



Understanding experiences with compulsory immigration surveillance in the U.S.

Kentrell Owens
University of Washington
Seattle, Washington, USA
kentrell@cs.washington.edu

Yael Eiger
University of Washington
Seattle, Washington, USA
yeiger@cs.washington.edu

Basia Radka
University of Washington
Seattle, Washington, USA
basia@cs.washington.edu

Tadayoshi Kohno
University of Washington
Seattle, Washington, USA
yoshi@cs.washington.edu

Franziska Roesner
University of Washington
Seattle, Washington, USA
franzi@cs.washington.edu

Abstract

People attempting to immigrate to the U.S. (through a port of entry or other means) may be required to accept various forms of surveillance technologies after interacting with immigration officials. In March 2025, around 160,000 people in the U.S. were required to use a smartphone application—BI SmartLINK—that uses facial recognition, voice recognition, and location tracking; others were assigned an ankle monitor or a smartwatch. These compulsory surveillance technologies exist under Immigration and Customs Enforcement (ICE)’s Alternatives to Detention (ATD) program, a combination of surveillance technologies, home visits, and in-person meetings with ICE officials and third-party “case specialists.” For migrants in the U.S. who are already facing multiple other challenges, such as securing housing, work, or healthcare, the surveillance technologies administered under ATD introduce new challenges.

To understand the challenges facing migrants using BI SmartLINK under ATD, their questions about the app, and what role technologists might play (if any) in addressing these challenges, we conducted an interview study (n=9) with immigrant rights advocates. These advocates have collectively supported thousands of migrants over their careers and witnessed firsthand their struggles with surveillance tech under ATD. Among other things, our findings highlight how surveillance tech exacerbates the power imbalance between migrants and ICE officials (or their proxies), how these technologies (negatively) impact migrants, and how migrants and their advocates struggle to understand how the technologies that surveil them function. Our findings regarding the harms experienced by migrants lead us to believe that BI SmartLINK should not be used, and these harms fundamentally cannot be addressed by improvements to the app’s functionality or design. However, as this technology is currently deployed, we end by highlighting intervention opportunities for technologists to use our findings to make these high-stakes technologies less opaque for migrants and their advocates.

CCS Concepts

• **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → **Social aspects of security and privacy**; • **Social and professional topics** → **Governmental surveillance**.

ACM Reference Format:

Kentrell Owens, Yael Eiger, Basia Radka, Tadayoshi Kohno, and Franziska Roesner. 2025. Understanding experiences with compulsory immigration surveillance in the U.S.. In *The 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT ’25)*, June 23–26, 2025, Athens, Greece. ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/3715275.3732057>

1 Introduction

Many asylum-seekers (and migrants broadly) come to U.S. borders fleeing various forms of violence or catastrophe and have overcome enormous challenges [26]. Those who are able to gain entry into the U.S. may face additional challenges after they enter the country, including temporary detainment by Customs and Border Protection (CBP), language barriers, the inability to work legally,¹ and finding affordable housing [25]. Moreover, before being admitted to the country, they must surrender troves of personal data (e.g., through device searches and searches of social media accounts [48]), and, if they are permitted to enter, must accept several conditions—often including being surveilled by a smartphone app: BI SmartLINK.

BI SmartLINK was first launched in 2018 under Immigration and Customs Enforcement’s (ICE) Intensive Supervision Appearance Program (ISAP), which is the primary component of ICE’s Alternatives to Detention (ATD) program [30]. According to ICE, the goal of ATD is “to ensure compliance with release conditions and provide important case management services for non-detained noncitizens” [56]. Instead of being detained while their immigration case is pending or released with routine in-person check-ins, migrants are assigned some form of electronic monitoring. These options have expanded over the years to include ankle monitors, home phone voice verification, smart wristbands, and BI SmartLINK [38]. According to ICE data from March 2025, of the 183,884 people enrolled in ATD (with an average enrollment of 651 days), at least 159,959 people were being monitored by BI SmartLINK, with the remaining people being monitored by an ankle monitor (n=17,689), smart



This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

FAccT ’25, Athens, Greece

© 2025 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-1482-5/25/06

<https://doi.org/10.1145/3715275.3732057>

¹People who have a pending asylum case with the United States Citizenship and Immigration Services (USCIS) may apply for work authorization but only after 180 days [24].

wristband (n=4,634), VoiceID (i.e., phone-based voice verification; n=1,554), or no technology (n=6) [53].

Migrants required to use BI SmartLINK must conduct remote check-ins using facial verification and have their location tracked. When this app is installed on a personal phone, it has access to personal data (e.g., images, videos, phone number(s)), in addition to the already sensitive location and biometric data collected. There is a power imbalance between migrants and the entities that monitor them, particularly regarding access to information about BI SmartLINK's behavior. If a migrant cannot successfully complete a check-in, or if they violate the terms of their supervision because of a misunderstanding about how the app functions, it could lead to them being subjected to more stringent surveillance or being detained. As computer science researchers, we seek to understand migrants' experiences with this compulsory surveillance technology, what knowledge gaps or uncertainties they may have about how these technologies function, and what role, if any, we can play in this ecosystem to make immigration more just and equitable for them.

To this end, we ask the following research questions:

- RQ1:** *What are people's experiences under ICE's ATD program, particularly with using BI SmartLINK?*
- RQ2:** *What are people's questions about the functionality of BI SmartLINK?*
- RQ3:** *What are people's recommendations regarding BI SmartLINK for developers, researchers, and policymakers?*

To answer these questions, we conducted a semi-structured, qualitative interview study with immigrant rights advocates (n=9; see Section 3.6 for a discussion of sample size and recruiting) that currently support or have supported people monitored by BI SmartLINK. These advocates—some of whom have personal experience with the U.S. immigration system—have collectively supported thousands of migrants under ATD over their careers and can offer unique and valuable insight into migrants' experiences with the surveillance technologies they've been required to use. We asked them about their perceptions of the app, how people have described their experiences with the app, and the questions that they have heard from people that they have supported.

Our results highlight the power imbalance between the migrants and the people surveilling them, the negative impacts of the tech on migrants, and participants' questions about app functionality (arising from a lack of transparency regarding its behavior). Moreover, participants shared higher-level reflections about the pitfalls of viewing increased surveillance as a reform and provided recommendations across the ecosystem, from app developers to policymakers. Our findings regarding the harms experienced by migrants lead us to believe that BI SmartLINK should not be used, and these harms cannot be stopped by attempting to improve the app or its design. However, our findings point to potential intervention opportunities for technologists to address transparency around the functionality of BI SmartLINK to support migrants and inform future policy decisions regarding its deployment.

2 Background and Related Work

2.1 ATD, ISAP, BI SmartLINK, and critiques

ICE's Alternatives to Detention (ATD) program includes the Intensive Supervision Appearance Program (ISAP). ICE promotes ISAP as a method for reducing absconsion (i.e., fleeing or not attending) from immigration court hearings [56]. According to ICE data, 95% of people under electronic monitoring attended their final immigration hearings, compared to 83% of migrants generally (based on a research report on immigration cases between 2008 and 2018) [27, 54]. This data might suggest that electronic monitoring is an effective tool for preventing absconsion. However, the same report found that 96% of migrants who were represented by lawyers attended all immigration hearings, suggesting that a variety of factors are at play. Moreover, a 2022 report from the U.S. Government Accountability Office (GAO) indicated that ICE presents inaccurate, misleadingly-positive numbers regarding compliance rates and recommends that ICE develops better ways of assessing program performance and provide more oversight of its ATD contractor (BI, Inc.) [55].

Several immigrant rights organizations have previously investigated ICE's surveillance practices [12, 13, 34]. In April 2022 three organizations (Just Futures Law, Mijente Support Committee, and Community Justice Exchange) sued ICE for failing to comply with a September 2021 public records request regarding documents on ICE's use of BI SmartLINK [1, 2, 9]. After ICE was compelled to comply with their request, these organizations jointly published a report [34] disclosing their findings. Regarding accuracy of public information, they found that the documents contained information that contradicted claims made by ICE and its parent agency, the Department of Homeland Security (DHS). For example, DHS' Privacy Impact Assessment (PIA) [5], ICE's FAQ [56], and the "ISAP BI SmartLINK Agreement" obtained in the public records request all differ regarding when location data is collected from mobile devices. The report also highlights the role of BI (a government contractor) in making decisions about how migrants are surveilled and how BI is also contractually responsible for helping ICE manage negative publicity regarding ISAP and its usage of BI SmartLINK. Strikingly, the report exposes how ICE conducted a pilot study with BI SmartLINK in 2016, found that 56% of facial recognition check-ins failed, yet decided to continue promoting its usage. It should be noted that ICE currently claims that its facial recognition system has an accuracy of 98.5% and has undergone an independent evaluation [56]. Lastly, according to the report "in 2017, BI reported that the 'pass rate' for SmartLINK voice biometrics was 75% and that the factors that contribute to the low pass rate 'are not subject to improvement.'" In Section 5, we reflect on how the lack of public information and the contradictory nature of this information may increase confusion among migrants and their advocates.

2.2 Borders, technologists, and power

Mahmoudi's book "Migrants in the Digital Periphery" highlights the blurring line between borders and border subjects, as biometrics, surveillance, and datafication place the border upon the bodies of the subjects [37]. This foreshadows our findings in Section 4.1.2 that migrants who are not in ATD may not want to live or socialize

with those under ATD. In a way, those under ATD carry the border (and its corresponding harms) with them.

Work by Chelsea Barbaras highlights the potential for technologists to play an active role in resisting power abuses exacerbated by technology through “refusal as resistance” [17]. Due to the high demand for technical skills and the privileging of technical knowledge over other ways of knowing, technologists are in “a powerful position to negotiate and challenge the underlying theories of change associated with a given data project.” Barbaras outlines 3 common missteps that technologists take when investigating carceral technologies: “(1) ‘proving’ harm, (2) adopting deficiency narratives and (3) optimizing harmful systems.” The consequences of “optimizing harmful systems” also arise in Ben Green’s work [28], which discusses how technologists who intend to do social good often fall short, in part because they often (wrongly) assume that technology-centric gradual reform is the way to achieve social good. We describe our approach to ensuring that we avoid these common pitfalls in Section 5.3.

2.3 Related work

Guberek et al. conducted an interview study with undocumented people in the U.S. and asked them about their technology use, risk perceptions, and protective strategies [29]. While none of the participants described being monitored under ISAP (which had not yet been launched when the interviews were conducted in 2017), they described a general fear of surveillance and a perception that ICE was constantly monitoring their online activity, mirroring work study the security & privacy needs of refugees [51].

BI SmartLINK was one of several of electronic monitoring smartphone apps from a variety of domains (e.g., probation, parole, pre-trial release) studied by Owens et al. [43]. Based on Google Play reviews for the apps, people described the apps as invasive and said they frequently malfunctioned, consistent with our interview findings in this paper. Additionally, Austin Kocher wrote about how another app (CBP One) was imposed on migrants applying for asylum at the U.S.-Mexico border [36]. CBP One digitizes several forms required for entering the U.S. at a port of entry, tracks the location of migrants’ phone, and uses facial recognition for identity verification. Kocher argued that while this app is marketed as streamlining the administrative process of applying for asylum, it actually introduces digital barriers for asylum seekers, both in its proper function and as a result of “glitches.”²

3 Methods

3.1 Author positionality

We are five computer security & privacy researchers trained in qualitative methods, and we have all done research on the security & privacy needs of marginalized populations. Some of us have studied carceral surveillance inside prisons and after people are released from prisons, and its impact on those monitored and their families. Consequently, when we observe power imbalances that are exacerbated by technology, we tend to focus our efforts on understanding and mitigating harm or risks to those most vulnerable.

²Shortly after President Donald Trump was sworn into office on January 20, 2025, it was announced that CBP One would no longer be able to schedule appointments, and all existing future appointments were cancelled [10].

While one of us immigrated to the U.S. as a child and is now a naturalized citizen, none of us have ever been undocumented in the U.S. or had any interaction with Immigration and Customs Enforcement. Due to our lack of personal connection or experience with migrants the U.S. immigration system, there may be questions or context that we did not consider when designing our interview protocol. We also acknowledge that computer scientists often attempt to do work that they deem “social good” without adequately engaging with the social context in which relevant social issues arise or considering the negative impacts of their work. While we attempted to be thoughtful and thorough in this work’s framing, research questions, and methods, we acknowledge that this may still be insufficient.

3.2 Recruitment

To recruit participants we used a variety of methods. We directly contacted local and national immigrant rights organizations to schedule interviews with their staff; some organizations shared our study on national email lists for immigrant rights advocates. We reached out to universities’ immigration law clinics. We leveraged snowball sampling [46], allowing people we recruited to connect us with other potential participants. We also made study recruitment fliers and shared digital copies on social media and physical copies in-person at local non-profits.

All participants took a screening survey that asked demographic and contact information and verified that they met our inclusion criteria: that they were immigrant rights advocates who supported people monitored by BI SmartLINK. Four participants in our study were attorneys, and five were community organizers. Three participants were formerly undocumented, and another participant was formerly enrolled in ATD. A majority of participants (6/9) were women, and participants fell into three age ranges: 25-34 (1), 35-44 (7), and 55-64 (1). Several were bilingual in English and Spanish. Collectively they supported thousands of migrants over their careers.

3.3 Ethical considerations

We considered interviewing migrants currently or recently monitored by BI SmartLINK directly and decided that the potential risks to participants were significant. Multiple news reports indicate ICE has targeted migrants who publicly criticize its policies for expedited removal [3, 22, 33, 45]. Following guidance from Bellini et al. on conducting research with at-risk populations [19], we instead chose to interview *proxies*, namely, immigrant rights advocates that have supported numerous people monitored by BI SmartLINK. We sent a draft of our paper to participants to solicit their feedback.

Our study was deemed exempt by our institution’s human subjects research review board. We walked through an informed consent document with participants and answered any questions they had before beginning the interview. As the nature of the study might lead participants to mention identifying information about other people, we asked them to use pseudonyms for other people and removed any mentions of people from the interview transcripts.

3.4 Interview protocol

All interviews were conducted remotely (between July 2024 and January 2025) and audio-recorded (with participants' consent). We transcribed the interviews using an automated tool [42] that kept audio-recordings and their transcripts stored on our local machine. The interviews lasted an average of 48 minutes (not including the time spent reviewing the consent form), and we compensated participants with a \$35 USD VISA gift card that was mailed to them.

We began the interviews with rapport-building questions to help participants feel comfortable. We then prompted participants for any questions they have or the people they have supported have had regarding BI SmartLINK and informed them that we would prompt them again at the end of the interview. We then asked several specific questions about the people they have supported; for example, we asked participants, to best of their knowledge, how people start and stop using BI SmartLINK and how people use BI SmartLINK. We asked participants about what they have heard about people's experiences using BI SmartLINK and if they have concerns about people using the app. We closed the interviews by asking participants about feedback that they would give to the apps' developers and about their suggestions for what researchers should focus on. The full interview protocol is available in Appendix A.

3.5 Data analysis

Our qualitative analysis involved inductive and deductive coding. One researcher created an initial codebook based on the first three interviews. Two researchers then independently coded the fourth interview. Lastly, they discussed their coding of the fourth interview and the codebook until they reached consensus on themes and codes, creating several addition codes and consolidating others. The researchers separately coded the remaining interviews, iteratively discussing and updating the codebook as necessary. We include the full codebook in Appendix B.

3.6 Limitations

In Section 3.2 we outlined multiple recruiting techniques we employed; nevertheless, we struggled with recruitment. We leveraged personal contacts within immigrant rights organizations for recruitment. After six months of recruiting efforts, we had nine participants in our study. In three instances, participants suggested that we reach out to other people that we had already interviewed. When we asked participants what we could do to recruit more (such as increasing pay, reducing the duration of the interview, changing our messaging in the recruitment blurb), they shared that people might have concerns about the motivation for the work and concerns that the research would harm migrants. One participant mentioned how they signed up for the study initially but almost did not participate because they were worried that our research would be used to further entrench surveillance in the immigration system. Despite our low number of participants, we reached saturation for our interview protocol, as no new themes emerged in the last several interviews. The average sample size at ACM CHI (a top venue for human-computer interaction research) is 12, and 20% of papers had a sample size of 10 or less [23]. While we hoped to

recruit more participants, we are cognizant of avoiding the “threshold myth” [16]: that there is some fixed threshold for participants after which a study becomes valid.

We recruiting advocates to participate in our study instead of migrants. This decision may skew our results, as interviewing advocates is fundamentally different from interviewing migrants. We cannot expect our results to comprehensively capture the lived experiences of migrants under ATD. Relatedly, advocates goals (e.g., comprehensive reform of the U.S. immigration system) may not be identical to migrants' (e.g., avoiding imminent deportation), and this discrepancy may affect our results in ways that we are unable to perceive. That said, advocates' broad experience with a large and diverse set of migrants is uniquely valuable, particularly as we attempt to solicit questions.

4 Results

4.1 Experiences with ATD (RQ1)

While we began our study with intention of focusing on migrants' experiences with BI SmartLINK, we found that several of them used the app simultaneously or immediately after being required to use an ankle monitor. Consequently, in this section we describe migrants' experiences with surveillance technology broadly under ATD rather than only with BI SmartLINK. Where appropriate and relevant, we highlight the differences between people's experiences with the app versus ankle monitors.

4.1.1 (Abuses of) power imbalances. ICE officials and BI staff (referred to as “case specialists”) hold significant power over migrants, including controlling where they can travel, when they have to be at home, which technology is used to surveil them, and whether they are detained in a facility. Conversely, migrants, who are fighting removal proceedings from the U.S., often cannot legally work and experience multiple forms of precarity in their daily lives. This deep power imbalance was highlighted by participants in our study, particularly regarding abuse by officials, a lack of accountability for improper behavior, and the role of case specialists.

Our participants describe how migrants they supported experienced power abuses when interacting with their BI case specialists. These abuses of power included lying to migrants about how long they would be in ATD and the steps they would have to take to be removed from ATD (internally referred to by BI as “graduating” from ATD). P7 describes how case specialists have lied to migrants in the past:

I know they've lied. I know they've lied quite a bit. So at first, like with the ankle monitors, [migrants I've supported] were told, you know, you have to be on it for like, six months or a certain amount of period. And then ...they return at that ...six month mark. And then it's just like, an excuse, 'because of this or that we're not going to remove it.'

P3 similarly notes that “*your case manager might ... intimate like, you know, [if] you follow the rules, [if] you show up for your hearing, maybe like in six months we'll get you off. But like that's just their word. It's not like you have a piece of paper that you can hold you can hold on to.*” Additionally, migrants described how they were threatened by their case specialists with more technology-based

surveillance (e.g., getting an ankle monitor put back on after getting it removed) or detention. As P8 recalled: *“I’ve heard reports of just like ... really intense threats of, you know, ‘If you don’t do this’ ... if someone’s complaining about whatever technology they’re on, it’s like ‘well, if you don’t do this, we’ll take you back to jail, to ICE detention.”*

Additionally, participants described the apparent lack of accountability of ICE and BI officials for bad or negligent behavior. ICE’s website states that its best practice is “to perform compliance reviews every 30 days a participant is enrolled in the ATD ISAP program” to ensure that migrants have “the most appropriate form of case management and supervision” [56]; according to participants in our study, this is not reflected in practice. As P5 states: *“It says that their recommended best practice is to review the case of each person on ISAP every 30 days to make a determination case by case using all the factors about whether they merit being graduated out of the program, terminated from the program. But that doesn’t shed much light into what actually happens.”* Migrants may wait for months or years before being unenrolled from ATD either through advocacy by community organization or self-advocacy: *“there’s also like clearly a lack of administrative ... review processes to really evaluate what level of surveillance an individual should experience. Like it really seems like it’s just template all of the [same] things for everybody ... until you complain enough and you come off of certain parts of that surveillance cocktail”* (P7). P8 shared a theory regarding why these reviews and de-escalation of surveillance do not happen as frequently as they should: *“For the people that are compliant, it’s pretty rare to see ICE affirmatively following its own policies and affirmatively taking people off of this tech. And I think that there’s probably some incentives for ICE to keep people on this technology.”*

In a structural sense, ICE and DHS displayed a lack of accountability by failing to release a Privacy Impact Assessment (PIA) for ATD (as required by Section 208 of the E-Government Act [4]) until April 2023—almost two decades after the program started in 2004. This is something that advocates have requested for years, but only got recently, and it is unclear if there were any consequences for such a delay. As P3 points out *“you know that the privacy impact assessment for this program; they operated it for like close to 20 years without one.”*

ICE claims that it provides “case management” for migrants, but participants pointed out how different what BI case specialists actually do is from case management. According to ICE, a goal of ATD is to “provide important case management services for non-detained noncitizens” [56], which implies that case specialists (sometimes referred to as case managers) administer these services. Participants described how case specialists are more akin to a parole or probation officer than a case manager; for example, P8 stated:

I think that the case manager term is something that’s been brought over from social work and is seems to me deliberately confusing or ambiguous ... These are not social service agencies. This is a for-profit, carceral corporation and its primary function is to surveil and coerce the people that are under its control. I think that most of the interactions with these case managers is more like something that I imagine is

akin to interfacing with a probation officer. They’re not there to help you, they’re there to make sure that you’re doing what you’re told to do.

ICE says that case specialists offer community referrals for different resources (e.g., food, housing, health) to migrants [56], but P3 says *“The reality is they give people like a piece of paper that says like ‘call this number for a food pantry.’ That’s not case management.”*

Migrants’ relationship with their case specialist can be complicated, as it can feel like (perhaps accurately) their freedom from detention or unenrollment from ATD may depend more on their relationship with their case specialist rather than their own actions. Their case specialist can recommend to ICE that they be unenrolled from ATD, but they can also recommend detention. As P7 noted, it can be challenging for migrants to manage this type of relationship: *But a lot of the time it’s a really difficult relationship to navigate in which there are all these really weird power dynamics. And there’s a lot of like having to appease your case manager and like keep [them] happy. And there are a lot of, there’s a lot of verbal abuse and a lot of threats that happen between those interactions.*

4.1.2 (Negative) Impacts on people. Participants described how both technical (e.g., BI SmartLINK or an ankle monitor) and non-technical (e.g., home visits) aspects of being enrolled in ATD impacted migrants’ lives.

The requirements of an ATD program can cost migrants their jobs. Participants described how the demands of remote BI SmartLINK check-ins have led to migrants losing employment. P7 explained that:

There’s also been a lot of loss of employment as a result of SmartLINK because if they ask you to take a picture on a Tuesday at two o’clock and you’re in an assembly line at a factory, you can’t just leave. So a lot of [my clients] have lost jobs because they don’t have the kind of employment where they can excuse themselves to go take a picture in the bathroom for 10 minutes. One [person] lost three jobs as a result of it.

P7 described the impacts of having mandatory home visits that are not at a specific time on a given day, requiring migrants to stay home waiting for the case specialist to visit:

So a lot of people are losing, that’s five days a month of employment for these surveillance requirements when they also have SmartLINK or when they also have an ankle monitor. So they have the GPS capability, but they’re also being forced to stay home and lose an entire day’s worth of work.

Being monitored puts others in harms way, leading to housing difficulties and alienation. Participants noted that their clients often struggled to find housing, as surveillance of themselves would mean the surveillance of those with whom they lived. P1 described how one of their clients lost housing because the other (undocumented) housemates were *“very worried that ICE would come to the door.”* P7 also described this, by explaining:

I know that with the ankle monitor, it has been hard for some people to have a place to stay, especially

if they're staying with non-asylum seeking undocumented families. The idea of bringing something that's connected to immigration that has GPS feels scary and harmful.

Beyond housing, P5 described the general alienation clients experienced because they were *"avoiding gathering with any friends or family because they didn't want to endanger their loved ones by putting a target on their back so to speak."* These housing challenges reflect Mahmoudi's observation that for migrants, surveillance "practices of digital bordering go beyond material borders and seep into the realm of the everyday" [37]. Because BI SmartLINK's surveillance practices is not dissimilar from those that happen at borders, in a sense, by using the app migrants *carry the border with them* and separate themselves from loved ones to protect them.

Being monitored impacts migrants' mental and physical health. Participants described how the instability, fear, pressure, and stress while being monitored harmed their clients' mental health. P1 said that their clients live in a *"great deal of just kind of constant anxiety that they're gonna get redetained or that they're gonna get deported."*

P7 said that *"I think there's always the looming threat of if you don't comply then we will physically detain you ... I've heard of someone having a panic attack and being forced into an ankle monitor. That doesn't sound like consent to me."*

P6 connected this fear and stress to the lack of transparency about what data is actually being collected by the technology. They describe how their clients *"feel monitored all the time. The fact that they don't know exactly what the data is used for is very scary."* But the pain is not just psychological, it can also be physical. P7 explained how their client *"developed really horrific medical symptoms, like both psychological and physical as a result of the ankle monitor."*

Migrant might also experience stress as a result of officials' mistakes and misleading advice. On an individual level, ICE officers and case specialists sometimes are required to manually input information about migrants, such as their address. When this information is entered incorrectly and an alert is triggered (e.g., from being in a location that is not known to be one's home after a curfew), migrants are the ones who are under stress and penalized, not the government or its contractors. Regarding location P1 said: *"I've heard of instances where like the data gets entered kind of wrong somewhere. So like, ... they're being told that they're out of their region and they're not."*

Given that ICE and BI administer ATD, migrants might expect that they have fairly accurate information regarding the immigration process and legal proceedings. However, some participants described how migrant sometimes get bad or false legal advice. P2 said, *"ICE will tell them a lot of things that are not true ... they don't know what they're talking about. So they'll give them legal advice ... They are, yeah, not to be trusted."*

Being monitored may impact access to healthcare. Not only does being monitored negatively impact migrants' mental and physical health, but it may also impact their ability to get healthcare. P1 explained that *"you know I also really worry about [them] getting health care like if you have a sick kid and you need to get them to the hospital and it's not in your 100 mile radius or it's after your curfew. I*

really worry that people might not be inclined to seek out emergency care."

Passports are confiscated. Participants described how migrants' passports are used as a bargaining chip. Supposedly, if a migrant turns in their passport, they are unenrolled from ATD or have an ankle monitor removed (while still being required to use BI SmartLINK). However, as P7 articulated, *"They'll confiscate them forever. And sometimes they'll take the ankle monitor off. Sometimes they don't. And then they also leverage it as a threat. 'If you don't bring me your passport from your home country, I will then have to put an ankle monitor on you.'" This threat is arguably as harmful as the technology itself, as P7 concludes: How harmful is this technology, but also how harmful is just the threat of this technology?"* P8 explained how this was likely desirable for immigration officials because it makes for an easier deportation. Unfortunately, passports may also be migrants' sole valid form of ID: *"For ICE to have a valid passport for someone is from their perspective like one step closer to being able to like actually remove someone ... [and if] they're undocumented, for example, North Carolina passed a law a while ago where you can't use other forms of ID. Your foreign passport is your only legally valid form of ID for school registration, notarizing documents, stuff like that."*

Monitoring opens migrants up to other surveillance. Participants described how BI SmartLINK changes migrants' typical privacy behaviors, because they have to allow for the monitoring. P5 explained how their clients were forced to keep location services turned on at all times:

Well, I've heard that people have not been able to switch off their location settings ... I've heard at least one person say that when they tried to disable the location services on their device ... they were contacted by BI and, you know, told they needed to stay on location services at all times.

The monitoring technologies have usability problems with significant consequences. Participants described problems with BI SmartLINK's facial recognition software used to confirm the identity of a migrant during a remote check-in. P1 explained that it was common: *"When they try to do the selfies for the facial recognition ... the phone doesn't accept them."* P8 also described how *"the facial recognition technology has been reported to be worse and less accurate in terms of recognizing folks of darker skin tones."*

Participants also mentioned frequent hardware problems with the ankle monitors. P5 described how *"They were running into all kinds of battery failures with their ankle monitors, because they had the interval for location tracking set to continuous, and that would constantly ping the device and drain the battery and their batteries were crappy."*

Having to use BI SmartLINK can create problems for many migrants who are low literacy or speak languages not supported by the app. P8 described how *"It doesn't support more than three or four languages, I think. It doesn't, of course, account for people that have limited literacy or no literacy."*

Another purported function of the app is to remind migrants of upcoming appointments and court dates, but participants described how siloed, and often wrong, this data is. P1 explained that:

The app doesn't tell you about your [immigration] hearing dates and so ... as a migrant you think you're [good] checking in on the app. You're going to your [in-person] reporting requirements ... But then the actual immigration court hearing dates that are the most important dates of all, they don't tell you. And they change all the time.

Altogether, these problems cause great stress. These usability problems carry tremendous weight because technology failure can lead to the detention of a migrant who is accused of not being available or present for a check-in. P1 summarized this by describing:

I've worked with clients who are having to ... leave a meeting, an important meeting with me, because they got to go deal with the check-in and then it doesn't work and then they're freaked out because they think they're about to get arrested. And I mean it's ... like all the time, you know, you're worried about this stupid app.

4.1.3 ATD's promises fall short in practice. Participants described how their perspectives regarding the potential positive impacts of ATD have changed over time.

Advocates originally supported ATD because they thought it would genuinely be an alternative to detention. P3 explains:

We all kind of bought into it too right. Like if you look at some of my organizations and other organizations in the early 2000's, we supported the ATD program. We wanted funding for the ATD program. We really thought it would be the way to get rid of detention but now ... it's become pretty apparent that like we kind of have to start from scratch.

ATD is not a real alternative. Despite initial optimism, participants now believe that the Alternatives to Detention program is not a true alternative to detention, but rather "*digital detention*" (P6).

In addition to possibly being "*put back in detention anytime*", P6 also explained how the expectation of ATD replacing detention or being the precursor to freedom is misleading. They describe:

Again, a lot of people think that it's a trajectory [where] you go from physical detention to ankle bracelets to phone app, and then [no detention] ... [T]he actual trajectory is that you go to the court. This is all for making sure that you comply with court orders to appear, and then you're able to be deported. But I think the way that it's talked about, it's called alternatives to detention, they'll often say that it's a way to keep the community with the community. It's just being kind of like, oh, it's a humanitarian solution. But there's I think lots of intentional misinformation about how it ends for people.

This sentiment echoes work by Sarah Sherman-Stokes: rather than being a real "alternative to detention," surveillance technologies administered by ATD create "[d]igital cages, masquerading as a more palatable version of enforcement and surveillance, [which] create devastating harms that are hidden in plain sight, while duping us into thinking of these measures as more humane" [50].

P9 described how the technology is "*a way to control and contain and in some ways I think SmartLINK ... I do think it's a way to kill people*," particularly because the technology can facilitate and increase the efficiency of deportation, which means many migrants will be forced to return to the violence that they fled.

ATD has expanded beyond its stated goals. Participants described how ATD has become the default for all migrants and not only those who meet certain restrictions. P3 describes the expansion of the program: "*The numbers that we see now for the ATD program are huge compared to what it used to be in the early 2000s. The clients that I saw that had it, it was not the norm across all of them.*" They additionally report that, unlike today when being released from physical detention likely results in electronic monitoring, "*when I was practicing 10 years ago, it was not unusual for somebody to be released from government custody without any restrictions.*" P6 also describes the expansion of ATD, particularly during COVID. They explain:

During COVID, ATD went up, especially because we shut down three of the four detention centers in [my state]. And especially during COVID, the ATD numbers went up like 274%. And my sense has been that ATD has brought more women under surveillance, that has been one of the big outcomes.

Although ATD's stated purpose is about increasing compliance for court requirements, participants felt that this is no longer — or was never — the case in practice. P1 expressed that:

It's not actually about making sure that people appear for all their hearings because in the vast majority of cases they have [ankle monitors and other technology] taken off at some point before their final hearing ... [which is the] period when you'd want to make sure that they're actually going to come to their hearing and that if they get ordered deported that they're locatable and all of that. But that's not the way it works.

P8 also described how, if compliance was truly the purpose of the program, there are much more effective, less harmful, solutions. They explain:

There are studies that document that providing legal representation to people is at least if not more effective in making sure that they comply with going to every court day and complying with the law. There are other alternatives looking at community-based case management programs with actual social service agencies that would help stabilize folks who have recently arrived or who are coming out of [detention] providing actual resources. Those are the things that help people do what they have to do under the law.

ATD actually hurts compliance. Despite the stated goals of increasing compliance, participants described how the current ATD conditions actually work against this goal. P3 described how: "*people just get fed up and they cut off the ankle monitor or they get rid of the app because it's so onerous*". P9 described how following the rules is an undesirable path because it opens you up to further tracking, surveillance, and subjugation. They explained that "*The more you*

do that stuff, the more they're getting information on you ... but that's also the route toward securing asylum. So it's this very tricky thing because on the one hand you want to follow the ISAP rules because ... you're trying to just be perfect."

They further explained how the trauma and violence experienced in detention after a legal border crossing encourages a self-preservation instinct to cross illegally and avoid experiencing that harms of further surveillance. P9 describes:

You know people tend to think about undocumented people and they tend to think about crossing the border and the dangers of the desert and all that. Going through a legal route to request asylum at a port of entry, doing everything right, unfortunately is more life-threatening, I think ... I've never met anyone actually who's gone through the detention experience of the border without experiencing some form of torture. Either through being put into what they call an 'ice box' which is a very cold room like 50 degrees or ... having ... very bright lights on all the time, 24/7. Not being given access to medical care ... physically assaulted, sexually assaulted ... Being separated from their children or spouses is common, being humiliated is common by the guards. And then when people are released they're released with a tracking device, well now they know where you are. And if you're undocumented and you cross the border [secretely] ... they don't know where you are.

While this sentiment from P9 describes how people experience psychological and physical torture [14] while in ICE detention, scholars have outlined how carceral surveillance technologies (including electronic monitoring apps like BI SmartLINK) extend psychological torture outside of carceral spaces into other places, such as migrants' homes. [39, 47, 52].

DHS is moving towards a future where no one is unmonitored. Participants predicted that this surveillance will likely grow to surveil *everyone* who comes through government custody. P7 expressed that: *"I think that these types of technologies will probably just increase over time and I'm really concerned about where we're heading."* P3 likewise stated: *"DHS ... is working towards a place where nobody is released without any sort, like everyone released from government custody is going to be subject to some level of supervision."*

4.2 Questions about BI SmartLINK (RQ2)

We explicitly asked participants if they had any questions or areas where they would like clarification regarding BI SmartLINK and its behavior or functionality. These questions or knowledge gaps regarding BI SmartLINK have an impact on migrants' lived experiences when interacting with this technology. The below results highlight potential opportunities for researchers to technically investigate the answers to these questions and offer increased transparency for migrants and their advocates.

The most prevalent question, raised by every participant, was about the nature of location tracking: *"I am obsessed with figuring out the extent to which the Smart Link app can continuously track the geolocation of individuals"* (P5). On ICE's FAQ page for

ATD [56], it states that *"BI SmartLINK® is not capable of persistent tracking when loaded on a participant provided device,"* and that while it is possible on BI-provided phones, ICE does not use this capability. Participants were aware that ICE says that it only tracks migrants' location while they are actively using the app. However, based on anecdotal experiences and news exposés, participants questioned if this was true. P3 said: *ICE says that they only track someone's location when the app is being used but ... I keep hearing from individuals who ... they've received phone calls from their case manager from the ICE officer in charge of their case asking them like, why they were at a place, at a certain place. And clearly the only way they could have figured that out is that they were tracking ... them on their phone.*

Participants also asked questions about BI SmartLINK's behavior regarding data collection, sharing, use, retention, and storage. A prevalent question was about the app's ability to collect other, non-location information from a migrant's smartphone such as their contacts, stored photos, or activity on other apps. Participants were unsure about the potential scope of data collection and wanted to understand what was possible. For example, P4 asked *"what is the data being collected from your ability to track me and ... what are you accessing on my phone that I'm not aware of?"* Participants' questions regarding data sharing & use highlighted concerns about data being shared outside of ICE and that data being used to detain not only people monitored by BI SmartLINK but others around them.

I think that there's reasons to be concerned about what ICE would do with that data, not just under [the Biden] administration, but under especially a more overtly hostile anti-immigrant administration. I would not be surprised to see similar kinds of raids to what occurred in 2019 in Mississippi.³ I mean, Trump is promising mass deportations and this data would help ICE in a very granular way locate not just these people, but of course these folks are embedded in communities with lots of other immigrants, lots of other mixed status families. And so it would bring ICE to their doors pretty quickly. So, yeah, what is ICE doing with the data? (P8)

Some other questions were about where collected data was being stored, how long it was retained after someone is unenrolled from ATD, and whether their data was shared with third-parties and private companies. These questions highlight participants' concern about "function creep" [21]—when data originally collected for one purpose is used for another—and the ways that data collected about them might be used to harm migrants and those around them.

Participants also raised non-technical questions on topics beyond the app's behavior. They asked about the legality of passports being collected in exchange for changing the technology used to monitor migrants (Section 4.1.2) and the legal limits of BI SmartLINK's data collection practices. There were several questions regarding ICE's administrative decisions or policies, or why certain people have multiple surveillance mechanisms (e.g., ankle monitor and BI

³ICE conducted the largest workplace immigration raid ever in a single state. Seven food plants were raided, and 680 people were arrested. Unsealed court documents revealed these locations were chosen, in part, based on ankle monitor location data [32, 49].

SmartLINK) on them at once. One participant wanted to understand the prevalence and frequency of home visits under ATD. Another participant wanted to understand why some people use BI-provided phones and why others do not.

The answers to these questions have important implications for migrants' safety and human rights. If migrants believe they are not being tracked when they are, they may increase risk to other migrants with whom they interact (e.g., by going to a previously-unknown gathering place). Moreover, depending on which data are collected, BI SmartLINK could be violating migrants' privacy rights. Although courts in the U.S. have found that certain classes of undocumented immigrants can be denied Fourth Amendment rights (i.e., against unreasonable search and seizure) [41], courts in the EU have found attempts to exclude undocumented immigrants from the General Data Protection Regulation (GDPR) [11] to be unlawful.

4.3 Recommendations from immigration rights advocates (RQ3)

In our interviews, participants provided recommendations for developers, researchers, and policymakers, regarding how to improve the state of ATD technology use.

4.3.1 Recommendations for developers. When we asked our participants if they have any feedback for the developers of the app, every participant said a variant of what P6 succinctly recommended: “destroy it”. P4 asked, “can you just get rid of it?”. P7 expressed that “these apps are a form of social control and they should not exist”. P2 noted how “there’s all these super like talented, smart people that again use their skills for evil”, and P8 said:

Just don’t [make it]. Yeah, I don’t want this technology to exist. I don’t think that it’s necessary. I don’t think that it’s helpful. I think that it is used to extend ICE’s reach into people’s lives, into the lives of immigrant communities and to put a gentler face on government surveillance and control of people.

P6 expanded on how the original use case for the technology informs its use today:

I don’t think people need to be tracked. As far as I know, the app, BI actually developed it as to like track the movement of cattle first.⁴ And in some ways that says it all ... you know, [the United States is] a place built on people’s enslavement, enslaved labor and theft and genocide. So it’s the same thing. It’s like people just ... track cattle. Are you using it to track migrants? What does this say?

Short of abolishing the app and the technology, P3 suggested that the app should at the very least improve clarity about their data collection practices (“more transparency over the geo-monitoring and what they can listen in on”) in addition to adding a support line for technical problems: “the app needs to have a better technical

⁴According to a 2022 press release, BI’s “founders used Radio Frequency (RF) technology to create a feed management system for dairy farmers to increase milk production ... In 1977, Judge Jack Love of Albuquerque, New Mexico, read a comic book about a villain that used an EM device to track Spider-Man ... in 1982 he worked with National Incarceration Monitor and Control Services (NIMCOS) to develop an EM prototype. BI acquired NIMCOS in 1984, and the EM industry was born.”

assistance line because people end up having like nightmares that they’re about to be hauled off into immigration detention jail because they can’t upload [photos to] their phone and there’s no like 800 number you can call to quickly get assistance with technical issues.”

4.3.2 Recommendations for researchers. Participants recommended that researchers focus attention on projects for social good. P2 encouraged researchers to “support things like mutual aid, collective action, you know, organizing, in general”, P1 explained that “we need some real studies of what the mental health impacts are of this kind of monitoring because I think they’re real”, and P2 & P7 recommended researchers study how carceral technologies function and extend surveillance: “[Researchers should study] the way these technologies function and ... the way the government or private companies are using them to increase surveillance” (P2) and “... these technologies are incredibly harmful and it just seems like the advocates who are exposed to it the most also don’t have the time or necessarily the expertise to figure out how to support the, like the fight against surveillance. So it’s like, it’s an issue that just like a handful of people end up really spending time on” (P7).

4.3.3 Recommendations for policymakers. The recommendations for policymakers echo those for developers. P1 expressed “I don’t think we should be using it at all”, and P4 explains how “One, I don’t think anybody should be placed on any kind of surveillance or monitoring. Two, I just, there’s no reason for it. It’s, you know, even the rates of like, what they call absconders who, you know, abandon the app and just, you know, go freely, it’s so low”. If these policies do continue, participants mentioned reforms like standard timelines for reviewing cases: “that’s one of the key problems with the program now and that is why I believe strongly that the program should have designated benchmarks in which people’s cases ... they know their case will be reviewed.” and furthermore, to reduce high caseloads by lowering the number of people on ATD as opposed to hiring more ICE officers: “I think it’s like one officer for every like 600 cases.⁵ They’re not doing the regular reviews now, I personally don’t think the solution is they should hire more ICE officers. The solution should be ... much more limited in who you desire to enroll in this level of supervision instead of just giving it to anybody because they are standing in front of you.” (P3). P1 echos this sentiment, the ATD should only be applied to the most serious of cases, and not be default: “if we are going to use it only in truly serious cases where there is an actual flight risk where the person will really be otherwise detained, then I’d be willing.”

5 Discussion

5.1 Opacity by design

Migrants enrolled in ATD lack transparency into multiple aspects of their surveillance, including how long they’ll be monitored, why they received a specific technology assignment, how they can ‘deescalate’ their monitoring to a different option, how they can be unenrolled from ATD, what the thresholds are for behavior that could result in detainment, and the technical behavior of the technology that monitors them. This opacity, combined with the discretion given to BI employees, facilitates perpetual stress and insecurity regarding migrants’ futures and freedom, independent

⁵According to ICE’s website, the caseload is 1:125 [56].

of the already stressful nature of their pending immigration removal proceedings. Unfortunately, this lack of transparency does not seem to be the type that can be resolved by better user education (as academic researchers often call for). As we discuss in Section 2, ICE's internal documents and public statements regarding their practices or how technology functions are contradictory. It is hard for migrants under ATD to make informed decision regarding their behavior while being surveilled when there is not a stable ground truth to inform these decisions.

5.2 Electronic monitoring of migrants

Like others under electronic monitoring, migrants bear the mental toll of surveillance and how it “transforms the most private spheres of life—our bodies, homes and families—into highly regulated carceral spaces” [31]. Migrants exist in a precarious situation in which their ability to live, work, and experience community is restricted before they are even coerced to use technologies like BI SmartLINK. For migrants who continue to be forced to use BI SmartLINK despite complying with everything they are told they need to do to be removed from ATD, it can feel like the surveillance itself is a form of punishment [57].

It is important to acknowledge that while the risks (or the threat model [7]) for migrants is similar to U.S. citizens under electronic monitoring [15, 43, 57], they are distinct in important ways. For example, if someone under electronic monitoring (e.g., via a smart-phone app [43]) as a condition of pre-trial release [40] violates a condition of their release (as determined by the app), they might be put in jail/detention, similar to a migrant. And like a migrant, the person on pre-trial release has a pending legal case (in this example it is a criminal case instead of a civil immigration one), the outcome of which they will still be subject to, *even if they use the surveillance app perfectly*. One difference arises when the legal proceedings are resolved. The citizen on pre-trial release will, at worst, be incarcerated. The migrant is at risk of *deportation*. Moreover, the app that the migrant used (“perfectly” in this example) may be used to facilitate their own detention and deportation. Lastly, BI SmartLINK introduces risks (namely detention and deportation) to other migrants that may be around the person monitored in ways that the pre-trial release electronic monitoring app does not. While efforts to challenge the use of carceral technologies in these different contexts are related (e.g., BI SmartLINK is advertised as a general electronic monitoring tool for a variety of domains [6]), the use of technologies like BI SmartLINK distinctly exacerbate the marginalization of migrants.

5.3 The role of technologists

Barbaras [17] outlines common mistakes that technologists make when investigating carceral technologies: “(1) ‘proving’ harm, (2) adopting deficiency narratives and (3) optimizing harmful systems.” In our work, we attempt to avoid these mistakes. We do not try to quantitatively prove harm but rather engage with advocates who understand and can relay the minutiae of harms based on their vast experience supporting migrants. Rather than focusing on the shortcomings of migrants and helping them cope, we focus on the existing power imbalance in the U.S. immigration system and how technology exacerbates it.

Researchers may be tempted to assume the failures of BI SmartLINK and technologies like it are questions of implementation, and that its problems are “resolvable through changes to input data and deployment” [35]. We do not aim to improve the functionality, performance, or even privacy within BI SmartLINK. In line with prior work that considers the ethics of conducting usability testing on tools for oppressing undocumented people [18], rather than seeking to improve the functionality or efficiency of BI SmartLINK, we focused on understanding the questions of people monitored by the app with the goal of eventually increasing transparency around its behavior. We have determined that the app can cause harm and seek to promote opportunities for technologists to help migrants and their advocates that are not “reformist reforms” [28] that “limit their objectives to the maintenance and practicality of the current system” [44].

5.4 The limits of reports

In its July 2022 report on ATD [55], the Government Accountability Office (GAO) called for more oversight of BI by ICE and for developing mechanisms to ensure that it is meeting the demands laid out in its contract. Other recommendations included things like improving the accuracy of its data, improving metrics for tracking if ATD is successful at achieving its stated goals, and ensuring that reviews of migrants' cases (also known as “supervision reviews”) are happening at the appropriate cadence (i.e., 30 days as opposed to six months as some ICE officers they interviewed stated). Almost three years later, only one of its ten recommendations has been addressed, and it was that migrants be given access to “legal orientation presentation [55].” This report reveals that the U.S. government is aware of some of the problems with ATD highlighted in our study (e.g., the frequency of supervision reviews), has published its own reports on these problems, and seems to be largely inactive in working towards resolving them.

When we researchers think about the impact of this work and what we hope it will do, we are soberly aware that yet another “report” may not move the needle towards a more just, equitable, and less surveillance-driven immigration system. We hope that our work can inform the FAccT community about the experiences of those surveilled under ATD and those who advocate for them. By interviewing advocates and soliciting their questions, we aim to lay a foundation for future critical analysis of compulsory immigration surveillance technologies that attempts to answer their questions.

6 Conclusion

Although technology is only one component of the larger system of surveillance and control in the U.S. immigration system, our work shows how it can exacerbate already challenging circumstances for migrants. Justice and safety for migrants, particularly asylum-seekers, will become more precarious as immigration policy in the U.S. is expected to become more hostile towards migrants [20]. Participants in our study called for researchers to study how technologies function and how institutions are wielding them for increased surveillance. We embrace this call and hope that this work serves as a synecdoche [8] for the FAccT community and the computer science research community more broadly.

Acknowledgments

We thank our participants for their time and valuable insights. We thank our anonymous reviewers for their informative and instructive reviews. We thank UW Security and Privacy Research Lab members Rachel Hong and Christina Yeung for feedback on an earlier draft of this paper.

References

- [1] UC Berkeley Law 2024. *Community Justice Exchange et al v. U.S. Immigration and Customs Enforcement et al*. UC Berkeley Law. <https://www.law.berkeley.edu/case-project/alternative-detention-programs-foia/>
- [2] 2022. COMMUNITY JUSTICE EXCHANGE, JUST FUTURES LAW, MIJENTE SUPPORT COMMITTEE v. U.S. IMMIGRATION & CUSTOMS ENFORCEMENT and U.S. DEPARTMENT OF HOMELAND SECURITY. https://www.law.berkeley.edu/wp-content/uploads/2022/04/22cv2328_ECF1_Complaint.pdf
- [3] NYCLU - ACLU of New York [n.d.]. *NYCLU, ACLU Challenge Ravi Ragbir Arrest, Cite ICE Targeting of Activists*. NYCLU - ACLU of New York. <https://www.nyclu.org/press-release/nyclu-aclu-challenge-ravi-ragbir-arrest-cite-ice-targeting-activists>
- [4] U.S. Department of Justice 2014. *Office of Privacy and Civil Liberties | E-Government Act of 2002*. U.S. Department of Justice. <https://www.justice.gov/opcl/e-government-act-2002>
- [5] 2023. Privacy Impact Assessment for the Alternatives to Detention (ATD) Program. <https://www.dhs.gov/sites/default/files/2023-08/privacy-pia-ice062-atd-august2023.pdf>
- [6] BI Incorporated [n.d.]. *Smartphone Monitoring*. BI Incorporated. <https://bi.com/mobile-monitoring/>
- [7] Electronic Frontier Foundation 2015. *Surveillance Self Defense: Threat Modeling*. Electronic Frontier Foundation. <https://www.eff.org/document/surveillance-self-defense-threat-modeling>
- [8] Rediet Abebe, Solon Barocas, Ron Kleinberg, Karen Levy, Manish Raghavan, and David G. Robinson. 2020. *Jobs for Computing in Social Change*. (2020). doi:10.1145/3351095.3372871 arXiv:1912.04883
- [9] Jasmine Aguilera. 2022. *Privacy Advocates Sue Over Immigrant Tracking Program*. TIME. <https://time.com/6167467/immigrant-tracking-ice-technology-data/>
- [10] Hamed Aleaziz and Paulina Villegas. 2025. *Trump Shuts Down CBP One App, Signaling the Start of His Immigration Crackdown*. (2025). <https://www.nytimes.com/2025/01/20/us/politics/trump-shuts-down-migrant-entry-app-cbp-one.html>
- [11] Sara Alsharif. 2024. *Government Does the Bare Minimum to Update the Immigration Exemption*. Open Rights Group. <https://www.openrightsgroup.org/blog/government-does-the-bare-minimum-on-the-immigration-exemption/>
- [12] Aly Panjwani and Hannah Lucal. 2022. *Tracked & Trapped: Experiences from ICE Digital Prisons*. https://notechforice.com/wp-content/uploads/2022/05/TrackedTrapped_final.pdf
- [13] Aly Panjwani and Julie Mao. 2021. *ICE Digital Prisons: The Expansion of Mass Surveillance as ICE's Alternative to Detention*. <https://web.archive.org/web/20240415162858/https://www.flipsnack.com/justfutures/ice-digital-prisons-1u8w3fndtj/full-view.html>
- [14] Andrew Hursh. 2020. *UN Rights Expert Defines 'Psychological Torture' in New Report*. JURISTnews. <https://www.jurist.org/news/2020/02/un-rights-expert-defines-psychological-torture-in-new-report/>
- [15] Chaz Arnett. 2019. *From Decarceration to E-carceration*. *Cardozo L. Rev.* 41 (2019), 641.
- [16] Peter Bacchetti. 2010. *Current Sample Size Conventions: Flaws, Harms, and Alternatives*. 8, 1 (2010), 1–7. Issue 1. doi:10.1186/1741-7015-8-17
- [17] Chelsea Barabas. 2022. *Refusal in Data Ethics: Re-Imagining the Code Beneath the Code of Computation in the Carceral State*. 8, 2 (2022), 35–57. Issue 2. doi:10.17351/ests2022.1233
- [18] Joseph Bartolotta. 2019. *Usability Testing for Oppression*. 7, 3 (2019), 16–29. doi:10.1145/3321388.3321390
- [19] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L. Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2024. *SoK: Safer Digital-Safety Research Involving At-Risk Users*. In *2024 IEEE Symposium on Security and Privacy (SP)*. 635–654. doi:10.1109/SP54263.2024.00071
- [20] Betsy Woodruff Swan and Myah Ward. 2024. *Trump's Immigration Crackdown Is Expected to Start on Day 1*. POLITICO. <https://www.politico.com/news/2024/11/18/immigration-100-days-trump-executive-action-00189286>
- [21] Sarah Brayne and Angèle Christin. 2021. *Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts*. 68, 3 (2021), 608–624. doi:10.1093/socpro/spaa004 pmid:38250480
- [22] John Burnett. 2018. *Immigration Advocates Warn ICE Is Retaliating For Activism*. (2018). <https://www.npr.org/2018/03/16/593884181/immigration-advocates-warn-ice-is-retaliating-for-activism>
- [23] Kelly Caine. 2016. *Local Standards for Sample Size at CHI*. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose California USA, 2016-05-07). ACM, 981–992. doi:10.1145/2858036.2858498
- [24] Nancy Chen. 2024. *Asylum Employment Authorization, Explained*. Documented. <https://documentedny.com/2024/06/14/asylum-employment-authorization-document-clock/>
- [25] Christina Nuñez. 2014. *7 of the Biggest Challenges Immigrants and Refugees Face in the US*. Global Citizen. <https://www.globalcitizen.org/en/content/the-7-biggest-challenges-facing-refugees-and-immig/>
- [26] American Immigration Council. 2024. *Asylum in the United States*. https://www.americanimmigrationcouncil.org/sites/default/files/research/asylum_in_united_states_update_jan_2024.pdf. [Accessed 12-12-2024].
- [27] Ingrid Eagly and Steven Shafer. 2019. *Measuring in absentia removal in immigration court*. *U. Pa. L. Rev.* 168 (2019), 817.
- [28] Ben Green. 2019. *"Good" Isn't Good Enough*. In *AI for Social Good Workshop at NeurIPS* (2019). <https://www.semanticscholar.org/paper/%E2%80%9C%E2%80%9D%E2%80%9D-isn%E2%80%99t-good-enough-Green/dc2fed36474b1d1dd497b8f0e06183bb65cf48f>
- [29] 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* (Montreal QC Canada, 2018-04-19). ACM, 1–15. doi:10.1145/3173574.3173688
- [30] Tom Hanson, Laura Geller, Josh Peña, John Kelly, Aaron Munoz, and Jose Sanchez. 2024. *ICE's SmartLINK App Tracks Migrants by the Thousands. Does It Work?* CBS News. <https://www.cbsnews.com/news/does-ices-smartlink-app-work/>
- [31] James Kilgore, Emmett Sanders, and Kate Weisburd. 2024. *Carceral Surveillance and the Dangers of "Better-than-Incarceration" Reasoning*. The Law and Political Economy Project. <https://lpeproject.org/blog/carceral-surveillance-and-the-dangers-of-better-than-incarceration-reasoning/>
- [32] Jimmie E. Gates and Alissa Zhu. 2019. *Ankle Monitors and Informants: How ICE Chose the 7 Mississippi Food Plants to Raid*. The Clarion-Ledger. <https://www.clarionledger.com/story/news/politics/2019/08/09/ice-raids-federal-investigation-mississippi-poultry-plants/1960576001/>
- [33] Jose Olivares and John Washington. 2021. *ICE Discussed Punishing Immigrant Advocates for Peaceful Protests*. The Intercept. <https://theintercept.com/2021/06/17/ice-retaliate-immigrant-advocates-surveillance/>
- [34] Just Futures Law, Mijente Support Committee, and Community Justice Exchange. 2023. *Fact Sheet on ICE FOIA Lawsuit: ICE Documents Reveal Alarming Scale of Surveillance in ISAP Program*. <https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/6512da273ccb7321c334ab6c/1695734312687/ATDFOIAFinal.pdf>
- [35] Os Keyes, Jevan Hutson, and Meredith Durbin. 2019. *A Mulching Proposal: Analysing and Improving an Algorithmic System for Turning the Elderly into High-Nutrient Slurry*. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow Scotland Uk, 2019-05-02). ACM, 1–11. doi:10.1145/3290607.3310433
- [36] Austin Kocher. 2023. *Glitches in the Digitization of Asylum: How CBP One Turns Migrants' Smartphones into Mobile Borders*. 13, 6 (2023), 149. Issue 6. doi:10.3390/soc13060149
- [37] Matt Mahmoudi. 2025. *Introduction*. In *Migrants in the Digital Periphery* (1 ed.). University of California Press, 1–20. doi:10.2307/jj.25494964.6 jstor:jj.25494964.6
- [38] Camilo Montoya-Galvez. 2023. *ICE to Test Smartwatch-like Tracking Devices for Migrants Facing Deportation*. CBS News. <https://www.cbsnews.com/news/ice-smartwatch-tracking-device-migrants-deportation/>
- [39] Nedah Nemati and Dasha Pruss. 2025. *Carceral Technology and the Normalization of Psychological Torture*. OpenGlobalRights. <https://www.openglobalrights.org/carceral-technology-and-the-normalization-of-psychological-torture/>
- [40] Yazmine Nichols. 2022. *For Defense Attorneys: Tips for Effectively Challenging Pretrial Electronic Monitoring | ACLU*. American Civil Liberties Union. <https://www.aclu.org/news/criminal-law-reform/defense-attorneys-tips-for-challenging-electronic-monitoring>
- [41] D. Nuñez. 2011. *Inside the Border, Outside the Law: Undocumented Immigrants and the Fourth Amendment*. 85 (2011), 85–139. https://digitalcommons.law.byu.edu/faculty_scholarship/108
- [42] OpenAI. 2025. *Whisper*. OpenAI. <https://github.com/openai/whisper>
- [43] Kentrell Owens, Anita Alem, Franziska Roesser, and Tadayoshi Kohno. 2022. *Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives*. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA. <https://www.usenix.org/conference/usenixsecurity22/presentation/owens>
- [44] Dasha Pruss, Hannah Pullen-Blasnik, Nikki Stevens, Shakeer Rahman, Clara Belitz, Logan Stapleton, Mallika G. Dharmaraj, Mizue Aizeki, Petra Molnar, Anika Pinch, Nathan Ryan, Thallika Lima, David Gray Widder, Amiya Tiwari, Ly Xinzhen Zhangsün Brown, Jason S. Sexton, and Pablo Nunes. 2025. *Prediction and Punishment: Critical Report on Carceral AI*. doi:10.2139/ssrn.5017321

- [45] Joel Rose. 2021. Immigrant Activists Say ICE Is Purposely Targeting Them. They're Urging Biden To Help. (2021). <https://www.npr.org/2021/08/04/1024348198/immigrant-activists-ask-biden-administration-to-ban-ice-from-retaliating-against>
- [46] Georgia Robins Sadler, Hau-Chen Lee, Rod Seung-Hwan Lim, and Judith Fullerton. 2010. Research Article: Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & Health Sciences* 12, 3 (2010), 369–374. doi:10.1111/j.1442-2018.2010.00541.x arXiv:<https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1442-2018.2010.00541.x>
- [47] R Schulkind, W Brade, J Hynes, and K Allinson. 2022. Every Move You Make: The Human Cost of GPS Tagging in the Immigration System. *Report, Bail for Immigration Detainees, Medical Justice, and the Public Law Project, UK* (2022).
- [48] Adam Schwartz. 2017. *Digital Privacy at the U.S. Border: Protecting the Data On Your Devices*. Electronic Frontier Foundation. <https://www.eff.org/wp/digital-privacy-us-border-2017>
- [49] Ari Shapiro. 2019. Months After Massive ICE Raid, Residents Of A Mississippi Town Wait And Worry. (2019). <https://www.npr.org/2019/11/17/778611834/months-after-massive-ice-raid-residents-of-a-mississippi-town-wait-and-worry>
- [50] Sarah Sherman-Stokes. 2024. Immigration Detention Abolition and the Violence of Digital Cages. 95, 1 (2024), 219–266. <https://heinonline.org/HOL/P?h=hein.journals/ucollr95&i=233>
- [51] 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)* (San Francisco, CA, 2018-05). IEEE, 409–423. doi:10.1109/SP.2018.00023
- [52] Diane Taylor. 2022. GPS Tagging Migrants 'Psychological Torture', Says Report. (2022). <https://www.theguardian.com/uk-news/2022/oct/31/gps-tagging-migrants-psychological-torture-says-report>
- [53] TRAC. 2025. *TRAC Immigration - Comprehensive, Independent, and Nonpartisan Information about Immigration Enforcement - Alternatives to Detention (ATD)*. Transactional Records Access Clearinghouse. https://tracreports.org/immigration/detentionstats/atd_pop_table.html
- [54] Elizabeth Trovall. 2023. *The Growing Business of Immigrant Surveillance*. Marketplace. <https://www.marketplace.org/2023/08/02/the-growing-business-of-immigrant-surveillance/>
- [55] U. S. Government Accountability Office. 2022. Alternatives to Detention: ICE Needs to Better Assess Program Performance and Improve Contract Oversight | U.S. GAO. <https://www.gao.gov/products/gao-22-104529>
- [56] U.S. Immigration and Customs Enforcement. 2024. *Alternatives to Detention Frequently Asked Questions*. ICE.gov. <https://www.ice.gov/atd-faq>
- [57] Kate Weisburd. 2021. PUNITIVE SURVEILLANCE. *Virginia Law Review* 108 (2021).

A Interview protocol

Below is the interview protocol we used during our semi-structured interviews. The semi-structured nature of these interviews meant that we did not ask every question below in every interview, and all questions that we asked are not captured below. For example, whenever a participant mentioned a topic with which we were unfamiliar, we asked several clarifying questions to solidify our understanding of the topic before moving on. Naturally, these type of clarifying questions were more prevalent in earlier interviews and became less prevalent over time.

Consent form

Hello, thank you for agreeing to participate in this user study. Did you have a chance to look at the consent form before? No worries if not; we will go through it right now.

Report building

- Q1 What type of work do you do as an advocate?
- Q2 How many directly-impacted people have you worked with in the past?
- Q3 How did you become an immigrant rights advocate? What motivates you to do this work?
- Q4 What are the typical backgrounds of people with whom you work?

Main study

One goal of this research is to understand what questions people have about this app and how it functions. In future work we would like to attempt to answer these questions. For today we cannot offer answers to these questions because we likely do not yet know them but we would like to hear what they are. We would like to begin this interview by asking you to think about what questions you have about how the app functions or what it does. You can voice these questions now or you can voice the questions as they come to you during the rest of the interview. It may be the case that discussing a specific topic might remind you of questions that you have heard in the past. There are no stupid questions.

- Q1 What type of questions have you heard people ask about BI SmartLINK? What would you like to know more about BI SmartLINK's behavior or functionality? What are things about the app that you would like to understand better? If nothing comes to mind now, no worries; we can come back to this towards the end of the interview.
- Q2 What type of technologies do people describe being monitored by under ATD?
- Q3 Based on your understanding, how do people:
 - (a) Begin to be monitored by the app?
 - (b) What reason are they given for why they have to use the app (vs being released etc)? Do they/you believe this reason to be true/valid?
 - (c) Have you heard of people getting their passports taken, as a threat of more monitoring?
 - (d) If you don't want to use the app, is the only alternative being detained?
 - (e) How long are people told they'll be monitored? How long does it actually end up being?
 - (f) Do they have to pay to use the app? Did they install it on their own phones or did they get a phone from someone else? Was that phone free? Was there any assistance offered with setup?
 - (g) Stop being monitored by the app? What led to this? What impact did this have on them?
- Q4 What types of things do they do with the app? What type of changes (if any) have you heard about how the app functions?
- Q5 How did the app impact their behavior?
- Q6 In general, what have you heard about people's experiences using the app? Think about a specific positive, neutral or negative experience you have heard and describe it to us.
- Q7 Do you have any concerns about people using this app?
- Q8 If you could give feedback to the app's developers, what would it be?
- Q9 What have you heard about people's interactions with their case managers related to the app?
- Q10 Have you heard of people experiencing technical problems with the app, such faulty location detection?
- Q11 Now that we have discussed the app thoroughly, do any additional questions come to mind that you did not previously mention?
- Q12 What drew you to participate in this study?
- Q13 What do you wish researchers would focus on or study?

Q14 We only have a few minutes left; is there anything else you want to share before the interview is over?

Demographics

I have a few demographic questions. Feel free to decline to answer them.

Q1 Please select your age range from the following: 18-24, 25-34, 35-44 ...

Q2 What is your gender?

Recruitment

Could you share the study with others who might be good participants? Here is a link to the screening survey and here is a link to the recruitment flier.

B Codebook

Below is our codebook. We list our codes in the following format: [theme:code].

- Power imbalances: Abuse by officials
- Power imbalances: Lack of accountability

- Power imbalances: Relationships with case specialists
- Negative impacts: Employment
- Negative impacts: Housing
- Negative impacts: Well-being/Stress from mistakes or bad advice
- Negative impacts: Passports confiscated
- Negative impacts: Increased surveillance
- Negative impacts: Usability problems impact compliance
- Shortcomings of ATD: Historic support for ATD
- Shortcomings of ATD: Not a real alternative
- Shortcomings of ATD: ATD has widened its net
- Shortcomings of ATD: ATD hurts compliance
- Shortcomings of ATD: Monitoring is becoming ubiquitous
- Recommendations: For developers
- Recommendations: For researchers
- Recommendations: For policymakers
- Questions about BI: Location tracking
- Questions about BI: Data practices