[80] Department of Homeland Security. 2022. DHS/CBP/PIA-006 Automated Targeting System | Homeland Security. https://www.dhs.gov/publication/automated-targeting-system-ats-update

[81] Department of Homeland Security. 2024. S&T Mobile Device Acquisition | Homeland Security. https://www.dhs.gov/publication/st-mobile-device-acquisition

[82] OFFICE OF INSPECTOR GENERAL Department of Homeland Security. 2021. CBP Continues to Experience Challenges Managing Searches of Electronic Devices at Ports of Entry (REDACTED). https://repository.library.georgetown.edu/bitstream/handle/10822/1081865/OIG-21-63-Sep21-Redacted.pdf?sequence=1

[83] Office of Sen. Wyden, Oregon. 2023. Sen. Wyden's Letter to DOJ IG on money transfer surveillance.

[84] American Bar Association Commission on Immigration. 2018. Electronic Monitoring of Migrants: Punitive not Prudent. https://www.americanbar.org/content/dam/aba/administrative/immigration/electronic-monitoring-report-2024-02-21.pdf#page=15.14.

[85] Wanda J. Orlikowski. 2000. Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organization Science* 11, 4 (2000), 404–428. http://www.jstor.org/stable/2640412

[86] Wanda J Orlikowski and Jack J Baroudi. 1991. Studying information technology in organizations: Research approaches and assumptions. *Information systems research* 2, 1 (1991), 1–28.

[87] Kentrell Owens, Camille Cobb, and Lorrie Cranor. 2021. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 62, 18 pages. doi:10.1145/3411764.3445055

[88] Noel Parker and Nick Vaughan-Williams. 2009. Lines in the sand? Towards an agenda for critical border studies. *Geopolitics* 14, 3 (2009), 582–587.

[89] Jonathon W Penney. 2016. Chilling effects: Online surveillance and Wikipedia use. *Berkeley Tech. LJ* 31 (2016), 117.

[90] Lisbeth Perez. 2024. Lawmakers Push for More Border Technology Funding. https://www.meritalk.com/articles/lawmakers-push-for-more-border-technology-funding/.

[91] Laura R. Pina, Carmen Gonzalez, Carolina Nieto, Wendy Roldan, Edgar Onofre, and Jason C. Yip. 2018. How Latino Children in the U.S. Engage in Collaborative Online Information Problem Solving with their Families. *Proceedings of the*

ACM on Human-Computer Interaction 2, CSCW, Article 140 (Nov 2018), 26 pages. doi:10.1145/3274409

[92] Marlei Pozzebon. 2004. Conducting and evaluating critical interpretive research: Examining criteria as a key component in building a research tradition. *Information systems research: Relevant theory and informed practice* (2004), 275–292.

[93] U.S. Customs and Border Protection. 2018. CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant. https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf#page=1.74

[94] U.S. Customs and Border Protection. 2021. CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics | U.S. Customs and Border Protection. https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and

[95] Jasbir K. Puar. 2017. *Terrorist Assemblages: Homonationalism in Queer Times*. Duke University Press, Durham, NC.

[96] Lubna Razaq and Sucheta Ghoshal. 2024. What to the Muslim is Internet search: Digital Borders as Barriers to Information. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 773, 17 pages. doi:10.1145/3613904.3642770

[97] Matt Reichel. 2017. Race, Class, and Privacy: A Critical Historical Review. *International Journal of Communication* 11, 0 (Nov. 2017), 12. https://ijoc.org/index.php/ijoc/article/view/7018 Number: 0.

[98] Urbano Reviglio and Rogers Alunge. 2020. "I am datafied because we are datafied": An Ubuntu perspective on (relational) privacy. *Philosophy & Technology* 33, 4 (2020), 595–612.

[99] Bruno Riccio, Chiara Brambilla, et al. 2010. *Transnational Migration: Cosmopolitanism and Dis-located Borders*. Vol. 7. Guaraldi Rimini, Italy.

[100] Yasaman Rohanifar, Sharifa Sultana, Shaid Hasan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2022. "Kabootar": Towards Informal, Trustworthy, and Community-Based FinTech for Marginalized Immigrants. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 1–32. doi:10.1145/3555109

[101] Chris Rumford. 2013. Introduction: Citizens and borderwork in Europe. In *Citizens and borderwork in contemporary Europe*. Routledge, London, UK, 1–12.

[102] Dina Sabie and Syed Ishtiaque Ahmed. 2019. Moving into a technology land: exploring the challenges for the refugees in Canada in accessing its computerized infrastructures. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS '19)*. Association for Computing Machinery, New York, NY, USA, 218–233. doi:10.1145/3314344.3332481

[103] Sharmin Sadequee. 2018. Surveillance, Secular Law, and the Reconstruction of Islam in the United States. *Surveillance & Society* 16, 4 (Dec. 2018), 473–487. doi:10.24908/ss.v16i4.6979

[104] Shruti Sannon and Andrea Forte. 2022. Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 1–33. doi:10.1145/3555556

[105] Charlie Savage and Ron Nixon. 2017. Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011. https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html

[106] Stanford Law School. 2009. Returning Home: How U.S. Government Practices Undermine Civil Rights at Our Nation's Doorstep. https://law.stanford.edu/publications/returning-home-how-u-s-government-practices-undermine-civil-rights-at-our-nations-doorstep/

[107] Adam Schwartz. 2017. Digital Privacy at the U.S. Border: Protecting the Data On Your Devices. https://www.eff.org/wp/digital-privacy-us-border-2017

[108] James C. Scott. 2020. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press.

[109] Tahseen Shams. 2018. Visibility as Resistance by Muslim Americans in a Surveillance and Security Atmosphere. *Sociological Forum* 33, 1 (2018), 73–94. doi:10.1111/socf.12401 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/socf.12401.

[110] Andrew Sheivachman. 2017. Muslim-American Travelers Are Quietly Having Global Entry Privileges Revoked. https://skift.com/2017/02/18/muslim-american-travelers-are-quietly-having-global-entry-privileges-revoked/

[111] Sarah Sherman-Stokes. 2024. Immigration Detention Abolition and the Violence of Digital Cages. *U. Colo. L. Rev.* 95 (2024), 219.

[112] Elisa Shoenberger. 2019. PayPal and Venmo's anti-terrorism regulations are causing headaches for average businesses. https://www.dailydot.com/debug/venmo-paypal-arabic-words/.

[113] Daniella Silva. 2019. GPS tracking of immigrants in ICE raids troubles advocates. https://www.nbcnews.com/news/us-news/gps-tracking-immigrants-ice-raids-troubles-advocates-n1042846.

[114] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, 409–423. doi:10.1109/SP.2018.00023

[115] Ranjit Singh and Steven Jackson. 2021. Seeing Like an Infrastructure: Low-resolution Citizens and the Aadhaar Identification Project. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 1–26. doi:10.1145/3476056

[116] Christophe Sohn. 2015. On borders' multiplicity: A perspective from assemblage theory. (2015).

[117] Peter Sproat. 2005. The social impact of counter terrorist finance policies in the UK. *Crime, Law and Social Change* 44 (2005), 441. https://heinonline.org/HOL/Page?handle=hein.journals/crmlsc44&id=441&div=&collection=

[118] Bethan Staton. 2016. The New Humanitarian | Eye spy: biometric aid system trials in Jordan. https://www.thenewhumanitarian.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan

[119] Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. 2021. Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 382 (oct 2021), 24 pages. doi:10.1145/3479526

[120] Elizabeth Stoycheff, Juan Liu, Kai Xu, and Kunto Wibowo. 2019. Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New media & society* 21, 3 (2019), 602–619.

[121] Syracuse University Transactional Records Access Clearinghouse. 2024. ICE Increases Use of GPS Monitoring for Immigrants in Alternatives to Detention (ATD). https://trac.syr.edu/whatsnew/email.240315.html.

[122] Julia Travers. 2017. NASA Scientist Detained at Border, Forced to Unlock Phone. https://www.ecowatch.com/nasa-sidd-bikkannavar-detained-2259068390.html

[123] Texas Tribue. 2018. "It's humiliating": Released immigrants describe life with ankle monitors. https://www.texastribune.org/2018/08/10/humiliating-released-immigrants-describe-life-ankle-monitors/.

[124] Texas Tribue. 2018. Released immigrant describes life with ankle monitor. https://www.youtube.com/watch?v=IsYB-rzXS8I&t=139s.

[125] Melissa Villa-Nicholas. 2023. *Data Borders: How Silicon Valley is Building an Industry Around Immigrants*. Univ of California Press, Oakland, CA.

[126] Harsha Walia. 2014. *Undoing border imperialism*. Vol. 6. Ak Press, Chico, CA.

[127] Harsha Walia. 2021. *Border and rule: Global migration, capitalism, and the rise of racist nationalism*. Haymarket Books, Chicago, IL.

[128] Illan Rua Wall, Freya Middleton, and Sahar Shah. 2021. *The critical legal pocketbook*. Counterpress.

[129] William Walters. 2015. Reflections on Migration and Governmentality. *movements. Journal for Critical Migration and Border Regime Studies* 1, 1 (May 2015). http://movements-journal.org/issues/01.grenzregime/04.walters--migration.governmentality.html

[130] Langdon Winner. 1980. Do Artifacts Have Politics? *Daedalus* 109, 1, (1980), 121–136. http://www.jstor.org/stable/20024652

[131] Marisol Wong-Villacres, Aakash Gautam, Wendy Roldan, Lucy Pei, Jessa Dickinson, Azra Ismail, Betsy DiSalvo, Neha Kumar, Tammy Clegg, Sheena Erete, Emily Roden, Nithya Sambasivan, and Jason Yip. 2020. From Needs to Strengths: Operationalizing an Assets-Based Design of Technology. In *Companion Publication of the 2020 Conference on Computer Supported Cooperative Work and Social Computing* (Virtual Event, USA) *(CSCW '20 Companion)*. Association for Computing Machinery, New York, NY, USA, 527–535. doi:10.1145/3406865.3418594

[132] Susan P Wyche and Rebecca E Grinter. 2012. " This is how we do it in my country" a study of computer-mediated family communication among kenyan migrants in the united states. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*. ACM New York, NY, USA, Seattle, United States, 87–96.