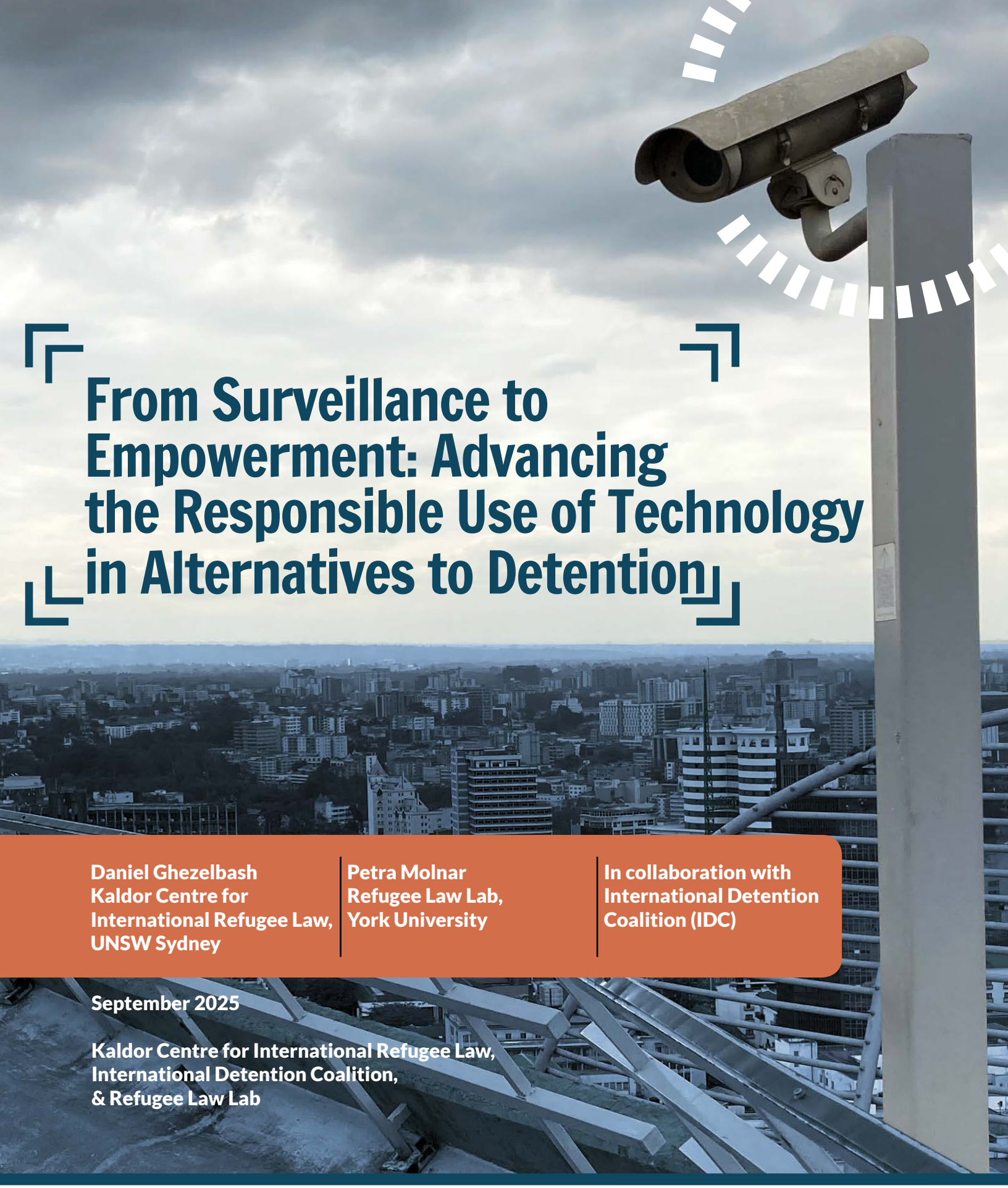


From Surveillance to Empowerment: Advancing the Responsible Use of Technology in Alternatives to Detention

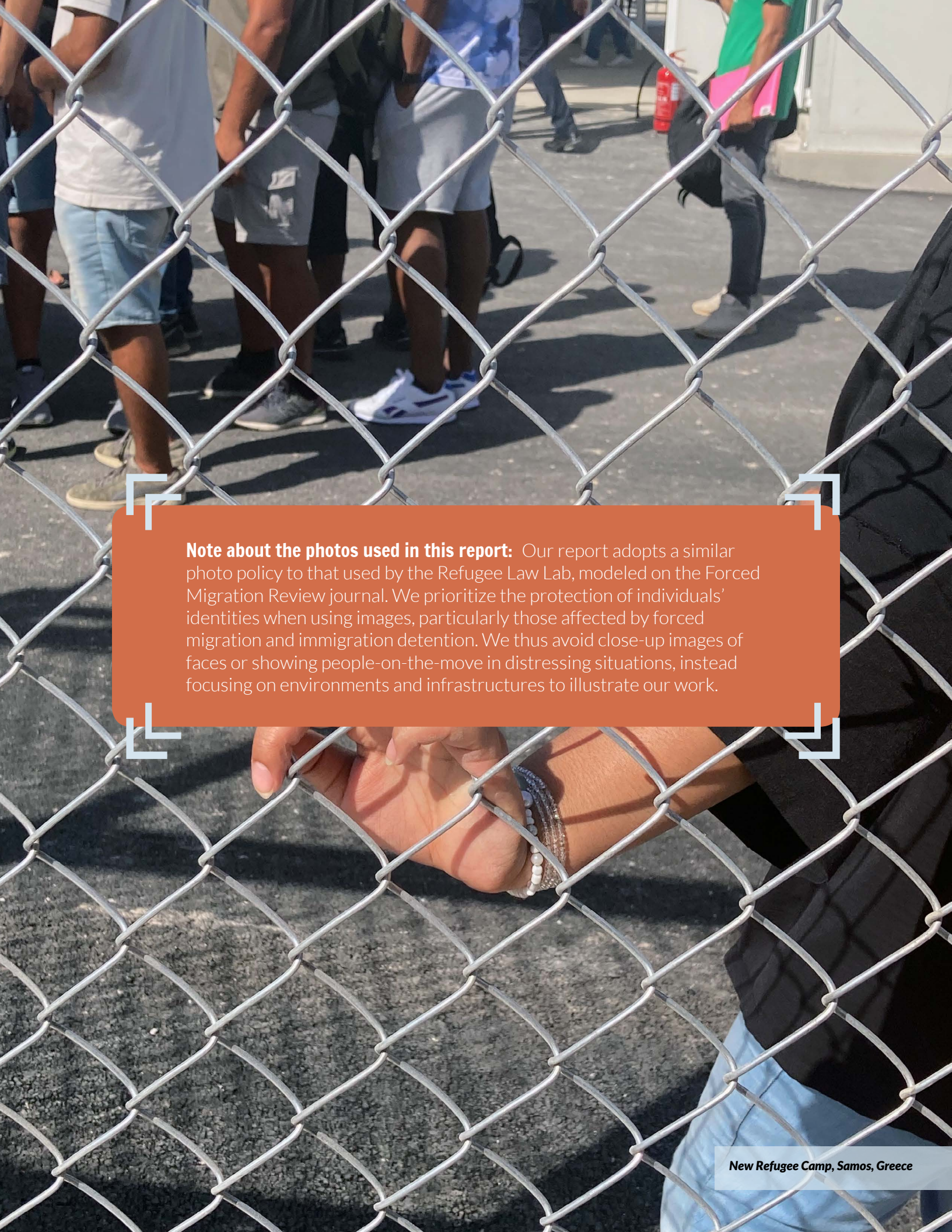
Daniel Ghezelbash
Kaldor Centre for International Refugee Law, UNSW Sydney

Petra Molnar
Refugee Law Lab, York University

In collaboration with International Detention Coalition (IDC)

September 2025

Kaldor Centre for International Refugee Law, International Detention Coalition, & Refugee Law Lab



Note about the photos used in this report: Our report adopts a similar photo policy to that used by the Refugee Law Lab, modeled on the Forced Migration Review journal. We prioritize the protection of individuals' identities when using images, particularly those affected by forced migration and immigration detention. We thus avoid close-up images of faces or showing people-on-the-move in distressing situations, instead focusing on environments and infrastructures to illustrate our work.

New Refugee Camp, Samos, Greece

ACKNOWLEDGMENTS

Authors: **Daniel Ghezelbash**, Kaldor Centre for International Refugee Law, UNSW Sydney, and **Petra Molnar**, Refugee Law Lab, York University, and the Berkman Klein Center, Harvard University. Written in collaboration with **Carolina Gottardo** and **Antonella Napolitano**, International Detention Coalition.

The authors wish to thank the 158 participants across eight global regions who participated in the consultations led by International Detention Coalition (IDC), whose perspectives and expertise helped to shape this report, as well as the academics, policymakers, and advocates who reviewed and provided feedback on the report. A special thank you to the numerous IDC team members from different regions who provided invaluable insights and input, including Asma Nairi, Bogdan Krasić, Gisele Bonnici, Hannah Jambunathan, and Mic Chawaratt. Thanks are also due to Aidan Hammerschmid for assisting with research and copyediting.

The authors also wish to acknowledge and thank all survivors of human rights violations at borders and in immigration detention. Their experience, agency, and insights have profoundly shaped the analysis and guided the development of this report, in order to advance the responsible use of technological tools in alternatives to detention. The legal standards, frameworks, and approaches presented here are rooted in their struggles, and we dedicate this work to them.

Report design by: Azza Abbaro, <www.azzaabbaro.com>
Photography by: Petra Molnar
Supported by: Robert Bosch Stiftung

Suggested citation: Daniel Ghezelbash and Petra Molnar. From Surveillance to Empowerment: Advancing the Responsible Use of Technology in Alternatives to Detention. Kaldor Centre for International Refugee Law, International Detention Coalition, and Refugee Law Lab, 2025.

UNSW SYDNEY

UNSW Kaldor Centre for International Refugee Law

The Kaldor Centre for International Refugee Law at the UNSW, Sydney is a leading research center dedicated to the study of international refugee law and forced migration. It provides evidence-based analysis to inform law, policy, and public debate, with a focus on protecting the rights of displaced people and advancing sustainable solutions.

refugee law lab

The Refugee Law Lab, which is a joint project between York University's Centre for Refugee Studies and Osgoode Hall Law School, undertakes research and advocacy related to new legal technologies and their impact on refugees, other displaced communities, and people-on-the-move.

INTERNATIONAL DETENTION COALITION

International Detention Coalition (IDC) is a global network with members in more than 75 countries that advocates to end immigration detention and promote rights-based alternatives. IDC conducts research, advocacy, and capacity-building to support humane, non-custodial approaches to migration governance.

CONTENTS

Surveillance camera in Nairobi, Kenya

EXECUTIVE SUMMARY

In recent years, some governments have adopted digital technologies to monitor people-on-the-move. Framed as alternatives to detention (ATD), tools such as GPS ankle monitors and smartphone-based tracking apps are promoted as humane and cost-effective. In reality, these technologies often replicate and extend the control and harms of detention in new digital forms. They can restrict liberty, undermine dignity, erode trust, and cause serious mental and health impacts, particularly when used by default and without safeguards. As such, they are better characterized as alternate forms of detention, rather than ATD.

This report, based on consultations with 158 participants across eight global regions and a survey of emerging practice, reveals a common pattern: technology framed as ATD is too often used for surveillance and enforcement, rather than rights-based support. Under the guise of efficiency, programs in some countries expand the detention net, entrench coercive control, and normalize invasive data collection. Many of these functions are outsourced to profit-driven companies with limited accountability and oversight.

Yet, technology also has the potential to be part of the solution, not the problem. When designed with and for affected communities, grounded in human rights law, and subject to strict proportionality, purpose-limitation, and oversight measures, digital tools can facilitate easier and more efficient reporting to migration officials, help people navigate complex migration systems, connect with essential services, work towards case resolution, and live freely and flourish in the community. Promising applications include alternate non-biometric digital reporting tools, digital case management systems, and geolocated support service directories.

The report sets out 10 guiding principles to ensure technology is used to reduce rather than extend detention, and to promote freedom, dignity, rights, and community integration. These principles address key risks, including the rise of expanded digital forms of detention; the lack of transparency and consent; weak legal safeguards and oversight; excessive data collection and discriminatory algorithms; privatization and profit-driven migration surveillance; and the psychological and physical harms caused by constant monitoring.

The principles should be applied holistically rather than individually, with each reinforcing and complementing one another. Together, the principles can guide the efforts of governments, international organizations, civil society, people with lived experience, and technologists to move away from surveillance-driven approaches and toward genuine alternatives grounded in trust, procedural fairness, and meaningful engagement.

Guiding Principle 1: **Prioritize, Respect, and Advance Human Rights**

Technological tools used in ATD must be designed and implemented in full accordance with international human rights standards. They must prioritize the liberty, dignity, privacy, and autonomy of individuals over coercion and surveillance.

Guiding Principle 2: **No Deprivation of Liberty**

Technological tools used in ATD must not amount to a deprivation of liberty, either individually or cumulatively (whether alongside other surveillance technologies, digital reporting tools, or non-tech compliance requirements). This would amount to de facto — or alternate forms of — detention.

Guiding Principle 3: **Reduce, Rather than Expand, Detention**

Technological tools must only be deployed in ATD where they enable people at risk of or in detention to live freely in the community. The use of technology should be non-intrusive and supportive, not punitive or coercive. Approaches that replicate or run parallel to existing immigration detention systems without helping to reduce the use of detention, or that impose continuous or unnecessary monitoring, do not constitute true ATD.

Guiding Principle 4: **Proportionate and Necessary**

Technological tools that restrict liberty should be used only when there is a clear and specific lawful basis to do so, and only when absolutely necessary, following a careful, individualized assessment of a person's circumstances. Such measures must be the least intrusive and most rights-compatible option available. They must never be applied as default or blanket solutions, must be strictly limited to what is essential in each case, and must be subjected to proportionality and necessity tests with strict purpose-limitation requirements to ensure that implementation is minimized to the specified and lawful purpose. The implementation of the restrictions must be time-limited, justified, and subject to regular review.

Guiding Principle 5: **Free and Informed Consent**

Participation in digital programs that restrict liberty should be based on free and informed consent. Individuals must be fully informed about how digital technology tools work, what data is collected, how long data is stored, what alternatives are available, what rights exist to challenge decisions, and the ability to opt out of participating in digital programs at any point. Individuals must not be penalized for making the choice to opt out.

Guiding Principle 6: **Access to Review and Oversight**

Individuals subject to technologies that restrict liberty must have meaningful access to independent oversight and review mechanisms so that they can challenge the imposition of restrictions and have access to legal recourse. This review process should assess whether the decision to restrict liberty was lawfully authorized and was both necessary and proportionate. It should involve specific consideration of the individual's circumstances and vulnerabilities and of the potential harms of the restrictions, including harm to family members. Measures must not only have a basis in law, but the grounding law must also be accessible, foreseeable, and sufficiently precise and must provide safeguards against arbitrariness. Ongoing human rights monitoring should be institutionalized to evaluate the impacts – and to mitigate the harms – of digital tools for the entire life cycle of each tool's development and implementation.

Guiding Principle 7: **Data Minimization and Privacy**

Data collected must be strictly limited to what is necessary for a specified, legitimate, and lawful purpose. It also must be anonymized where possible and must be stored securely, with people-on-the-move having clear access rights and data control as well as the right to erasure and the ability to opt out of data collection.

Guiding Principle 8: **Moratorium on Algorithmic Risk Assessments**

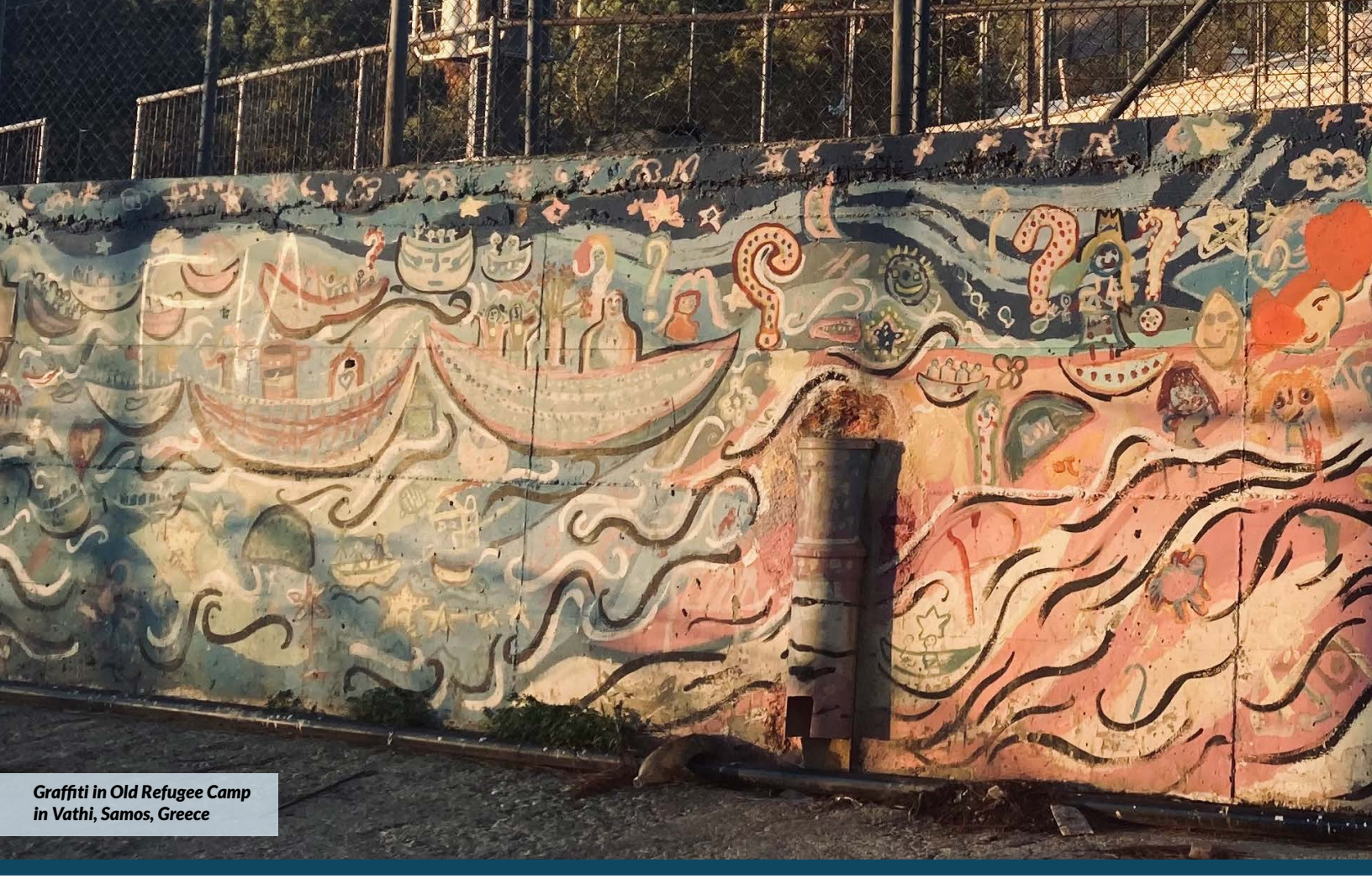
A precautionary moratorium on algorithmic risk assessments for imposing surveillance technologies should be adopted unless and until demonstrable and ongoing safeguards can ensure transparency, accuracy, the absence of bias and discrimination, and accountability in their design and implementation.

Guiding Principle 9: **Public Interest over Profitability**

Any technology used in immigration detention, surveillance, or ATD should be developed, managed, and deployed by governments or non-governmental organizations (NGOs) as far as possible. Any outsourcing, whether to NGOs or commercial entities, must adhere to the principles of open and public procurement, be subject to ongoing human rights and data impact assessments, and include safeguards to ensure transparency and accountability.

Guiding Principle 10: **Engagement not Enforcement**

Technology used in the context of ATD should focus on enhancing community-based support, integration, and case resolution and should respect rights. This means moving away from enforcement-focused surveillance that harms, stigmatizes, and criminalizes people-on-the-move to engagement-based approaches. Technology should empower individuals toward a just and fair resolution of their case by facilitating effective case management and holistic community-based support to help people achieve stability, navigate complex systems, and access services. Technology and evaluation processes should also be actively designed or co-designed with people-on-the-move.



Graffiti in Old Refugee Camp in Vathi, Samos, Greece

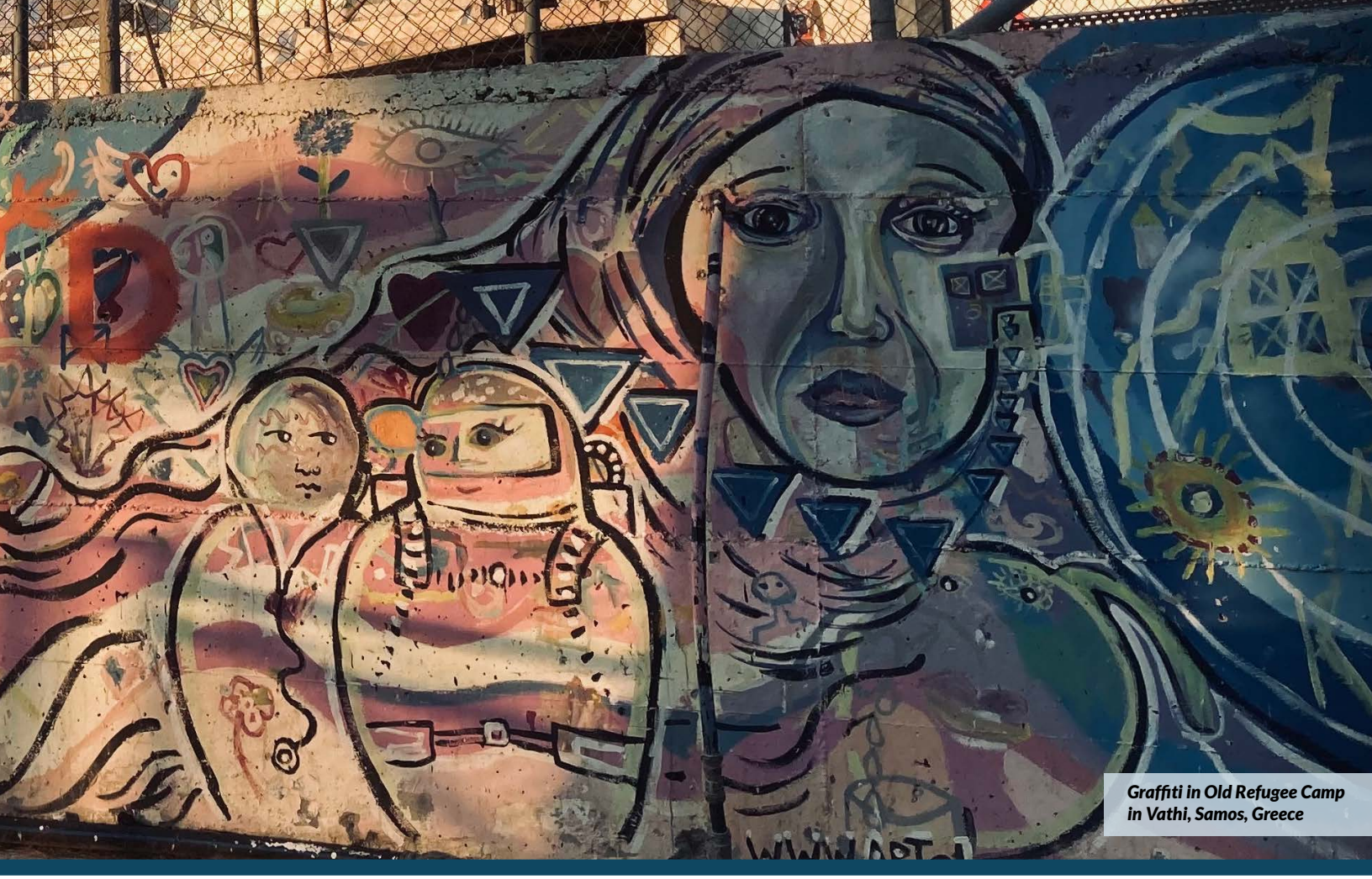
INTRODUCTION

This report is a collaboration between the Kaldor Centre for International Refugee Law at UNSW Sydney, International Detention Coalition (IDC), and the Refugee Law Lab at York University, with support from Robert Bosch Stiftung.

In recent years, some governments have turned to digital technology to monitor people-on-the-move. At times, these tools are presented as alternatives to detention (ATD) claimed to be more humane and less costly than holding people in detention facilities. But, in some cases, these systems replace physical walls with digital ones, reproducing the same structures of control and coercion in less visible ways. As such, they can often be better characterized as alternate forms of detention rather than true rights-based ATD.

This report examines how technology is reshaping immigration detention, ATD, and the surveillance of people-on-the-move. It explores how technology can harm or help, depending on its design, purpose, and governance. We distinguish between three types of technology.

- **Surveillance technologies** continuously monitor, track, or record people's movements or behaviors, without user initiation. Examples include GPS ankle monitors, GPS-enabled watches, and smartphone tracking apps. These often constitute alternate forms of detention instead of ATD due to the level of control and restriction imposed.



Graffiti in Old Refugee Camp in Vathi, Samos, Greece

- **Digital reporting tools** require individuals to actively check in, provide updates, or confirm compliance, usually at scheduled intervals, though sometimes at random or unpredictable times. Verification can involve biometric methods (such as facial recognition or voice authentication) or non-biometric methods (such as PIN codes or community attestation). While generally less intrusive than continuous surveillance, reporting can become burdensome or surveillance-like when it is frequent or unpredictable or when it demands biometric data.

- **Digital support services** are systems designed to assist and empower people in ATD programs rather than control them. These include case management platforms, communication tools, and service directories that connect users to legal and other support services. When co-designed with affected communities and grounded in rights-based principles, these tools can foster trust and promote agency and community integration.

The findings are clear: some states have prioritized technological surveillance and overly intrusive digital reporting tools over digital support services. Technology has been integrated into migration enforcement with limited transparency, often without independent oversight or meaningful consent. These trends raise profound concerns under international human rights law, including risks to privacy, liberty, equality, and the right to health.

However, it does not have to be this way. Technology can be reoriented toward supporting freedom and integration and facilitating easier and more efficient reporting to migration officials. It could support case resolution, which benefits states and people-on-the-move, if managed in the right way. For this type of reorientation to occur, technology must be developed with people-on-the-move, grounded in legal safeguards, and used to expand — rather than restrict — choice and agency.

The report begins by setting out the context of immigration detention, the international frameworks that govern the practice, and its many harms. The report then introduces ATD and its benefits. The focus then turns to outlining the various forms of technology that have been used in this space, further unpacking the distinction between surveillance technologies, digital reporting tools, and digital support services. The report proceeds to offer a jurisdictional analysis of the current state of play in the use of technology in surveillance and ATD, focusing on North America, Latin America and the Caribbean, Europe, Southwest Asia and North Africa (SWANA), the African continent, the Asia-Pacific region, and Australia/New Zealand.

The report then presents a series of guiding principles for the use of technology in surveillance and ATD. These are integrated into the analysis of key cross-cutting risks, including the lack of transparency and accountability, the role of privatization and profit in migration surveillance, and the need for a rights-based approach to introducing technology in the context of digital surveillance and ATD. The report then moves from principles to practice, concluding with a discussion of the opportunities technology offers for improving and expanding rights-based ATD, including in relation to case management and holistic legal support. It also highlights the need to advocate for community-based design and participatory approaches to innovation in the migration space.

In our effort to integrate a collaborative and participatory methodology throughout this project, IDC led a series of global consultations with 158 participants across eight regional meetings, with invited experts from the non-governmental organization (NGO) sector, international organizations, academia, and people with lived experience. Their insights helped shape the framing, substantive analysis, and guiding principles of this report. Their expertise has been reflected throughout the report under Chatham House rules (without individual and organizational attribution), supplemented by a cross-jurisdictional review of publicly available sources and an analysis of relevant legal frameworks.

Wherever possible, this report uses people-centered language. We specifically use the term "people-on-the-move" to expand the terminology commonly used when discussing human migration and how immigration detention technologies are experienced. This deliberate use of more inclusive terminology does not seek to undermine the fact that some categories of mobile communities, such as refugees, face particular vulnerabilities and often experience greater risks and harms as a result of migration management technologies. It simply highlights that, at the end of the day, there are *people* at the center of all technological development and deployment.

“Invisible Leash”[1]

Mariela crossed into Arizona just after dawn, her daughter Isabela pressed tightly to her chest, both of them shivering despite the desert heat rising around them. She was 35 years old, with deep lines etched around her eyes, not from age, but from years of waiting: waiting for her asylum claim to be processed in Guatemala, for her brother’s remittances from Houston to arrive, for the violence in her town to stop.

Border Patrol picked them up near Nogales. Mariela had practiced sharing what happened to her: how she had fled after refusing to pay the gang tax that tripled when they learned she was receiving dollars from the north. She asked for asylum then and there, clutching Isabela as a translator fumbled her words in a language she had never spoken.

Mariela and Isabela were separated that night. “Just for processing,” the officer said. It was 24 hours before Mariela saw Isabela again, but time twisted inside the cold, metallic box they called *la hielera*, the icebox. Fluorescent lights flickered overhead. The floor was concrete. The mylar blanket rustled like plastic leaves. She could not sleep. She could not cry. She could not think until she was reunited with Isabela, who was catatonic from fear.

From there, Mariela and Isabela were moved to a privately-run family detention center in Texas. Mariela had no idea what that meant. The facility looked like a warehouse. Cameras tracked her every movement, and a heavy bracelet was clasped to her ankle. It buzzed softly every few hours. She later learned it logged her location, steps, and even patterns of restlessness at night.

Every call to her brother cost nearly a dollar a minute. Medical care required a request, followed by a long wait. Isabela developed a cough that would not go away. Mariela began hiding extra food in napkins for Isabela to eat later, hoping it wouldn’t make her daughter sick.

Two weeks later, a caseworker told her she qualified for the Alternatives to Detention program run by Immigration and Customs Enforcement (ICE). She was fitted with a new ankle monitor and released, but she didn’t feel free. A case manager explained how to check in through an app called SmartLINK, which would use her phone’s camera to scan her face. “Just once a day,” they said. But the app sometimes asked three times, sometimes 10. If she missed a scan, she feared deportation.

In her brother’s small apartment in Houston, Mariela set alarms for SmartLINK check-ins. She stopped taking Isabela to the park in case the monitor sent the wrong signal. One night, she woke in a panic, convinced the app had recorded her face incorrectly. Her phone had died. She cried silently so Isabela wouldn’t hear.

Even though she was no longer in detention, Mariela’s freedom existed within the boundaries of an app. Mariela didn’t call this surveillance. She called it *la cuerda invisible*, the invisible leash.

Border wall in Sonoran Desert, Arizona, United States

Moria Refugee Camp, Lesvos, Greece

What Is Immigration Detention?

Immigration detention refers to any situation in which a person is deprived of liberty on grounds related to their immigration status, regardless of the label or reason given for carrying out the deprivation of liberty, or the name of the facility or place where the person is held. Unlike criminal detention, which follows a judicial process in response to a criminal offense, immigration detention is usually a civil — and often administrative — measure. It is used by states to manage the movement, identification, assessment, or removal of non-citizens, including people seeking asylum, undocumented and stateless persons, victims of trafficking, and people awaiting deportation.

Detention may occur at borders, in transit zones, or within a country, and can take place in dedicated immigration facilities, police stations, or prisons. IDC has also identified the rising trend of ad hoc sites being used as alternative places of detention — including hotels, barracks, boats, and isolated locations — some of which function similarly to formal immigration detention facilities[2]. Increasingly, states are incorporating digital technologies — such as electronic monitoring, biometric tracking, and algorithmic decision-making — into detention regimes, either as alternatives or extensions of confinement[3]. This has been accompanied by a push to privatize both immigration detention as well as the digital technology used in this space.[4]

International legal frameworks governing immigration detention — most notably, the International Covenant on Civil and Political Rights (ICCPR),[5] the Convention on the Rights of the Child (CRC),[6] and the Convention relating to the Status of Refugees (Refugee Convention)[7] — require that any form of detention be lawful, non-arbitrary, necessary, and proportionate to the aim pursued, with procedural safeguards in place to protect individual rights. Article 9 of the ICCPR affirms the right to liberty and protection against arbitrary detention, which applies equally to non-citizens regardless of their migration status. Various United Nations committees have also stressed the exceptionality of immigration detention and the need for alternatives,[8] underscoring that immigration detention should only be used as a last resort.[9] This principle of last resort does not apply to children.[10] Detaining children because of their — or their parents' — migration status is prohibited under international law as it will always violate the "best interests of the child" principle.[11]

In practice, immigration detention is often used as a deterrent against irregular migration or as a mechanism to facilitate deportation. However, research shows that this approach is not effective, is inhumane, and costs much more than other, more effective options.[12] Detainees may face prolonged and arbitrary detention or, in some cases, indefinite confinement due to bureaucratic delays, a lack of documentation, or statelessness, as well as the absence of explicit time limits or review mechanisms. Immigration detention can result in limited access both to legal advice and to fair immigration and asylum proceedings, which often causes lengthy — or even indefinite — delays in resolving migration processes.

Detention conditions vary widely across contexts, but many facilities suffer from overcrowding, poor sanitation, and inadequate access to medical care. Immigration detention practices have drawn widespread criticism[13] from human rights bodies, particularly when used on vulnerable groups, such as survivors of trafficking, LGBTQI+ individuals, or those with mental health conditions. Children also continue to be detained in various jurisdictions in direct contravention of international law, leading to profound psychosocial and developmental issues and compounded trauma. Immigration detention has been found to harm children even if the detention is of a relatively short duration and is carried out in so-called "child-friendly" facilities.[14] Immigration detention has also been widely documented as a site of systemic harm, disproportionately impacting racialized and historically marginalized communities.[15] These harms of immigration detention are both physical and psychological. Numerous studies document high rates of depression, anxiety, post-traumatic stress disorder, and self-harm among detainees.[16] These effects are exacerbated for those already traumatized by war, persecution, or displacement. Importantly, these harms are not collateral; they are inherent in the logic of detention, which deprives individuals of their liberty without criminal charge or trial.

The use of prolonged and arbitrary detention, often without access to legal counsel or meaningful oversight, reproduces patterns of structural violence and contributes to the dehumanization of detainees.[17] These effects disproportionately impact racialized groups, whose vulnerability is magnified by intersecting inequalities related to language, legal status, and socio-economic precarity.[18] Efforts to address the harms of immigration detention must therefore reckon with its entanglement in systems of racialized control and carceral governance. The effects of immigration detention are also gendered and intersectional, with detention having a disproportionate effect on women and gender-diverse people. Reformist approaches that simply seek to make detention more humane risk obscuring its foundational violence. Perspectives which call instead for the dismantling of detention regimes and the development of rights-based, community-led alternatives[19] are part of a more transformative agenda, one that centers people's dignity, decolonial justice, and freedom of movement as core principles of any just immigration system.

What Are Alternatives to Detention?

ATD refers to mechanisms that provide states with a means to manage migration without resorting to custodial detention. IDC defines ATD as "any law, policy or practice by which persons are not detained for reasons relating to their migration status."[20] These can include a range of non-custodial approaches. Engagement-based ATD recommended by IDC include open reception centers, reporting requirements, and other community-based management options.[21] Examples of enforcement-based ATD include bond or bail systems, as well as designated residence conditions. The underlying goal of ATD is to avoid the harmful effects of incarceration for immigration-related reasons.

There are three main benefits of using ATD instead of detention. First, ATD has a positive impact on people's physical and mental health, simply because detention is inherently harmful. An evaluation of the ATD pilot in the United Kingdom (UK) — commissioned by the Office of the United Nations High Commissioner for Refugees (UNHCR) — found strong evidence that people supported in the community experienced greater stability and better health and well-being outcomes than when in detention.[22] The 2020 evaluation of ATD pilots in Bulgaria, Cyprus, and Poland commissioned by the European Philanthropic Initiative for Migration (EPIM) confirmed that case management strongly supported people's well-being, particularly their emotional and psychological health.[23] It helped them engage more proactively with immigration procedures, with 82 per cent of participants reporting improved psychological well-being.[24]

Second, ATD programs help manage migration more effectively than detention, which does not deter or reduce irregular arrivals.[25] Detention does not support case resolution, yet ATD can promote compliance and more efficient and sustainable immigration decision-making.[26] For example, IDC's *There Are Alternatives* report highlights evidence from 13 ATD programs with compliance rates ranging between 80–99.9 per cent.[27] Additionally, EPIM's evaluation of ATD pilot projects in Bulgaria, Cyprus, and Poland found that 86 per cent of individuals remained engaged with immigration procedures through community-based ATD.[28]

Third, ATD programs are much more cost-effective than immigration detention. According to IDC, ATD programs can be up to 80 per cent cheaper than detention, when taking into account the cost of detention infrastructure and operational cost, as well as associated litigation costs.[29] In Australia, detaining someone can exceed AUD$1,384/day,[30] while community programs cost around AUD$7/day.[31] In the United States, the cost of immigration detention averages $165 per day[32] (and almost USD$320/day for families with women and children),[33] yet community-based ATD programs like the former Family Case Management Program (FCMP) cost just USD$38.47/day per family.[34]

However, other so-called "alternatives" — which are more enforcement-based — have drawn criticism for replicating the punitive features of detention in less visible forms.[35] Reporting requirements, such as mandatory check-ins at police stations or immigration offices, can impose undue burdens, especially for those without access to transportation or childcare. These forms of control, although technically non-custodial, can still limit autonomy and produce fear, instability, and forced compliance.

There is also a trend toward integrating surveillance technologies and invasive digital reporting tools into so-called ATD programs.[36] Electronic monitoring is promoted by some states as an ATD,[37] but in effect it often amounts to an alternate form of detention instead of a true ATD. This is particularly the case with GPS ankle monitoring and other wearable technologies, as well as some forms of intrusive smartphone tracking apps that rely on continuous live location tracking and biometric information.

Ultimately, ATD are not merely about "managing compliance" but about reimagining responses to migration in ways that uphold the dignity, agency, and rights of all individuals, regardless of status. The challenge lies not in refining systems of control and surveillance, but in moving toward approaches that humanize migration processes altogether. In this sense, it is important to move to a new migration governance paradigm based on permanent solutions, access to rights, and protection and regularization pathways, where governments around the world do not detain people for reasons related to their migration status and instead proactively protect their rights in the community.

Digital Technologies Used in Surveillance and ATD Programs

Some governments describe surveillance technologies as ATD, but their focus on enforcement and the restriction of liberty means they may function more as alternate forms of detention than genuine ATD. Not all technology in this space is equally intrusive: the level of interference with personal freedom varies by type and design of the tool. It is essential to distinguish between surveillance technologies, digital reporting tools, and digital support services, as each category carries different implications for agency, intrusiveness, and the scope of data collection.

SURVEILLANCE TECHNOLOGIES

Surveillance technologies are digital tools deployed by authorities to passively or actively monitor, track, or record the movements and behaviors of individuals in the community, usually with little or no user initiation. These technologies typically operate continuously, often collecting broad and ongoing data to support enforcement and risk management objectives.

Electronic Monitoring Devices

Wearable devices — such as GPS ankle monitors or GPS-enabled watches — that continuously track a person's real-time location using satellites, cell towers, and Wi-Fi positioning. Newer devices may also incorporate biometric authentication.

Smartphone-Based Tracking

Apps installed on smartphones that operate in a similar manner to wearable electronic monitoring devices, continuously tracking a person's real-time location using GPS and other data. These apps also often employ biometric facial and voice recognition to verify identity and monitor compliance.

Biometric Verification Systems

Technology integrated into electronic monitoring devices and smartphone-based tracking — as well as digital reporting tools (see below) — that collect biometric data for the purpose of verification. These systems may use the real-time capture of a person's face or voice for one-to-one matching against previously stored personal biometric data.

Algorithmic Risk Assessments

Automated systems that analyze various factors to determine a person's flight risk or security classification. They can influence decisions about detention conditions, monitoring intensity, and eligibility and monitoring conditions for ATD programs.

DIGITAL REPORTING TOOLS

Digital reporting tools require active and ongoing participation from the monitored person to provide status updates, report their location, or demonstrate compliance. They operate on the user's initiative and, when designed with strong safeguards, may offer greater agency and autonomy. These tools are generally less intrusive than continuous monitoring, functioning at set points in time and gathering only limited, specific data. However, some digital reporting tools blur the line with surveillance,

New Refugee Camp, Kos, Greece

particularly where reporting intervals are random or unpredictable, or where they rely on intrusive biometric verification. Such features result in reduced agency and a disruption of daily life, and they can create impacts similar to continuous monitoring.

Mobile Check-In Apps

Smartphone apps that prompt individuals to check in at regular or unscheduled times using PIN codes, selfies, video calls, or other active response mechanisms that often rely on biometric verification. Unlike continuous smartphone-based tracking (see above), data is only collected upon user action. The mechanism for reporting can significantly shape both the risk profile and the participant experience: biometric verification introduces heightened privacy, accuracy, and security concerns, while participatory reporting tools can foster greater agency and trust but may still involve power imbalances and risks if safeguards are weak. The choice of mechanism influences not only data protection requirements but also the intrusiveness, stigma, and overall impact on the individual's daily life.

Telephone Reporting

Practices that require participants to check in over the phone at predetermined times. Newer, automated systems can initiate calls and verify identity using biometrics.

Participatory Reporting Tools

Alternatives to voice biometrics that allow users to choose verification methods (such as community leader attestations or visual PIN codes).

DIGITAL SUPPORT SERVICES

Distinct from compliance or monitoring mechanisms, digital support services aim to empower and assist rather than to control. These services do this by prioritizing freedom of movement, community-led design, rights-preserving architectures, and integration-focused tools over purely compliance-driven systems.

Digital Case Management Platforms

Secure, centralized systems that help coordinate and support people-on-the-move in ATD programs. They enable case managers to track legal deadlines, facilitate communication, and connect individuals to vital services. Designed with user needs in mind, they promote stability, dignity, and compliance while also safeguarding privacy and fostering trust.

Integration-Focused Digital Resources

These resources include platforms and geolocated apps that connect people-on-the-move to centralized and decentralized service directories. They help individuals access healthcare, legal assistance, housing, education, and employment opportunities, and they are often co-maintained by people-on-the-move and NGOs.

By clearly differentiating between surveillance technologies, digital reporting tools, and digital support services, it becomes possible to better evaluate their respective impacts on liberty, dignity, and compliance, and to advance truly rights-based ATD.

New Refugee Camp, Kos, Greece

DIGITAL TECHNOLOGIES IN SURVEILLANCE AND ATD PROGRAMS

This section sets out the current state of play when it comes to the use of digital technology in surveillance and ATD programs, drawing on the input of participants in the regional consultations, as well as a survey of publicly available sources. It reveals that the use of technology by some states has focused on intrusive digital surveillance, rather than on promoting rights-based ATD. The United States, Canada, the UK, and Australia have led the way in terms of the expansion of privatized surveillance technologies — such as electronic monitoring and smartphone-based tracking — that extend state control into communities under the guise of efficiency and cost-effectiveness. The consultations revealed that numerous governments in other regions are also considering deploying similar technologies, raising the risk of further diffusion of surveillance technology. While documentation practices in areas such as Latin America, Africa, and the SWANA region are also increasingly relying on digital technologies like biometric registration, these practices need to be understood contextually, as documentation can be a way to prevent a person from being incarcerated in physical detention. However, documentation practices also present their own risks, such as inappropriate data retention and sharing, which amplifies the need to use a human rights-based approach to any implementation of technologies in documentation efforts and in the immigration detention and ATD space.

This rise of digital technologies also intersects with broader trends of border externalization, the criminalization of migration, and privatization, as governments increasingly partner with corporations to deploy systems that prioritize compliance over rights.[38] There are also contexts where surveillance technologies are used on internally displaced, inland, or otherwise captive populations. For example, the use of surveillance has expanded in the Occupied West Bank and Gaza, with private companies (such as Elbit Systems and Cellebrite) and other actors leading the development of these technologies.[39] Similarly, in China's Xinjiang Province, the Chinese government relies on private actors to develop technology used to detain the Uyghur Muslim population.[40] These tools — such as biometric databases, facial recognition, and predictive policing algorithms — are functionally similar to those used in immigration detention, but they operate at a broader and more oppressive scale, illustrating how surveillance infrastructure developed for border control can be redirected toward mass internment and social control and vice versa.[41]

The shift of states increasingly relying on new surveillance technologies reflects the broader pivot toward digital migration management and border control, where non-genuine, so-called "alternatives" often serve as vehicles for intensified migration control, rather than as pathways to liberty.

NORTH AMERICA (CANADA, UNITED STATES, MEXICO)

North America's migration enforcement landscape is increasingly defined by biometric tracking, algorithmic monitoring, and private sector partnerships in immigration detention. Whether through electronic monitoring devices, GPS-enabled apps, satellite-linked border monitoring, or biometric check-ins, governments are shifting immigration enforcement into the digital realm under the guise of efficiency and to meet political goals.[42] Our consultation participants raised concerns about the vast and urgent challenges that these technologies pose to transparency, accountability, and human rights protection.

In Context: Privatized and Digitized Immigration Detention

The United States has seen extensive and growing use of technology in immigration enforcement. ICE operates a sprawling network of detention facilities, many of them under the management of private prison corporations such as GEO Group and CoreCivic, which are equipped with advanced surveillance technologies.[43] Associated case management software, developed by private vendors like Palantir Technologies, integrate personal data, immigration histories, court statuses, and now even predictions about future behavior to monitor people-on-the-move in custody and to facilitate removals.[44]

Since January 2025, the second Trump administration has significantly escalated the use of artificial intelligence (AI) in immigration surveillance and detention.[45] Its AI-driven "Catch and Revoke" program monitors people's social media activity, targeting those deemed to express anti-Israel or pro-Palestinian sentiments, engaged in Diversity and Inclusion work, or in any other activity determined to "undermine public safety."[46] Simultaneously, federal intelligence and border agencies, along with private military and security contractors, have expanded the digital wall at the US–Mexico border, using a fusion of drones, satellite surveillance, and AI-powered analytics to detect border crossings in real time.[47] This infrastructure is monitored through the Department of Defense, the Department of Homeland Security, and private military contractors, enabling a massive expansion of the use of predictive surveillance and algorithmic risk assessments along the US–Mexico border.[48]

In February 2025, President Trump used an executive order[49] to revoke federal AI ethics guidelines and mandate the prioritization of national security applications of AI in the United States, dismantling the few safeguards that existed in relation to automated immigration enforcement and accelerating the normalization of algorithmic surveillance.

In Canada, the Canada Border Services Agency (CBSA) has also widely integrated digital surveillance tools into its immigration detention facilities. These tools include digital fingerprinting, facial recognition, and electronic case management systems to track detainee

movement and the progress of their legal cases. In Mexico, immigration detention takes place in federally-managed facilities that employ biometric registration, closed-circuit television (CCTV), and digital entry/exit logs to monitor detainees.[50] Mexico's National of Institute Migration fingerprints and photographs people-on-the-move upon arrival and information is cross-checked against US and Interpol databases via the Biometric Identification Transnational Migration Alert Program (BITMAP),[51] a US-funded initiative aimed at border security cooperation. This program can be seen as reflecting a larger trend of the US externalizing its border enforcement to Mexico.[52]

Surveillance Technologies and Digital Reporting Tools

The United States leads North America in deploying surveillance technology in the context of what the government frames as "ATD" in their supervision and release program.[53] The Intensive Supervision Appearance Program (ISAP) is the United States' largest and most technologically integrated non-custodial immigration enforcement program.[54] It is administered by ICE in partnership with BI Incorporated, a subsidiary of The GEO Group.[55] Originally launched in 2004, ISAP was designed as an ATD to ensure that people-on-the-move comply with immigration court requirements while remaining in the community. The program has since grown significantly and, by the end of the 2024 fiscal year, more than 179,000 people were participating in the program,[56] far surpassing the number presently held in physical ICE detention.[57] ISAP participants include people seeking asylum, individuals with removal orders, and those awaiting court outcomes. Digital technology plays a central role in how ISAP operates and enforces compliance. Participants may be required to wear GPS ankle bracelets and, more recently, wrist-worn GPS tracking devices, which transmit real-time geolocation data to BI Incorporated's centralized monitoring system.[58] Others are assigned to check in through the SmartLINK app, which uses facial recognition and geolocation technology to verify identity and track location.[59] The app also supports messaging between the contracted case manager and the individuals under supervision, adding a layer of case management to the surveillance infrastructure.[60]

Traditional telephonic check-ins remain in use as well. Automated calls using biometric voice check-ins are used for individuals without smartphones or in areas with limited connectivity. These systems analyze vocal patterns during phone calls to confirm identity.[61] While ICE has promoted these tools as effective, efficient, and less restrictive than detention,[62] rights groups have raised concerns about privacy, stigmatization, mental health impacts, and due process, particularly given the program's scale and opaque data-handling practices.[63] Scholars and advocates argue that ISAP's technological design mirrors punitive systems, embedding people-on-the-move in a digitally networked carceral regime rather than providing a truly rights-based alternative to confinement.[64] These digital surveillance tools do offer cost savings: detention costs approximately USD$165/day per individual,[65] while SmartLINK costs USD$4/day.[66] However, advocates have warned about the psychosocial impacts of this type of ongoing and continuous surveillance, which greatly expands the "surveillance dragnet" beyond traditional detention facilities into private homes and communities.[67] In comparison, genuine non-carceral ATD programs such as the FCMP cost USD$38.47/day per family unit,[68] while also facilitating overwhelming compliance and engagement, positive relations, and fewer adverse psychosocial impacts.[69]

In Canada, the CBSA has piloted surveillance technology and digital reporting tools in the context of what it frames as ATD. In 2018, the CBSA launched a national ATD program that included GPS ankle monitors for a limited number of persons identified as "high-risk individuals."[70] This program also introduced a voice recognition reporting system, allowing people to check in by phone with

biometric voiceprints and reducing the need for in-person appointments. These tools were paired with community-based supervision contracts with NGOs, aligning with Canada's broader policy goals of minimizing detention for children and asylum seekers and moving away from housing immigration detainees in provincial prisons.[71]

However, in 2025, the CBSA revised a surveillance technology contract to allow foreign companies to bid on supplying and tracking ankle monitors.[72] Additionally, the CBSA amended the relevant Request for Proposals (RFP) to allow for the storage of data outside Canada.[73] In November 2024, Canada launched an app similar to the US's SmartLINK, called ReportIn, which likewise uses facial recognition technology to verify people for immigration reporting while outside of custody.[74] However, our consultation participants, as well as scholars and advocates, have identified issues with voice-printing and facial recognition as ATD, including privacy concerns around data collection, data storage, and potential data sharing with other government departments and private actors,[75] as well as the lack of accuracy with voice-printing software and its potentially discriminatory effects.[76]

Mexico is yet to implement surveillance technologies and digital reporting tools in its ATD programs. Instead, Mexico often relies on periodic in-person check-ins to ensure compliance, particularly for individuals returned under bilateral asylum agreements with the US. However, human rights groups warn that the Mexican authorities may soon consider using electronic tagging for selected people with deportation or parole conditions, given the pressures for increased data collection and cross-border sharing.[77]

LATIN AMERICA AND THE CARIBBEAN

Some countries in Latin America and the Caribbean are also increasingly moving toward a digitally-enabled model of migration governance. Our consultations revealed that enforcement and identification are the top policy priorities in some countries in the region, driven by pressure from the United States for countries with transit migration contexts in Latin America to externalize border control.[78]

In Context: Detention and Border Externalization

The use of immigration detention technology varies widely across Latin America. Historically, most countries in South America and Central America maintained only ad hoc detention facilities, often briefly detaining people who irregularly migrated in police stations or administrative holding areas.[79] Some countries in South America, such as Ecuador and Uruguay, prohibit immigration detention, while others, such as Colombia, have used regularization models instead of resorting to immigration detention.[80] Chile and Peru have adopted electronic case management systems to process administrative violations, to track court hearings, and to coordinate removals, thereby minimizing the length of physical custody.[81]

However, ongoing regional geopolitical events — particularly Haitian migration, the mass displacement of Venezuelans, and transit movements from Central America — have prompted more restrictive state responses. In the few formal immigration detention centers that exist in Latin America, there is increasing attention to bringing in more technology. In Argentina, the

Unidad 35 immigration holding facility uses CCTV to monitor detainees.[82] And now, with the crackdown on immigration in the United States and the externalization of immigration detention to countries like El Salvador, Costa Rica, and Panama, digital detention infrastructure for the physical deprivation of liberty will likely be expanded, including surveillance inside detention centers and data sharing between transit countries.

Surveillance Technologies

While continuous electronic tagging (for example, through GPS ankle monitors) remains rare even in the criminal justice context in Latin America, discussions about its potential use have occurred. In 2019, for instance, the Dominican Republic publicly considered electronic bracelets for people with deportation orders, expanding their use from the domestic criminal justice context[83] and indicating the risk of diffusion of surveillance models from the Global North.[84]

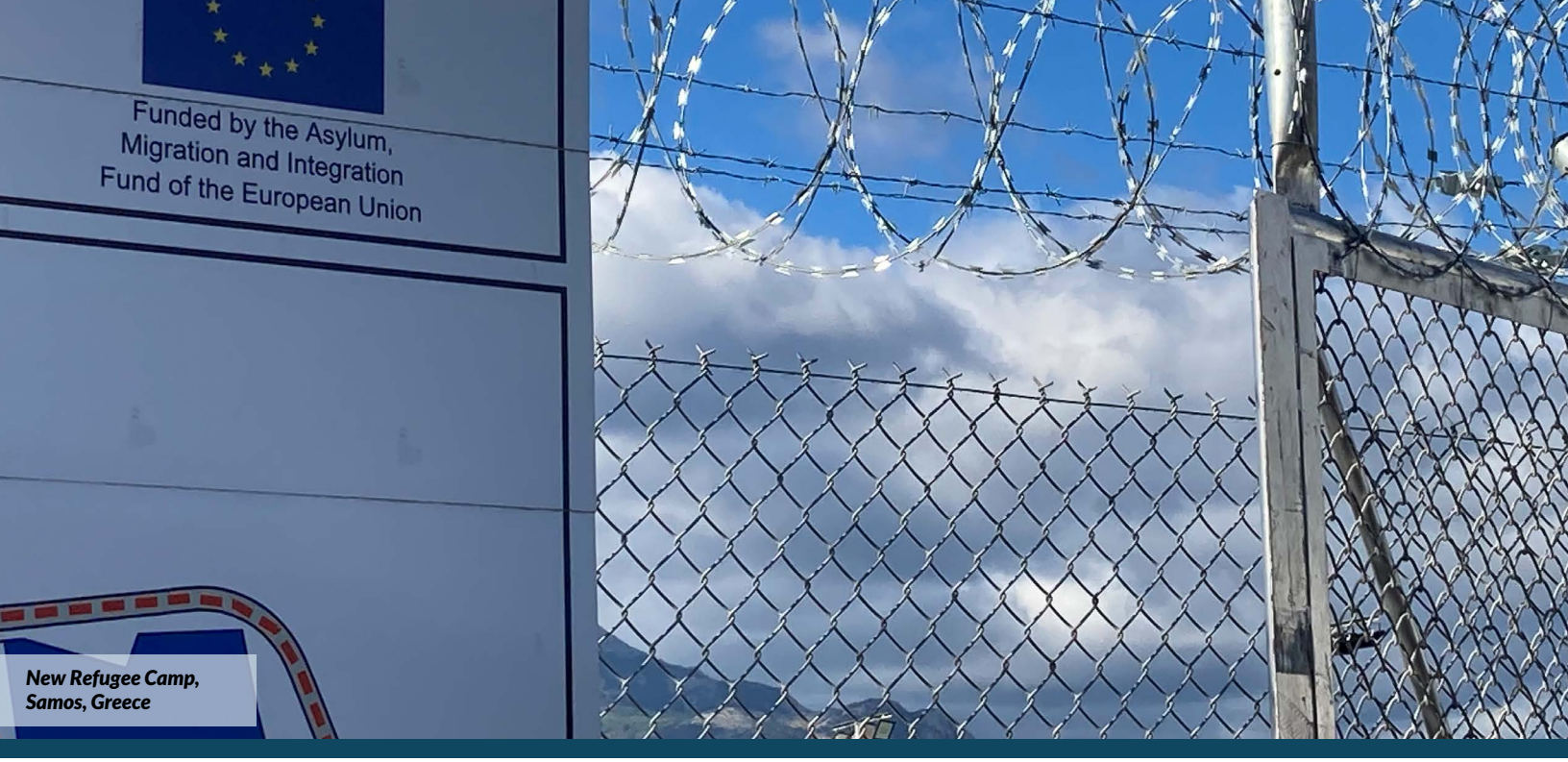
Our consultation participants and civil society organizations flagged growing concerns around data privacy and due process risks, particularly in contexts where data-sharing agreements with foreign powers (such as the United States) are not transparent or subject to judicial oversight.[85]

EUROPE

Europe's technological turn in migration governance reflects a growing preference for automated enforcement and biometric verification. Our consultation participants raised concerns that these technologies also introduce new risks, including data misuse, overreach, and the normalization of surveillance in contexts where liberty should be protected.[86] Similarly to the United States and Canada, private security firms and technology providers also play a significant role in delivering these systems in Europe, both within the European Union (EU) and in non-EU member states,[87] as well as within the UK. The region continues to refine its asylum and migration framework, particularly under the New Pact on Migration and Asylum.[88] In addition, the proposed Return Regulation[89] expands existing data infrastructures and allows for the use of electronic monitoring.[90] As such, for Europe, balancing technological innovation with legal accountability and human dignity will remain a critical challenge.

In Context: Digitized Immigration Detention

Across Europe, immigration detention practices have increasingly incorporated digital surveillance technologies, both within custodial settings and ATD programs. This shift reflects broader transformations in migration governance, where biometric systems, interoperable databases, and smart infrastructure are central tools of enforcement. While states present these technologies as increasing operational efficiency, they also raise significant concerns regarding legality, transparency, and the protection of fundamental rights.[91]



New Refugee Camp, Samos, Greece

Most European countries operate some form of detention facilities equipped with surveillance technologies and migration management systems. Known variously as removal centers or pre-removal facilities (such as the Centres de Rétention Administrative in France, the Multi-Purpose Reception and Identification Centers in Greece, and the Immigration Removal Centres in the UK), these centers routinely employ CCTV surveillance throughout shared and private areas. Greece has become a test case for the EU's smart detention infrastructure.[92] On the islands of Samos, Lesvos, Chios, Kos, and Leros, the new Closed Controlled Access Centers – which were built with EU funding[93] – incorporate biometric turnstiles, thermal cameras, X-ray scanners, and facial recognition technologies.[94] Residents use microchipped ID cards to enter and exit the refugee camps and their movements are constantly monitored while inside. Our consultation participants, along with scholars and human rights organizations, have raised serious concerns about this transformation of refugee camps into digital detention zones.[95]

Surveillance Technologies and Digital Reporting Tools

ATD and supervised release programs across Europe remain relatively modest in their technological sophistication, although this is beginning to change. The UK stands out as a prominent case in the region, having piloted one of the most expansive and controversial uses of electronic monitoring. In 2022, the Home Office launched a pilot program requiring certain asylum seekers to wear GPS-enabled electronic ankle tags as a condition of release from immigration detention. The pilot formed part of the UK government's broader strategy to deter unauthorized arrivals — especially those arriving by small boats — and to maintain surveillance over individuals deemed a flight risk.[96] Under the program, up to 600 individuals were subjected to 24/7 location tracking, with devices logging their precise movements in real time.[97] This data was transmitted to a centralized database accessible by immigration enforcement officials, forming part of what our consultation participants called – and what scholars and civil society organizations have characterized as – a "digital border" inside the UK with profound psychosocial impacts.[98]

The ankle tags used in the pilot were similar in form and function to those employed in the criminal justice system, reinforcing what scholars have termed the "carceral continuum" in immigration enforcement.[99] Although formally presented as an alternative to confinement, the technologies blurred the boundary between custodial and non-custodial control. Asylum seekers also reported that the tags disrupted their sleep, caused skin irritation, and led to stigmatization in their communities, with some describing the experience as a "type of torture" and explaining that they felt "constantly on edge."[100] Some likened the devices to digital shackles and expressed feelings of criminalization, despite not having been accused of any criminal offence.[101]

The pilot drew widespread criticism from civil society and data protection advocates, as well as our consultation participants. In 2024, the Information Commissioner's Office (ICO) conducted a privacy audit and found that the Home Office had failed to conduct a sufficient Data Protection Impact Assessment (DPIA) prior to launching the scheme.[102] The ICO concluded that the use of constant geolocation tracking lacked adequate legal safeguards and was disproportionate, particularly given the absence of individualized risk assessments.[103] The legal justification for the pilot rested on powers conferred under the Immigration Act 2016 (UK) and the Nationality and Borders Act 2022 (UK), but critics – including the ICO – considered that the deployment of surveillance technologies in this way exceeded the principles of necessity and proportionality under UK data protection law and the European Convention on Human Rights (ECHR)[104] (specifically, Article 8 on the right to privacy).[105]

Alongside human rights concerns, the scheme also raised practical questions. There was no clear evidence that the ankle tags improved compliance or reduced absconding rates, and many of those tagged were already reporting regularly to immigration officials.[106] Civil society organizations — including the Public Law Project, Medical Justice, and Bail for Immigration Detainees — questioned whether the tags were primarily symbolic and used to signal toughness on immigration as opposed to being evidence-based policy tools,[107] especially as even the Home Office itself acknowledged that the tagging did not increase compliance.[108]

In 2024, the High Court of Justice validated these concerns, finding the Home Secretary's use of electronic monitoring to be unlawful in several instances due to failures in considering individual circumstances, not providing adequate reasons for imposing monitoring, and not properly reviewing the necessity and proportionality of continued monitoring.[109] The Court also identified issues with data retention practices and delays in mandated quarterly reviews, highlighting procedural deficiencies and the potential for unlawful interference with rights.[110] These legal challenges have also raised concerns about the lack of procedural safeguards, the risk of disproportionate interference with liberty and privacy, and failures to ensure compliance with data protection laws.

Following the High Court's decision, the Home Office revised its immigration bail guidance[111] to include some additional safeguards, including more explicit guidelines around when digital reporting can be imposed, as well as the need for regular review and variation of electronic monitoring conditions.[112] Our consultation participants highlighted that the recent amendments to the bail guidance remain insufficient because they still permit widespread and routine use of electronic monitoring, which undermines the underlying presumption in favor of liberty through reliance on surveillance-based controls as opposed to genuine community-based alternatives.[113]

In 2021, the UK's Immigration Bail Digital Reporting (IBDR) pilot also introduced a voluntary app and email-based check-in system that allows individuals on immigration bail to acknowledge their bail conditions remotely. Importantly, the IBDR does not rely on biometric data and includes robust consent mechanisms: users must explicitly agree to have their device's GPS location recorded, only at the moment they check in, and this data is stored for a maximum of 90 days. Moreover, declining to share location data does not amount to noncompliance.[114] The system also allows address and contact details to be updated online, reducing the burden of routine in-person reporting. While this reporting format arguably offers a less intrusive alternative, it must be contextualized alongside the UK's broader use of electronic monitoring devices, which remain far more burdensome and resemble surveillance under the guise of "alternatives to detention."

The UK government has also indicated its intention to explore other alternatives, including the use of smartphone-based check-in apps, which use facial recognition or geofencing technology[115] that employs GPS or similar tools to create virtual boundaries that trigger alerts or actions when a tracked device enters or leaves a designated area. Thus, while showing some promising direction, the UK case study highlights the dangers of surveillance and intrusive reporting technologies, a trend which may also be replicated in the EU should similar programs be implemented there.

"It soon became clear that the technology attached to my ankle was pretty glitchy. One time, they came and told me, 'The system says the tag had been tampered with'. They checked my ankle and found nothing wrong. It sent my mind whirring. What had I done to jolt the strap? I suddenly felt anxious to leave the house, in case I knocked it while out somewhere.

I began to move through the world more carefully …

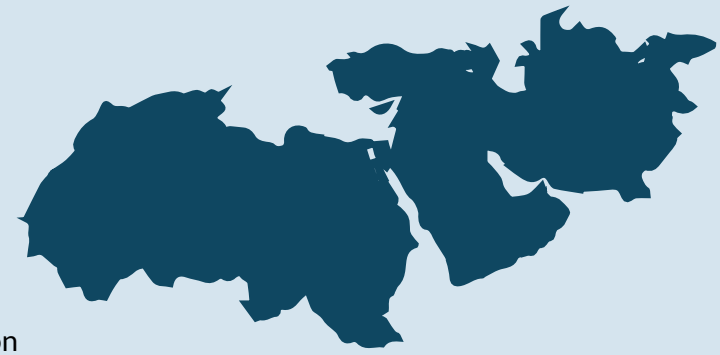
My world contracted, and my mental health went into freefall. I came to realize I wasn't really free: I was in an outside prison. The government knew where I was 24/7. Were they really concerned I would abscond, or did they simply want to intrude on my life?"[116]

-SAM, who came to the UK as a refugee when he was a small child and has lived in Britain ever since. Sam has been subjected to 24/7 surveillance with a GPS ankle tag while facing deportation.

Hebron, Occupied Palestinian Territories

SOUTHWEST ASIA AND NORTH AFRICA (SWANA)

The SWANA region presents a complex terrain of migration governance, shaped by protracted refugee crises, labor migration, and transit routes toward Europe. While contexts vary, from refugee camps in Jordan to deportation centers in the Persian Gulf, technology has become a central tool in managing migration. There is an interplay of humanitarian biometrics led by international organizations and state surveillance infrastructures that facilitate enforcement, expulsion, or restriction. While the use of technology in ATD remains scarce, our consultation participants reported an expansion of mobile self-reporting apps, biometric registration for visa renewals, and data sharing across sectors.



In Context: Humanitarian Biometrics and Their Benefits and Risks

Countries like Jordan, Lebanon, Türkiye, and Iraq have implemented large-scale biometric registration of refugees. This has been facilitated by UNHCR's Biometric Identity Management System that collects fingerprints and iris scans, creating a personalized identity record that underpins aid delivery, protection status, and mobility.[117] Türkiye has issued biometric ID cards to millions of Syrians, collecting fingerprints and demographic data.[118] Its GöçNet database allows instant access to case files and identity records, facilitating legal access but also potentially enabling surveillance and detention.[119] This system, partially funded by the EU,[120] demonstrates how digital identification can both reduce the need for detention but also consolidate state control.[121] The European Center for Not-For-Profit Law also reports that, in 2019, a German security company trained Egyptian security forces on how to use facial recognition technology for border control and security.[122]

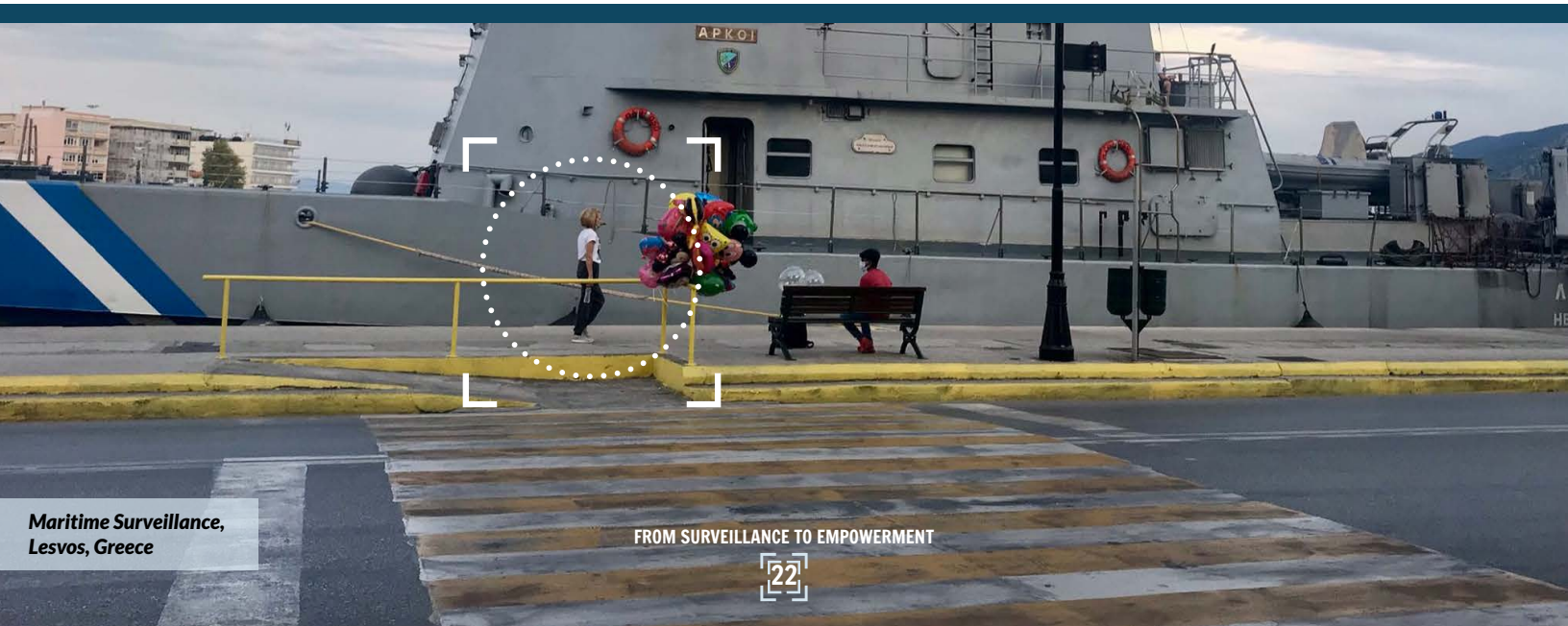
In the Gulf Cooperation Council countries, such as Saudi Arabia, the United Arab Emirates, Qatar, and Bahrain, technology plays a restrictive role, embedded in state surveillance of foreign labor populations. These countries host millions of low-wage temporary foreign workers[123] and operate extensive biometric systems (including mandatory fingerprinting on arrival, biometric residence permits, and facial recognition CCTV in public spaces).[124] The Absher platform, widely used in Saudi Arabia, is equipped with digital immigration controls that include overstay alerts, service restrictions for visa violators, and the tracking of dependents, enabling enforcement without always resorting to detention but greatly expanding surveillance and movement control capabilities.[125] Across the Gulf, private tech firms – often those supplying prison surveillance systems – also contract with immigration authorities, reinforcing the carceral logic behind many digital systems.[126]

North African countries — particularly Libya, Tunisia, and Morocco — are focal points for transit migration toward Europe. In Libya, detention centers are operated either by state forces or armed groups. UNHCR has sought to introduce biometric registration in detention facilities where security allows;[127] in doing so, UNHCR aims to provide detainees with a digital identity that can facilitate release, protection, or resettlement.[128]

Surveillance Technologies and Digital Reporting Tools

Türkiye has introduced a promising and increasingly structured approach to ATD. The Law on Foreigners and International Protection[129] and its amendments set out options for ATD, including (a) residing at a specific address, (b) reporting obligations, (c) family-based return, (d) return counseling, (e) volunteering in public services, (f) financial guarantees, and (g) electronic monitoring.[130] Digital surveillance and reporting can take place through a mobile phone app called Göçbil as well as ankle monitors, with the latter reserved for those who present a high risk to national security (subject to reviews and a 24-month time limit).[131] Ankle monitoring has not yet been implemented but the mobile app has become operational as of summer 2025.[132] Civil society groups – such as Refugee Rights Türkiye and the Turkish Bar Association – continue to reiterate that detention of any kind must be used as a last resort.[133]

In Tunisia, amid EU-funded migration governance discussions, officials have floated proposals to explore the electronic tracking of people awaiting deportation as a way to reduce overcrowding in detention centers. No formal programs have been implemented yet.



Maritime Surveillance, Lesvos, Greece

AFRICAN CONTINENT

The move toward biometric infrastructure, centralized databases, and internationally-funded data collection systems in Africa represents a new phase of migration governance. As explored in our consultations, the use of technology in migration management has accelerated in recent years across the African continent, particularly through partnerships with international organizations and donor governments in the EU. However, the use of digital technologies for detention or ATD remains limited. Our consultation participants explored the interplay of migration management technologies in humanitarian spaces and noted that these tools offer various benefits, such as more efficient aid delivery, identity verification, supporting documentation efforts, and preventing physical detention. However, in some instances, they also raised questions about data security, consent, proportionality, and due process.[134]

In Context: A Continent in Transition

Across the African continent, the use of technology in migration management has accelerated in recent years. Though still under-resourced compared to their Global North counterparts, some African states are beginning to introduce technological tools in detention settings. In South Africa, the Lindela Repatriation Centre – a large immigration detention facility near Johannesburg – uses CCTV monitoring and electronic fingerprinting integrated with the Department of Home Affairs' national database in order to verify detainees' identities and deportation histories.[135] This system has reduced duplication and enabled faster processing, although conditions at Lindela continue to raise human rights concerns.[136] In May 2025, the South African Department of Home Affairs also introduced Operation New Broom, a new biometric data collection and surveillance initiative to arrest, detain, and deport people who are in South Africa irregularly or who have overstayed,[137] illustrating the growing security narrative around immigration detention.

Digital Registration and Verification Tools

While electronic monitoring and tagging are still rare, the African continent is witnessing the growth of digital registration and identity verification tools. For example, Kenya has implemented various smartphone registration and other digital identity programs instead of relying on physical detention and encampment, allowing more people to remain in urban settings and closer to social services.[138]

ASIA PACIFIC REGION

Asia presents a diverse and rapidly evolving landscape in the use of technology for immigration enforcement and detention. From sophisticated biometric systems in East Asia to community-based supervision models in South and Southeast Asia, states across the region are experimenting with varying degrees of digitization, surveillance, and data management in managing mobility. Our consultation participants raised critical questions about privacy, legal safeguards, and the role of international actors in supporting or regulating these systems.

In Context: Surveillance in Migration Control

In South Asia, the use of technology in immigration detention is less advanced but rapidly expanding. Bangladesh, while operating rudimentary detention infrastructure for undocumented people, has led one of the world's largest biometric registration efforts for refugees housed in camps.[139] South Korea also employs comprehensive biometric systems, integrating border control and immigration detention with national databases.[140] All foreign nationals are fingerprinted and photographed upon entry and this data is used to verify identity instantly if someone is detained.[141] For example, at the Hwaseong immigration detention facility, CCTV, motion sensors, and electronic zoning alerts are used to control movement.[142] Civil society has also highlighted the growth of surveillance in Thailand's immigration detention centers, enabling more tracking using CCTV. This includes constant surveillance in the Detention Center for Mothers and Children, surveillance which extends to part of the shower area.[143] Malaysia also detains thousands of undocumented people in immigration depots that often lack adequate infrastructure. Following repeated abuse allegations, the Malaysian government announced plans to digitize detainee records and install CCTV systems in detention depots,[144] as well as plans to digitize its foreign worker program.[145] Malaysia has also experimented with introducing AI-based gait analysis to make determinations about detecting inmate fights or escape attempts in its criminal justice detention facilities.[146]

China's immigration enforcement merges with its broader surveillance infrastructure.[147] Foreign nationals — as well as Chinese citizens — must register their residence, and movement is tracked through a network of CCTV systems, facial recognition software, and police databases.[148] China also employs facial recognition gates at airports and train stations, which automatically flag individuals on immigration watchlists.[149] This reflects the logic of pre-emptive governance, where the state identifies and responds to "threats" through predictive algorithmic systems rather than through reactive detention.[150]

Surveillance Technologies, Digital Reporting Tools, and ATD

In 2023, Japan amended its Immigration Control and Refugee Recognition Act 1951,[151] introducing "supervisory measures" available for some individuals released from detention into the community on provisional status.[152] Thailand has advanced on community-based ATD through the "Memorandum of Understanding on the Determination of Measures and Approaches Alternative to Detention of Children in Immigration Detention Centers" (MOU-ATD).[153] Caregivers and children have benefited from community ATD such as HOST International's community-based case management program.[154]

AUSTRALIA AND NEW ZEALAND

Australia's immigration enforcement regime is internationally recognized for its hardline approach toward immigration detention and its reliance on private security partnerships. Consultation participants reflected in particular on the technologically intensive systems in detention centers. Concerns were raised about the impact of these systems on detainees' human rights – including privacy violations and infringements on personal dignity and mental health – as well as about oversight and transparency issues. Both onshore detention centers and offshore processing facilities have been testing grounds for surveillance technologies. More recently, the use of such technologies has been expanded to monitor certain non-citizens released into the community, including through GPS ankle monitoring. Australia has, however, made welcome progress in reducing the detention of children for immigration purposes, largely by shifting toward community-based ATD.[155]

New Zealand does not operate dedicated immigration detention centers and has historically maintained publicly-managed facilities overseen by government agencies. However, recent legislative changes may enable the use of electronic monitoring in certain circumstances.

In Context: The Privatization of Detention in Australia

Australia has a long history of privatization in its onshore immigration detention network through engaging private security corporations with experience in managing correctional facilities. In 2024, Secure Journeys, a subsidiary of the Management and Training Corporation, was contracted to take over responsibility from Serco for managing onshore detention centers.[156] These centers employ a surveillance architecture that mirrors prison systems: constant CCTV monitoring, electronic access controls, and biometric identity verification are the norm.

Australia's offshore detention regime on Nauru — and, formerly, on Manus Island (Papua New Guinea) — also incorporates technological control measures. On Manus Island, G4S (and later Broadspectrum/Ferrovial) operated facilities equipped with perimeter CCTV, central watchtowers, and infrared cameras.[157] Electronic roll call systems required detainees to scan their ID cards at checkpoints to confirm their presence.[158] On Nauru, which still hosts a "regional processing centre" in open format, digital control mechanisms include ID cards with barcodes, monitored internet access, and internal surveillance systems.

Another key area of concern raised in the consultations related to the Status Resolution and Assurance Tool (SRAT), which is used to carry out risk assessments for onshore immigration detainees. This algorithmic assessment tool, developed by Serco in partnership with the Department of Home Affairs, has been used since 2015: the risk rating determines whether a person is held in high-security compounds or subjected to physical restraints.[159] The SRAT's design and ongoing refinement have been shaped by Serco, reflecting a broader trend of private sector involvement in the management and technological oversight of immigration detention. Major concerns have been raised about the SRAT's lack of transparency, as detainees are not informed of their risk ratings and have no avenue to review or challenge them. Critics also argue that the tool unduly inflates risk scores, partly because it incorporates behavior inside detention — which

can be shaped by the mental health impacts of detention itself — creating a harmful feedback loop where distress leads to higher risk ratings and more restrictive conditions.[160] Independent experts have also criticized the SRAT's algorithmic design, highlighting that it is not grounded in sound scientific research and is vulnerable to data errors and inaccuracies, with documented cases of incorrect information leading to unnecessarily harsh detention conditions.[161] Despite these flaws, the SRAT continues to be used, with recent figures showing that at least 75 per cent of detainees were rated as a high or extreme risk as of January 2024,[162] raising serious concerns about fairness, accountability, and the consequences of outsourcing such critical decisions to a private corporation.[163]

Surveillance Technologies

The Australian government imposes ankle monitors on certain individuals released from physical immigration detention. This has been enabled by legislation[164] introduced in response to a 2023 decision of the High Court of Australia, which ruled that Australia's long-standing practice of detaining non-citizens indefinitely without a real prospect of removal was unlawful.[165] The new legislation provides for the imposition of various conditions on those released on bridging visas as a result of the High Court's ruling, including curfews, electronic monitoring with ankle bracelets, and reporting requirements. In a subsequent decision in 2024, the High Court ruled that the blanket and mandatory use of curfews and ankle monitoring was unlawful because it violated the principle of the separation of judicial power enshrined in the Australian Constitution.[166] More specifically, the Court reasoned that the imposition of the conditions in this manner constituted punishment, which – under Australia's constitutional arrangements – can only be imposed by the courts, not the executive. The Australian government responded by introducing legislative amendments that limit the mandatory imposition of conditions to cases where the responsible Minister is satisfied, firstly, that the person in question poses a substantial risk to the Australian community and, secondly, that the conditions are reasonably necessary and appropriate in the circumstances.[167] As of May 2024, 76 individuals remained subject to electronic monitoring.[168] The Australian government has also confirmed that it has been using drones to track some of those released from immigration detention.[169]

While the government maintains that these surveillance technologies are required to ensure public safety, our consultation participants noted that they often replicate the same coercive dynamics of detention. Key concerns included the stigmatizing effects of visible ankle devices, which impede employment and social integration, and the psychological toll of constant surveillance, including the constant fear of criminal sanctions for minor breaches like being late home or not recharging the device.

In 2025, the New Zealand government also introduced legislation providing for the electronic tagging of non-citizens who have been deemed to pose a security or absconding risk,[170] sparking fears from scholars and civil society about the psychosocial impacts of such surveillance and about the growing influence of the private sector in carceral spaces.[171]

"It is such a relief to have the monitor and curfew taken off. But I still feel broken. I sleep during the day and at night the trauma kicks in. I still have pain in my leg from the monitor. We all have to face hard things in life but this is mentally crushing."[172]

- **RVJB**, who has lived as a permanent resident in Australia since he was a child, reflecting on the debilitating impacts of ankle bracelet technology.

Graffiti in Old Refugee Camp, Samos, Greece

KEY RISKS AND GUIDING PRINCIPLES

This section builds on the above mapping and the real-world use of digital technology in ATD and surveillance programs to identify key risks and to outline cross-cutting guiding principles for addressing them. The principles provide a framework for deploying technology in ATD programs in a way that preserves the rights and dignity of individuals and that facilitates the use of ATD as a genuine alternative to closed and restrictive detention practices. These principles build upon IDC's ATD principles,[173] which are reinterpreted to respond to the specific challenges and dynamics of emerging digital technologies. The references in this section to technological tools that restrict liberty capture both surveillance technologies and digital reporting tools. However, it is important to note that surveillance technologies will generally not meet the requirements set out in the guiding principles. Moreover, given the fact that surveillance technologies can amount to alternate forms of detention, they should not be used in ATD programs.

IMPACT ON HUMAN RIGHTS

The use of technology in the context of ATD can have profound impacts on the ability of people to exercise their human rights and safeguard their dignity. This is particularly the case with surveillance technologies and overly intrusive digital reporting tools, which are better characterized as alternative forms of detention rather than as ATD. An overview of the key human rights standards that are relevant in the context of using technology in ATD and surveillance programs can be found in the Appendix.

GUIDING PRINCIPLE 1:

Prioritize, Respect, and Advance Human Rights

Technological tools used in ATD must be designed and implemented in full accordance with international human rights standards. They must prioritize the liberty, dignity, privacy, and autonomy of individuals over coercion and surveillance.

EXPANDED DIGITAL FORMS OF DETENTION

Digital surveillance tools are increasingly deployed under the rhetoric of "humane" migration management. However, technologies like ankle monitors, smartphone monitoring apps, and overly intrusive automated biometric check-in systems may constitute a form of de facto detention or "technologically mediated confinement" that blurs the boundary between freedom and restriction. While these mechanisms lack bars or physical walls, they reproduce the structures of carceral control, particularly when accompanied by punitive consequences for non-compliance.

In the United States, the widespread adoption of BI Incorporated's SmartLINK app and GPS monitoring tools under ICE's ATD program exemplifies this shift. The SmartLINK app, used to track location and verify identity through facial recognition, is not merely a compliance tool. It creates an omnipresent gaze, shaping behavior and limiting autonomy as well as having a negative impact on the social integration of non-citizens under supervision.[174] The use of electronic ankle monitors in the UK has been described as imposing "digital shackles" and as "e-incarceration." In Australia, individuals subjected to ankle monitoring have called the experience "mentally crushing."[175]

GUIDING PRINCIPLE 2:

No Deprivation of Liberty

Technological tools used in ATD must not amount to a deprivation of liberty, either individually or cumulatively (whether alongside other surveillance technologies, digital reporting tools, or non-tech compliance requirements). This would amount to de facto – or alternate forms of – detention.

Community Center for people on the move in Belgium

One of the most pressing risks associated with the use of surveillance technologies and overly intrusive digital reporting tools is the phenomenon of "net-widening," where — rather than reducing the use of detention — technologies expand the reach of immigration control to individuals who otherwise would have been released without conditions. The expansion of electronic monitoring, biometric surveillance, and algorithmic risk assessments often serves to reclassify low-risk individuals as subjects of control, creating new forms of coercion outside traditional detention.[176] Tools such as GPS ankle monitors, smartphone tracking apps, and biometric check-ins are increasingly being deployed against families, and others who have no history of absconding and who do not present a security risk. The use of technologies for continuous, real-time tracking creates new forms of coercion and digital control, amounting to de facto detention and raising serious human rights concerns. This shift undermines the core human rights rationale for ATD by replacing freedom with "freedom under surveillance," creating a digital surveillance net that may capture those who would never have been detained in the first place.

Digital reporting tools — such as telephone reporting and smartphone-based check-ins — can reduce intrusive oversight, but only if designed with flexibility and without biometric or real-time tracking. As seen in the UK's IBDR pilot project, where digital reporting is used, it should prioritize affirmative, context-bound consent, avoid biometric or continuous tracking, and remain strictly voluntary, offering — rather than enforcing — less intrusive means of compliance. However, even with these safeguards, these tools risk becoming overly burdensome or punitive if implemented with rigid or surveillance-like features.

GUIDING PRINCIPLE 3:

Reduce, Rather than Expand, Detention

Technological tools must only be deployed in ATD where they enable people at risk of or in detention to live freely in the community. The use of technology should be non-intrusive and supportive, not punitive or coercive. Approaches that replicate or run parallel to existing immigration detention systems without helping to reduce the use of detention, or that impose continuous or unnecessary monitoring, do not constitute true ATD.

A core challenge lies in the lack of transparent decision-making criteria for imposing digital surveillance and reporting measures, which are often applied as a result of blanket policies without individualized risk assessments. In the UK, the High Court of Justice ruled in ADL v. Secretary of State for the Home Department[177] that the GPS tagging of migrants on immigration bail violated Article 8 of the ECHR because the measure was applied automatically and without case-specific evaluations of necessity or proportionality. The Court also highlighted the Home Office's failure to conduct mandatory quarterly reviews of monitoring conditions. This "set-and-forget" approach allows surveillance and reporting measures to persist indefinitely, even when initial justifications (for example, being a flight risk) no longer apply, creating a system of open-ended punishment disconnected from objective threats.

The punitive nature of, and stigma associated with, wearable electronic monitoring devices can also visually associate people with criminality, reinforcing harmful stereotypes and perceptions. These forms of surveillance technology are unlikely to meet the principles of necessity and proportionality, which require the use of the least restrictive measures appropriate to each individual case.[178] In some circumstances, electronic monitoring may lead states to breach their human rights obligations. For example, electronic monitoring may amount to inhuman or degrading treatment when the device causes physical discomfort or psychological harm or when it exacerbates trauma, particularly for individuals with existing vulnerabilities. It may also infringe on the right to privacy and family life if the technology imposes restrictions that interfere with daily activities or exposes sensitive personal information. Continuous electronic monitoring may function as a form of de facto detention, undermining the right to liberty by confining individuals to a specific location for extended periods of time.[179]

GUIDING PRINCIPLE 4:

Proportionate and Necessary

Technological tools that restrict liberty should be used only when there is a clear and specific lawful basis to do so, and only when absolutely necessary, following a careful, individualized assessment of a person's circumstances. Such measures must be the least intrusive and most rights-compatible option available. They must never be applied as default or blanket solutions, must be strictly limited to what is essential in each case, and must be subjected to proportionality and necessity tests with strict purpose-limitation requirements to ensure that implementation is minimized to the specified and lawful purpose. The implementation of the restrictions must be time-limited, justified, and subject to regular review.

LACK OF TRANSPARENCY AND CONSENT

Another concerning issue with the use of digital technologies in ATD and surveillance programs is the lack of transparency and the erosion of free and informed consent. People affected by technologies that restrict their liberty should be informed about the decision of detention or the ATD measures, as well as about the available mechanisms to challenge the decision and seek a remedy. In order to ensure that digital technologies in ATD programs remain consistent with international human rights standards, these processes need to respect necessary procedural safeguards, including the provision of adequate information on their rights and the duties of the authorities administering ATD in a language the person can understand, access to legal advice, and access to review by an independent body.[180] It is important to emphasize that children can never meaningfully consent to digital technologies.

Yet, many people affected by surveillance technologies and digital reporting tools are neither given opportunities for informed prior consent, nor provided with clear explanations of how surveillance and reporting tools function, what data is collected, who has access to that data, or what rights the person in question retains. This opacity not only undermines trust in legal processes but also violates fundamental principles of due process and data protection.

Canada's pilot program concerning the ReportIn app illustrates this tension. Initially, participants reported that they were unaware of the app's facial recognition capabilities or of how the app determined check-in times.[181] Advocacy efforts also revealed that the app relies on Amazon Web Services.[182] The lack of clarity around data sharing between the CBSA and private vendors points to systemic failures in ensuring informed participation. In the EU, human rights watchdogs have raised similar concerns about systems that collect and store biometric data, often without adequate explanation or the ability to challenge inclusion.[183]

GUIDING PRINCIPLE 5:
Free and Informed Consent

Participation in digital programs that restrict liberty should be based on free and informed consent. Individuals must be fully informed about how digital technology tools work, what data is collected, how long data is stored, what alternatives are available, what rights exist to challenge decisions, and the ability to opt out of participating in digital programs at any point. Individuals must not be penalized for making the choice to opt out.

Reception Center on Kos Island, Greece

LEGAL ACCOUNTABILITY AND OVERSIGHT

Technological surveillance and some digital reporting tools raise serious legal accountability risks. There is a critical lack of transparency about how these technologies operate, the decision-making processes that determine when they should be applied, and how such decisions can be challenged. This lack of transparency has created a human rights vacuum in which people are exposed to surveillance and intrusive reporting requirements without legal clarity or recourse. There are often no mechanisms available to challenge the imposition of surveillance and reporting measures. Where they do exist, individuals can face significant barriers in exercising their rights, including a lack of access to legal and psychosocial support.

Compounding this problem is the fact that many digital surveillance and reporting programs lack independent oversight mechanisms to monitor compliance with relevant human rights obligations. Obligations under international human rights law and international refugee law, as well as regional governance mechanisms like the EU's General Data Protection Regulation (GDPR),[184] are routinely undermined by the involvement of private actors who are not held to the same standards as public authorities. Without independent oversight, these systems operate in legal "gray zones" that disproportionately affect the most vulnerable populations. This accountability vacuum leaves people-on-the-move exposed to disproportionate harms without meaningful recourse, as seen in cases where individuals have faced prolonged GPS tracking despite demonstrating consistent compliance with immigration proceedings.

GUIDING PRINCIPLE 6:
Access to Review and Oversight

Individuals subject to technologies that restrict liberty must have meaningful access to independent oversight and review mechanisms so that they can challenge the imposition of restrictions and have access to legal recourse. This review process should assess whether the decision to restrict liberty was lawfully authorized and was both necessary and proportionate. It should involve specific consideration of the individual's circumstances and vulnerabilities and of the potential harms of the restrictions, including harm to family members. Measures must not only have a basis in law, but the grounding law must also be accessible, foreseeable, and sufficiently precise and must provide safeguards against arbitrariness. Ongoing human rights monitoring should be institutionalized to evaluate the impacts — and to mitigate the harms — of digital tools for the entire life cycle of each tool's development and implementation.

Graffiti in Old Refugee Camp, Samos, Greece

DATAFICATION AND THE RISK OF ALGORITHMIC DISCRIMINATION

The expansion of surveillance technologies and digital reporting tools in immigration systems has normalized the "datafication" of individuals through the collection of vast and often unnecessary biometric and geolocation data, raising acute privacy and consent concerns. Programs like ICE's ISAP in the United States exemplify this trend, deploying GPS-enabled smartwatches, facial recognition apps, and ankle monitors to continuously harvest biometric identifiers, movement patterns, and behavioral data under the guise of administrative efficiency. This datafication operates within a consent vacuum, as people-on-the-move are already vulnerable to coercion and face surveillance as a condition of release, with no meaningful opt-out mechanism.

These risks are compounded by poor safeguards and by documented misuse of biometric data collected in immigration detention, as well as by a lack of transparency around third party contractors who manage the data.[185] This datafication of detention creates additional vulnerabilities, including profit-driven misuse and insufficient accountability for data leaks.

GUIDING PRINCIPLE 7:

Data Minimization and Privacy

Data collected must be strictly limited to what is necessary for a specified, legitimate, and lawful purpose. It also must be anonymized where possible and must be stored securely, with people-on-the-move having clear access rights and data control as well as the right to erasure and the ability to opt out of data collection.

Graffiti in Old Refugee Camp, Samos, Greece

The rise of data-driven technologies in immigration enforcement has introduced new risks related to bias, profiling, and discrimination. People-on-the-move are increasingly subjected to predictive analytics and algorithmic decision-making systems that assess "risk" or "compliance likelihood" based on incomplete, biased, or opaque data sets. These systems — like the EU's iBorderCTRL project, which piloted AI-driven lie detection and risk profiling technologies at border crossings[186] — convert complex human realities into digital abstractions, often leading to decisions that cannot be explained or contested.[187]

In the United States, ICE has used risk classification algorithms in detention and bond decisions and, most recently, in social media scraping.[188] Many of these algorithms reflect embedded racial and nationality-based disparities.[189] Similarly, Australia's SRAT algorithmic risk assessment tool developed in partnership with Serco has been widely criticized for being unscientific, biased, and inaccurate.[190]

These systems not only lack transparency but also violate vital procedural safeguards. Scholars have warned that people-on-the-move have little to no access to the criteria behind risk scores or the ability to challenge automated decisions.[191] The result is a technological system of judgement that mirrors structural racism while distancing responsibility through the supposed objectivity of algorithms. This process of datafication further dehumanizes people-on-the-move, treating them as data points rather than as rights-bearing individuals.[192]

GUIDING PRINCIPLE 8:

Moratorium on Algorithmic Risk Assessments

A precautionary moratorium on algorithmic risk assessments for imposing surveillance technologies should be adopted unless and until demonstrable and ongoing safeguards can ensure transparency, accuracy, the absence of bias and discrimination, and accountability in their design and implementation.

PRIVATIZATION AND PROFIT IN MIGRATION SURVEILLANCE

The privatization of immigration enforcement has extended beyond detention centers into the digital sphere. Corporations now design, implement, and manage technological surveillance that is used to restrict freedom of movement and that features in so-called ATD programs, turning the monitoring of people-on-the-move into a multi-billion-dollar industry.[193] These companies, which often have prior experience in prison and surveillance technologies, shape the infrastructure of digital enforcement with little democratic oversight or public accountability. These carceral markets commodify peoples' lives, turning incarceration into a revenue-generating enterprise.

In the United States, BI Incorporated (a subsidiary of The GEO Group) has become the dominant contractor for ICE's ATD technologies, including SmartLINK and GPS ankle monitoring.[194] These tools are not neutral; they are commercial products developed in an industry that profits from expanding its client base and embedding surveillance deeper into daily life.[195] Similar arrangements exist in the UK with Serco and in Australia with multiple private providers managing community detention and electronic tracking.

Unlike public institutions, private corporations are driven by profitability rather than public interest. This misalignment of values raises serious human rights concerns. Contracts often include per-person payments, performance incentives, and occupancy quotas that undermine efforts to reduce detention or surveillance and that further dehumanize people-on-the-move.[196] Our consultation participants voiced concern — and various human rights organizations have raised alarms — about the unregulated role of the private sector in the development of technologies. Former United Nations Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, E Tendayi Achiume, has also warned against the "digital borders" normalized by the private sector that automate racial profiling and violate privacy rights.[197] Yet, public procurement contracts remain shrouded in secrecy, and people-on-the-move often lack legal mechanisms to challenge how decisions are made.[198] Procurement decisions, however, present an opportunity for transparency, including the release of information concerning whether the technology (or part thereof) is a product or service of a private vendor. If a private vendor is involved, information about that vendor and about the nature of the contractual relationship between the parties should be made public, including such details as the ownership of intellectual property related to the technology, as well as the ownership and custody of, and accountability for, all collected data.

GUIDING PRINCIPLE 9:

Public Interest over Profitability

Any technology used in immigration detention, surveillance, or ATD should be developed, managed, and deployed by governments or NGOs as far as possible. Any outsourcing, whether to NGOs or commercial entities, must adhere to the principles of open and public procurement, be subject to ongoing human rights and data impact assessments, and include safeguards to ensure transparency and accountability.

PHYSICAL AND PSYCHOSOCIAL HARMS OF SURVEILLANCE

While digital surveillance may seem less invasive than incarceration, it produces profound psychological and social harms and it adversely impacts people's physical health and well-being. People-on-the-move under constant digital observation often report anxiety, fear of non-compliance, and social isolation.[199] Technologies such as ankle monitors, smartphone tracking apps, and overly intrusive smartphone check-in apps create a sense of being "always watched," leading to behavioral changes, diminished trust in institutions, and feelings of criminalization, even in the absence of wrongdoing.

For example, individuals in ICE's ATD program have reported that the unpredictability of SmartLINK check-ins leads to interrupted sleep, an inability to work consistently, and a reluctance to participate in community activities.[200] Mothers with young children face added stress, fearing that any missed check-in might result in enforcement action.[201] This form of de facto detention is especially damaging for survivors of trauma — who may experience digital surveillance as a continuation of past coercion and abuse — as well as for community and family members who experience vicarious trauma.[202]

To avoid and mitigate these physical and psychosocial harms of surveillance, it is crucial to reframe the focus of technology away from enforcement and surveillance and toward tools that facilitate engagement and that genuinely support community-based integration and well-being. This shift requires centering the voices and experiences of people-on-the-move, ensuring that digital solutions empower rather than control, and support rather than stigmatize. Co-designing technology with affected individuals is essential for creating systems that are dignified, just, and responsive to real community needs. For example, processes such as audits and the UK's DPIAs should actively involve those with lived experience and their advocates. Engaging with these communities before, during, and after implementation allows evaluation processes to be directly informed by the realities and priorities of those most impacted, leading to more humane and effective technological practices.

GUIDING PRINCIPLE 10:

Engagement not Enforcement

Technology used in the context of ATD should focus on enhancing community-based support, integration, and case resolution and should respect rights. This means moving away from enforcement-focused surveillance that harms, stigmatizes, and criminalizes people-on-the-move to engagement-based approaches. Technology should empower individuals toward a just and fair resolution of their case by facilitating effective case management and holistic community-based support to help people achieve stability, navigate complex systems, and access services. Technology and evaluation processes should also be actively designed or co-designed with people-on-the-move.

Wall of Ritsona Refugee Camp, Greece

FROM PRINCIPLES TO PRACTICE: RETHINKING THE ROLE OF TECHNOLOGY IN ATD

When designed and deployed within a rights-based and community-centered framework, technology can serve as a facilitator of empowerment rather than control. IDC has emphasized that ATD should not simply involve less restrictive forms of detention, but must constitute a genuine shift toward freedom, dignity, rights, and case resolution. This perspective calls for a reorientation: from using technology to enforce compliance toward using it to build trust, to enhance access to legal and other support services, and to support well-being. Technology must be embedded in a broader ecosystem of care, underpinned by transparency and community involvement. Governments and implementing organizations need to move beyond the false binary of detention versus surveillance. Instead, the focus should be on leveraging digital tools to foster justice, empowerment, inclusion, and integration as part of community-centered, rights-based ATD.

Enhancing Access to Legal Advice and Information

One of the most transformative applications of technology in the context of ATD is its capacity to enable informed and meaningful participation in immigration and asylum processes. People-on-the-move — many of whom are navigating unfamiliar legal systems while facing language barriers, limited literacy, and digital exclusion — are particularly vulnerable to missing critical deadlines or misunderstanding their obligations. Legal representation is often one of the strongest predictors of successful case outcomes, yet many people-on-the-move face structural barriers to securing it. Here, technology can play a transformative role in facilitating access to legal advice and information. Secure videoconferencing platforms, online scheduling tools, and encrypted document-sharing systems are increasingly being deployed to bridge the gap between people-on-the-move and legal service providers.[203]

Tools like Mobile Pathways in the United States — a multilingual mobile platform that delivers real-time legal updates, case-specific reminders, and educational content — aim to close this gap by delivering contextualized legal information in ways that are culturally and linguistically accessible.[204] Platforms such as these do more than inform: they reduce the likelihood of missed

court dates, enhance legal literacy, and ultimately improve appearance rates, offering a rights-based alternative to surveillance-focused approaches. In this way, accessible technology becomes a tool of procedural justice, helping people-on-the-move understand and exercise their rights rather than simply complying with enforcement.

Beyond the United States, similar innovations are emerging globally. In some contexts like Mexico, these tools take the form of "legal kiosks" — secure stations located in shelters like the Border Line Crisis Center, or in transit hubs, that allow users to schedule appointments, upload documents, and receive updates in their preferred language.[205] In Colombia, humanitarian organizations have also piloted WhatsApp-based legal guidance channels and mobile legal clinics with local actors like Voices of Venezuela, using offline-capable apps that deliver pre-recorded "know-your-rights" content to asylum seekers in rural or transit areas.[206] These locally designed models underscore the importance of designing for low-connectivity environments, offering offline functionality, visual literacy aids, and voice-guided interfaces. Importantly, these tools are increasingly being co-designed with people-on-the-move, ensuring not only linguistic and cultural relevance, but also trust and usability. Our consultation participants noted — and scholars have argued — that such participatory design is central to shifting ATD technologies away from punitive surveillance and toward empowerment-oriented digital infrastructure.[207] Moving forward, embedding accessibility, community ownership, and legal empowerment into tech solutions will be key to ensuring that digital innovation upholds the human rights of people-on-the-move.

However, the deployment of such technologies must also grapple with persistent digital divides. Many people-on-the-move lack consistent access to mobile data, Wi-Fi, or even basic smartphone hardware.[208] In rural and border regions, connectivity infrastructure may be weak or unreliable, and digital literacy can vary significantly across communities. As a result, simply introducing legal tech is not enough. Successful implementation must be paired with targeted investments in access and inclusion, including the provision of free data plans, community Wi-Fi hubs, and multilingual digital literacy support. Scholars and rights advocates have emphasized that digital legal access must not become a substitute for in-person support when needed but rather serve as an augmenting tool that enhances availability and responsiveness.[209] When thoughtfully implemented, technologies that facilitate access to legal advice and information can be instrumental in building trust in the system, safeguarding due process, and promoting just outcomes for people navigating complex immigration and detention regimes.

Enhancing Case Management and Access to Support Services

Community-based ATD programs prioritize dignity, empowerment, and individualized support, offering a stark contrast to custodial approaches that rely on surveillance or confinement. These models treat people-on-the-move not as enforcement targets but as rights-bearing individuals navigating complex migration systems. In this framework, case management – which includes ongoing assessments, legal orientation, assessment and referrals, trust relationships, access to services, and psychosocial support – is a foundational component.

Countries like Colombia, Ecuador, Uruguay, Belgium, and Thailand have demonstrated that ATD can function in practice. Colombia uses a model based on regularization instead of detention to manage large numbers of people-on-the-move, while Ecuador and Uruguay prohibit immigration detention. Belgium has a specific ATD department and promotes casework management for

people in the community through the Individual Case Management (ICAM) system. Belgium also recently legislated against child immigration detention and promotes government–civil society partnerships on ATD. Thailand has progressed in implementing the MOU-ATD and has released more than 2,000 children from immigration detention, promoting casework models and government–civil society partnerships. Some of these models, while not perfect, emphasize relational support over monitoring and treat people-on-the-move as active participants in their legal processes, not as subjects to be controlled. Such models point to the possibility of designing ATD systems that promote healing, agency, and trust instead of amplifying harm through technological coercion.

Digital technologies can significantly enhance these efforts by facilitating real-time coordination between case managers, service providers, and people-on-the-move. For example, AsylumConnect (recently rebranded as InReach) connects LGBTQI+ asylum seekers across North America to tailored and verified legal, housing, health, and social services, with filters for gender identity, sexual orientation, language, and immigration status.[210] These platforms prioritize anonymity, privacy, and mobile-first design, addressing the specific vulnerabilities of LGBTQI+ asylum seekers who may face stigma or unsafe conditions in traditional shelter systems.

When digital case management tools are embedded within trauma-informed, person-centered, and rights-based models, they become scalable mechanisms for humane migration governance and long-term stability. Platforms such as RefAid – used by over 7,500 NGOs and service providers in Europe and the Americas – offer people geolocated listings of nearby services while allowing aid organizations to update their offerings and availability in real time.[211] Another platform, called boniĝi, monitors human rights conditions in immigration detention facilities around the world.[212] These innovations can enhance consistency, transparency, and accountability across jurisdictions, especially in high-volume migration corridors. However, **digital tools must never replace human relationships**. As our consultation participants repeatedly emphasized, the success of any community-based ATD hinges on trust, casework, cultural competence, individualized screening and assessment, access to services, and continuity of care, elements that technology can support but not replace. Prioritizing user-centered design, multilingual accessibility, and inclusive data practices ensures that digital systems serve the needs of people-on-the-move and that these systems strengthen – not displace – the relational fabric of support networks.

Digital tools in the context of ATD can also play a pivotal role in fostering stability, empowerment, and long-term integration. Many people-on-the-move face substantial barriers to rebuilding their lives in new contexts, including a lack of access to employment, education, healthcare, community networks, and reliable information. Technology can help bridge these gaps. In Spain, for instance, the Comisión Española de Ayuda al Refugiado (CEAR) mobile app offers asylum seekers real-time updates on their legal cases, maps of nearby services, and information on language courses and health resources.[213] By equipping people-on-the-move with tools for self-navigation and informed decision-making, such platforms help reduce dependency on overburdened service providers while increasing autonomy and a sense of belonging in host societies.[214]

Beyond immediate service access, technology that supports case management, access to services, and integration can also help to enhance ATD, not as tools of containment but, rather, as platforms for contribution and flourishing. When people-on-the-move are meaningfully supported with safe housing, food security, education, mental healthcare, and other vital assistance that meets their basic needs, their engagement with legal processes improves and the likelihood of compliance rises significantly.[215] These outcomes challenge dominant narratives that portray people-on-the-

move as risks to be managed and instead position them as agents capable of building meaningful lives and contributing to their communities. When ATD programs include such technologies, they help shift the paradigm from punitive oversight to a human-centered, rights-based, and opportunity-driven model of migration governance.

Participatory and Community-Designed Technology and Evaluation

Rights-respecting use of technology in ATD hinges on its development through participatory, community-led processes. Rather than imposing top-down solutions, participatory design ensures that technologies reflect the lived realities, languages, risks, and preferences of people-on-the-move.[216] As emphasized by groups like the Localization Lab,[217] the Engine Room,[218] and the De|Center,[219] user-led approaches are critical in humanitarian tech contexts as they promote local partnerships, cultural sensitivity, and iterative testing. Participation improves not only usability but also trust and uptake, particularly in communities that have experienced coercive or extractive technologies. Tools designed with and for displaced people have proven more responsive to actual needs than generic case management apps, and they are also embedded in existing mutual aid networks that many people-on-the-move already rely on.

Collaborative design processes — such as partnerships with digital rights organizations — can facilitate independent audits (see, for example, US-based initiatives like the ICEwatch project from the Immigrant Defense Project, or the People Over Papers initiative),[220] participatory ethics reviews, and community-centered safeguards from the development phase onward. Such partnerships have helped refine impact assessments and build trust-based ecosystems in which people-on-the-move understand and can challenge the use of their data. Projects like Migration and Technology Monitor — which work directly with people-on-the-move to interrogate and design technologies — have highlighted the need not only for meaningful consultation processes, but also for shared ownership, transparent governance, and the right to develop technologies for and by affected communities.[221] Refugee-led initiatives like the Skilled Migrant and Refugee Technicians (SMART) project in Indonesia — which upskills refugees in information technology (IT) and provides online knowledge sharing — further highlight the need to support initiatives from the ground up.[222] This shift from "user-centered" to community-controlled design recognizes that people-on-the-move are not passive recipients of innovation, but knowledgeable actors capable of shaping tools in emancipatory ways. In the ATD context, this means embedding feedback mechanisms, rights of redress, multilingual access, and inclusive design from the very start.

There is also an opportunity to involve technologists – particularly those with lived experience of displacement and detention – in participatory design processes. Engaging tech workers as co-creators, not just implementers, ensures that digital tools reflect the values, needs, and rights of the communities they impact. This approach also challenges dominant top-down development models by fostering mutual learning between designers and directly-affected communities.

As digital technologies become embedded in ATD programs, their design and implementation must be governed by robust accountability frameworks. Too often, digital tools are evaluated solely on the basis of efficiency, cost savings, or compliance rates, without assessing their deeper implications for rights, dignity, and outcomes for people-on-the-move. Mechanisms for community feedback should be built into every stage of deployment.[223] The EU Agency for Fundamental Rights (FRA) has emphasized the need for qualitative monitoring of people's experiences with

digital migration management, warning that metrics focused solely on control and containment risk reinforcing systemic inequality.[224]

Through participatory reporting tools for people subject to these technologies, people-on-the-move and NGOs can leverage technology to fill this accountability gap.[225] Ultimately, without transparent and rights-based evaluation, even well-intentioned technologies risk becoming unaccountable tools of exclusion. Embedding accountability to affected communities from the outset ensures that digital tools are not simply efficient but just, equitable, and aligned with the core purpose of ATD: reducing reliance on carceral practices in immigration detention.

When communities are empowered to build, adapt, or reject technological tools, digital interventions are more likely to support dignity, autonomy, rights, access to pathways, and long-term integration — the very goals that ATD programs are meant to advance.

APPENDIX: KEY HUMAN RIGHTS IMPACTED BY DIGITAL ATD AND SURVEILLANCE

1. Privacy and Data Protection

Surveillance technologies and digital reporting tools routinely collect sensitive biometric, locational, and behavioral data, often without meaningful informed consent or legal safeguards governing retention, access, or secondary use. Such practices risk undermining the right to privacy under Article 17 of the ICCPR. While regional and national data protection laws — including the EU's GDPR — are not human rights instruments per se, they play an important role in operationalizing privacy and data rights in the digital age.

2. Equality and Non-Discrimination

Algorithmic tools and surveillance disproportionately affect racialized and marginalized people, reinforcing entrenched inequalities in immigration enforcement. These effects breach states' obligations under Articles 2 and 26 of the ICCPR, which prohibit discrimination on the ground of race, nationality, social origin, or other protected status.

3. Cruel, Inhuman, or Degrading Treatment

Electronic monitoring, unpredictable app check-ins, and constant digital observation can amount to coercive or degrading treatment (whether in isolation or cumulatively), especially for vulnerable individuals like children and trauma survivors. These conditions may contravene Article 7 of the ICCPR as well as protections under the Convention against Torture (CAT),[226] particularly when surveillance mimics punitive or carceral conditions.

4. Mental and Physical Health Impacts

The cumulative psychological toll of surveillance – including stress, anxiety, social withdrawal, and disrupted sleep – has been documented across the use of electronic tagging and monitoring and other surveillance-based programs. These harms may violate the right to health under Article 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR).[227] These harms also call into question the humanitarian framing of tech-based ATD models.

5. Freedom of Movement

Surveillance technologies often constrain physical mobility and instill a fear of enforcement, effectively undermining freedom of movement under Article 12 of the ICCPR. They may also violate Article 31 of the 1951 Refugee Convention, which prohibits the penalization of refugees for their irregular entry or presence. Article 31(2) requires any restrictions on movement to be "necessary." UNHCR Guidelines make it clear that "[a]utomatic, routine or collective measures to restrict the freedom of movement of unlawfully present refugees would be in violation of Article 31(2)."[228]

6. Protection against *Refoulement*

Aggressive surveillance and data collection may deter asylum seekers from accessing protection mechanisms, increasing the risk of *refoulement* in breach of states' obligations under Article 33 of the 1951 Refugee Convention, under international human rights law, and under customary international law. It may also violate the right to seek asylum under Article 14 of the Universal Declaration of Human Rights (UDHR).[229]

7. Freedom of Association, Religion, and Expression

Surveillance chills participation in community, religious, and advocacy activities. People-on-the-move under monitoring may avoid speaking out publicly or attending religious services or community events for fear of triggering enforcement or other harmful consequences. These impacts infringe on rights guaranteed under Articles 18 (freedom of thought, conscience, and religion), 19 (right to hold opinions without interference), and 21 (right of peaceful assembly) of the ICCPR, particularly when surveillance occurs without judicial oversight or the possibility of opting out.

8. Right to Life, Liberty, and Security of Person

Surveillance technology blurs the line between liberty and detention. Ankle monitors, facial recognition software, and unpredictable app-based reporting functionally restrict freedom and increase vulnerability to arbitrary detention – particularly when they are not accompanied by judicial oversight – thereby potentially violating Article 9 of the ICCPR.

9. Right to Family Life

The impacts of surveillance and other digital technologies in immigration detention go far beyond the individual, affecting families and communities and compounding trauma and stigmatization. Surveillance technologies raise serious human rights concerns under Articles 9 (protection against arbitrary detention), 17 (right to privacy), and 23 (protection of the family) of the ICCPR, and under Article 8 of the ECHR (right to respect for private and family life).

10. The Best Interests of the Child

The detention of children for immigration purposes is prohibited under international law. The Joint General Comment No 4 of the Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families and No 23 of the Committee on the Rights of the Child (2017)[230] made clear that detaining children because of their or their parents' migration status constitutes a child rights violation and always contravenes the principle of the best interests of the child (Articles 3 and 37 of the CRC).[231] Unlike other contexts where detention of children may be permissible as a "last resort" (such as juvenile criminal justice), no circumstances justify the immigration detention of children. Subjecting children to surveillance technologies violates Article 37 (prohibition of arbitrary detention) and, in some circumstances, Article 9 (right not to be separated from their parents against their will) of the CRC, resulting in rights violations that persist long after physical release through digital containment and persistent family disruption.

11. Procedural Justice and Accountability

Surveillance technologies and digital reporting tools often lack clear mechanisms for individuals to understand, challenge, or seek redress against decisions that affect their liberty and fundamental rights. The use of proprietary or opaque algorithms to determine risk scores, compliance statuses, or enforcement actions makes it difficult for affected persons to know how or why decisions are made. Those subjected to surveillance often have no effective means to challenge decisions, correct data errors, or obtain legal recourse, particularly if discrepancies or wrongful enforcement occur. This lack of accountability is compounded by outsourcing to private companies, which further blurs the lines of accountability and hinders independent oversight.

These shortcomings contravene rights enshrined in Article 14 of the ICCPR (right to a fair and public hearing), Article 13 of the ECHR (right to an effective remedy), and Article 8 of the UDHR (also recognizing the right to an effective remedy).

ENDNOTES

1. This composite case study is drawn from several experiences faced by real people as told to the authors in various immigration detention settings. Rather than describing one individual or event, a composite case study synthesizes details such as experiences, patterns, or challenges from several sources to illustrate broader trends or systemic issues. This approach is especially useful in sensitive contexts (like immigration detention) where protecting anonymity is crucial. By blending multiple lived realities, a composite case can offer deep insight into common dynamics while avoiding the ethical risks of identifying specific individuals. In this way, a composite case preserves confidentiality, conveys complexity, and highlights recurring structural harms. See, e.g., Stephanie J. Silverman and Petra Molnar, "Everyday Injustices: Barriers to Access to Justice for Immigration Detainees in Canada," *Refugee Survey Quarterly* 35, no. 1 (2016): 109–27, https://doi.org/10.1093/rsq/hdv016.

2. See, e.g., Lidé Labs, "When and Where Are People Held in Immigration Detention?," International Detention Coalition, published Feb. 2, 2024, https://idcoalition.org/idc_faqs/when-and-where-are-people-held-in-immigration-detention/.

3. Lorna McGregor, *Detention and Its Alternatives under International Law* (Oxford University Press, 2023), https://doi.org/10.1093/oso/9780198866237.001.0001.

4. See, e.g., Mark Yin, "Privatisation and Accountability in Australian Immigration Detention: A Case of State–Corporate Symbiosis," *Punishment & Society* 25, no. 4 (2023): 1119–37, https://doi.org/10.1177/14624745221135175.

5. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

6. Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

7. Convention Relating to the Status of Refugees, Jul. 28, 1951, 189 U.N.T.S. 137.

8. See, e.g., Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families (CMW), *General Comment No. 5 (2021) on Migrants' Rights to Liberty and Freedom from Arbitrary Detention and Their Connection with Other Human Rights*, U.N. Doc. CMW/C/GC/5 (Jul. 21, 2022), paras. 16–17, 24, 38, 46–50, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-5-2021-migrants-rights-liberty.

9. See, e.g., Human Rights Council, *Report of the Working Group on Arbitrary Detention*, U.N. Doc. A/HRC/39/45 (Jul. 2, 2018), annex, para. 12, https://documents.un.org/doc/undoc/gen/g18/196/69/pdf/g1819669.pdf.

10. See, e.g., CMW and Committee on the Rights of the Child (CRC), *Joint General Comment No. 4 (2017) of the Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families and No. 23 (2017) of the Committee on the Rights of the Child on State Obligations regarding the Human Rights of Children in the Context of International Migration in Countries of Origin, Transit, Destination and Return*, U.N. Doc. CMW/C/GC/4–CRC/C/GC/23 (Nov. 16, 2017), para. 10, https://documents.un.org/doc/undoc/gen/g17/343/65/pdf/g1734365.pdf; CMW, *General Comment No. 5*, paras. 39–44.

11. G.A. Res. 73/195, Global Compact for Safe, Orderly and Regular Migration (Jan. 11, 2019), annex, para. 29 (Objective 13), https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_73_195.pdf. See also *Report of the United Nations High Commissioner for Refugees*, U.N. Doc. A/73/12 (Part II) (Sep. 13, 2018), para. 60, https://www.unhcr.org/au/media/report-united-nations-high-commissioner-refugees-part-ii-global-compact-refugees. These materials also stress that immigration detention be used as a last resort, call on states to end child immigration detention, and emphasize the importance of promoting alternatives to detention (ATD).

12. Alice Edwards, *Back to Basics: The Right to Liberty and Security of Person and "Alternatives to Detention" of Refugees, Asylum-Seekers, Stateless Persons and Other Migrants* (Office of the United Nations High Commissioner for Refugees (UNHCR), Legal and Protection Policy Research Series, Doc. PPLA/2011/01.Rev.1, Apr. 2011), https://www.refworld.org/reference/lpprs/unhcr/2011/en/79032; Robyn Sampson et al., *There Are Alternatives: A Handbook for Preventing Unnecessary Immigration Detention*, rev. ed. (International Detention Coalition, 2015), 7–15, https://idcoalition.org/wp-content/uploads/2016/01/There-Are-Alternatives-2015.pdf.

13. See, e.g., CMW, *General Comment No. 5*, paras. 3, 6–7.

14. Julie M. Linton et al., "Detention of Immigrant Children," *Pediatrics* 139, no. 5 (2017): e20170483, https://doi.org/10.1542/peds.2017-0483.

15. Melissa Phillips and Carolina Gottardo, "Deconstructing the Myth of the Need for Immigration Detention," in *Handbook of Critical Whiteness: Deconstructing Dominant Discourses across Disciplines*, ed. Jioji Ravulo et al. (Springer Nature, 2024), https://doi.org/10.1007/978-981-97-5085-6_49. See also *Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement: Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, E. Tendayi Achiume*, U.N. Doc. A/HRC/48/76 (Dec. 17, 2021), https://www.ohchr.org/en/documents/thematic-reports/ahrc4876-racial-and-xenophobic-discrimination-and-use-digital; Achille Mbembe, "Necropolitics," in *Foucault in an Age of Terror*, ed. Stephen Morton and Stephen Bygrave (Palgrave Macmillan, 2008), https://doi.org/10.1057/9780230584334_9.

16. See, e.g., World Health Organization (WHO), *Addressing the Health Challenges in Immigration Detention, and Alternatives to Detention: A Country Implementation Guide* (WHO Regional Office for Europe, May 4, 2022), 13–24, https://www.who.int/europe/publications/i/item/9789289057929; Mary Bosworth and Sarah Turnbull, "Immigration Detention, Punishment and the Criminalization of Migration," in *The Routledge Handbook on Crime and International Migration*, ed. Sharon Pickering and Julie Ham (Routledge, 2015), 173, 185–86, https://doi.org/10.4324/9780203385562-7.

17. Bosworth and Turnbull, "Immigration Detention," 170–73, 181–82, 184–87.

18. Phillips and Gottardo, "Deconstructing the Myth," 1141, 1144–45, 1149; Lucy Mayblin et al., "Necropolitics and the Slow Violence of the Everyday: Asylum Seeker Welfare in the Postcolonial Present," *Sociology* 54, no. 1 (2019): 108, https://doi.org/10.1177/0038038519862124. See also *Report of the Special Rapporteur, E. Tendayi Achiume*, para. 49.

19. See, e.g., Dasha Pruss et al., "Prediction And Punishment: Critical Report on Carceral AI," unpublished manuscript, Nov. 1, 2024, http://dx.doi.org/10.2139/ssrn.5017321; Shahram Khosravi, "Stolen Time," *Radical Philosophy*, Dec. 2018, https://www.radicalphilosophy.com/wp-content/uploads/2018/12/rp203_khosravi.pdf.

20. Sampson et al., *There Are Alternatives*, ii, 7.

21. Ibid., 59–71.

22. NatCen Social Research, "Evaluation of 'Action Access', an Alternatives to Detention Pilot: Report on an Independent Evaluation (March 2019–October 2021)" (UNHCR, Jan. 2022), 2, 54–55, https://www.unhcr.org/sites/default/files/legacy-pdf/61e1709b4.pdf.

23. Eiri Ohtani, "Alternatives to Detention: Building a Culture of Cooperation; Evaluation of Two-Year Engagement-Based Alternative to Immigration Detention Pilot Projects In Bulgaria, Cyprus And Poland" (European Programme for Integration and Migration, Jul. 2020), 32, https://www.epim.info/wp-content/uploads/2020/07/2020-ATD-Evaluation-Report_Final.pdf.

24. Ibid., 54.

25. Edwards, 2011.

26. International Detention Coalition (IDC), "Using Alternatives to Detention (ATD) as a Systems Change Strategy: Towards Ending Immigration Detention" (2022), 6, 7, https://idcoalition.org/wp-content/uploads/2022/01/ATD-Full-Paper-EN.pdf.

27. Sampson et al., There Are Alternatives, 10.

28. Ohtani, "Alternatives to Detention," 3, 17.

29. Sampson et al., *There Are Alternatives*, iii, 1, 76.

30. "Statistics on People in Detention in Australia," Refugee Council of Australia, published Aug. 7, 2025, https://www.refugeecouncil.org.au/detention-australia-statistics/10/. In 2022–23, the average annual cost of holding an individual in immigration detention was AUD$505,176, which equates to just over AUD$1,384/day.

31. Ibid. In 2022–23, the average annual cost of allowing a person to reside in the Australian community on a bridging visa was AUD$2,575, which equates to approximately AUD$7/day.

32. American Immigration Lawyers Association (AILA), "Featured Issue: Immigration Detention and Alternatives to Detention" (AILA Doc. No. 24121300, Mar. 14, 2025), https://www.aila.org/featured-issue-immigration-detention-and-alternatives-to-detention.

33. Department of Homeland Security, "U.S. Immigration and Customs Enforcement: Operations and Support; Fiscal Year 2018; Congressional Justification," (2018), 17, https://www.dhs.gov/sites/default/files/publications/ICE%20FY18%20Budget.pdf. This figure relates to the 2018 fiscal year.

34. Women's Refugee Commission, "Backgrounder: Family Case Management Program" (Apr. 2020), 1, https://www.womensrefugeecommission.org/wp-content/uploads/2020/04/Backgrounder-FCMP.pdf. The Family Case Management Program operated from January 2016 until June 2017.

35. See, e.g., Sampson et al., *There Are Alternatives*, 60–61, 65.

36. Carolina Gottardo and Hannah Cooper, "Digital Technology, Detention and Alternatives," IDC, published Jun. 25, 2024, https://idcoalition.org/digital-technology-detention-and-alternatives/.

37. Ibid.

38. See, e.g., Todd Miller, *Empire of Borders: The Expansion of the U.S. Border around the World* (Verso, 2019), https://www.versobooks.com/en-gb/products/264-empire-of-borders; Petra Molnar, "Surveillance Sovereignty: Migration Management Technologies and the Politics of Privatization," in *Migration, Security, and Resistance: Global and Local Perspectives*, ed. Graham Hudson and Idil Atak (Routledge, 2021), https://doi.org/10.4324/9781003058526.

39. Antony Loewenstein, *The Palestine Laboratory: How Israel Exports the Technology of Occupation around the World* (Verso, 2023); "Gaza: UN Experts Deplore Use of Purported AI to Commit 'Domicide' in Gaza, Call for Reparative Approach to Rebuilding," Office of the High Commissioner for Human Rights, published Apr. 15, 2024, https://www.ohchr.org/en/press-releases/2024/04/gaza-un-experts-deplore-use-purported-ai-commit-domicide-gaza-call.

40. Johana Bhuiyan, "'There's Cameras Everywhere': Testimonies Detail Far-Reaching Surveillance of Uyghurs in China," *The Guardian*, Sep. 30, 2021, https://www.theguardian.com/world/2021/sep/30/uyghur-tribunal-testimony-surveillance-china. See also Darren Byler, *Terror Capitalism: Uyghur Dispossession and Masculinity in a Chinese City* (Duke University Press, 2021), chap. 1; Human Rights Watch (HRW), *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App* (May 2019), https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

41. Lorna McGregor and Petra Molnar, "Digital Border Governance: A Human Rights Based Approach" (Office of the High Commissioner for Human Rights, Sep. 2023), 12, https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf. See also Loewenstein, *The Palestine Laboratory*; Petra Molnar, *The Walls Have Eyes: Surviving Migration in the Age of Artificial Intelligence* (The New Press, 2024), https://thenewpress.org/books/the-walls-have-eyes/?v=eb65bcceaa5f.

42. For an analysis of one of the harmful impacts of the increased use of surveillance infrastructure in the North American migration context, see Samuel Norton Chambers et al., "Mortality, Surveillance and the Tertiary 'Funnel Effect' on the U.S.–Mexico Border: A Geospatial Modeling of the Geography of Deterrence," *Journal of Borderlands Studies* 36, no. 3 (2021): 443–68, https://doi.org/10.1080/08865655.2019.1570861.

43. Transactional Records Access Clearinghouse (TRAC), "Immigration Detention Statistics: A Retrospective and a Look Forward," TRAC Reports, published Feb. 21, 2025, https://tracreports.org/reports/753/. See also Mizue Aizeki et al., *Smart Borders or a Humane World?* (Transnational Institute (TNI) and Immigrant Defense Project's Surveillance, Tech & Immigration Policing Project, 2021), https://www.tni.org/en/publication/smart-borders-or-a-humane-world; Nina Wang et al., *American Dragnet: Data-Driven Deportation in the 21st Century* (Center on Privacy & Technology, Georgetown University, 10 May 2022, updated May 2025), https://americandragnet.org/.

44. See, e.g., Sheera Frenkel and Aaron Krolik, "Trump Taps Palantir to Compile Data on Americans," *New York Times*, May 30, 2025, https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html; Joseph Cox, "This Is Palantir's Justification for Building ICE's Master Database," *404 Media*, Apr. 29, 2025, https://www.404media.co/this-is-palantirs-justification-for-building-ices-master-database/.

45. See, e.g., Adrian Shahbaz, "Trump's Immigration Crackdown Is Built on AI Surveillance and Disregard for Due Process," *Bulletin of the Atomic Scientists*, May 21, 2025, https://thebulletin.org/2025/05/trumps-immigration-crackdown-is-built-on-ai-surveillance-and-disregard-for-due-process/.

46. See, e.g., Petra Molnar, "Trump's Social Media Surveillance: Social Scoring by Another Name," *Tech Policy Press*, Apr. 21, 2025, https://www.techpolicy.press/trumps-social-media-surveillance-social-scoring-by-another-name/; "Automated Tools for Social Media Monitoring Irrevocably Chill Millions of Noncitizens' Expression," Center for Democracy and Technology, published Apr. 15, 2025, https://cdt.org/insights/automated-tools-for-social-media-monitoring-irrevocably-chill-millions-of-noncitizens-expression/.

47. See, e.g., Steve Fisher, "Inside the Windowless Shipping Container Where Analysts Hunt Migrants by Drone," *Los Angeles Times*, Aug. 15, 2025, https://www.latimes.com/world-nation/story/2025-08-15/immigration-border-drone-command-center-mexico-military; Marisa Taylor and Jeffrey Dastin, "Exclusive: Trump Administration Is Pointing Spy Satellites at U.S. Border," *Reuters*, Mar. 28, 2025, https://www.reuters.com/world/us/trump-administration-directs-spy-satellite-agencies-surveil-us-mexico-border-2025-03-27/.

48. See, e.g., "Using AI to Secure the Homeland," Department of Homeland Security, last updated May 28, 2025, https://www.dhs.gov/ai/using-ai-to-secure-the-homeland; Sam Biddle, "Border Patrol Wants Advanced AI to Spy on American Cities," *Intercept*, Jul. 23, 2025, https://theintercept.com/2025/07/23/cbp-border-patrol-ai-surveillance/.

49. Exec. Order No. 14179, 90 C.F.R. 874 (2025).

50. Brenda Isabel Murrugarra Retamozo, "Border Surveillance: Biometric Technologies and Personal Data in Latin American Migration," *Epistemia Revista Científica* 8, no. 2 (2024): 1–16, https://doi.org/10.26495/erc.2820.

51. "Biometric Identification Transnational Migration Alert Program," U.S. Immigration and Customs Enforcement, last updated Mar. 7, 2025, https://www.ice.gov/about-ice/hsi/our-offices/hq/bitmap.

52. For a lucid illustration of the trend of U.S. border externalization in Latin America, see, e.g., Todd Miller, *Empire of Borders*, 1–14.

53. "Alternatives to Detention," U.S. Immigration and Customs Enforcement, last updated Feb. 27, 2025, https://www.ice.gov/features/atd.

54. See, e.g., Johana Bhuiyan, "Vast Immigration Surveillance Program in Dire Need of Reform, Biden Administration Warned," *Guardian*, Feb. 23, 2022, https://www.theguardian.com/us-news/2022/feb/23/us-immigration-isap-surveillance.

55. See, e.g., "The GEO Group Announces Five-Year Contract with U.S. Immigration and Customs Enforcement for Intensive Supervision and Appearance Program (ISAP)," The GEO Group, published Mar. 24, 2020, https://investors.geogroup.com/news-releases/news-release-details/geo-group-announces-five-year-contract-us-immigration-and.

56. Immigration and Customs Enforcement (ICE), *Annual Report: Fiscal Year 2024* (Dec. 19, 2024), 29, https://www.ice.gov/doclib/eoy/iceAnnualReportFY2024.pdf.

57. TRAC, "Immigration Detention Quick Facts," TRAC Reports, last updated Aug. 10, 2025, https://tracreports.org/immigration/quickfacts/.

58. Camilo Montoya-Galvez, "ICE to Test Smartwatch-Like Tracking Devices for Migrants Facing Deportation," *CBS News*, Apr. 24, 2023, https://www.cbsnews.com/news/ice-smartwatch-tracking-device-migrants-deportation/.

59. See, e.g., HRW, *Dismantling Detention: International Alternatives To Detaining Immigrants* (Nov. 2021), 3–5, https://www.hrw.org/report/2021/11/03/dismantling-detention/international-alternatives-detaining-immigrants.

60. See, e.g., Sofía Mejías-Pascoe, "ICE Uses Cellphones to Track Thousands in San Diego, Imperial Counties," *KPBS*, May 25, 2022, https://www.kpbs.org/news/local/2022/05/25/ice-uses-cellphones-to-track-thousands-in-san-diego-imperial-counties.

61. "Alternatives to Detention."

62. Ibid.

63. Jasmine Aguilera, "U.S. Officials Deploy Technology to Track More than 200,000 Immigrants, Triggering a New Privacy Lawsuit," *Time Magazine*, Apr. 18, 2022, https://time.com/6167467/immigrant-tracking-ice-technology-data/.

64. See, e.g., Dayana Maldonado, "The Persistent Harms of the U.S. Immigration Enforcement System," Friends Committee on National Legislation, May 10, 2022, https://www.fcnl.org/updates/2022-05/persistent-harms-us-immigration-enforcement-system; Joel Brown, "Digital Cages: How ICE Uses Digital Surveillance to Track Migrants," *The Brink*, Jan. 26, 2024, https://www.bu.edu/articles/2024/digital-cages-surveillance-to-track-migrants/.

65. AILA, "Featured Issue." This is the projected average daily cost of immigration detention for an adult non-citizen.

66. Tom Hansen et al., "ICE's SmartLINK App Tracks Migrants by the Thousands: Does It Work?," *CBS News*, Jun. 13, 2024, https://www.cbsnews.com/news/does-ices-smartlink-app-work/.

67. Aizeki et al., *Smart Borders*.

68. Women's Refugee Commission, "Backgrounder."

69. Ibid.

70. "Executive Summary: Alternatives to Detention Program," CBSA, last modified Jan. 17, 2019, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/atd-srd-eng.html. See also Joe Bongiorno, "The Electronic Shackling of Migrants," *Maisonneuve*, Jan. 4, 2022, https://maisonneuve.org/article/2022/01/4/electronic-shackling-migrants/.

71. See "Canada: All 10 Provinces to End Immigration Detention in Jails," HRW, Mar. 21, 2024, https://www.hrw.org/news/2024/03/21/canada-all-10-provinces-end-immigration-detention-jails.

72. Patti Sontag, "Migrant Surveillance Data No Longer Has to Remain in Canada: That Has Civil Liberties Advocates Worried," *Investigative Journalism Foundation*, Aug. 7, 2025, https://theijf.org/migrant-surveillance-data-no-longer-has-to-remain-in-canada-that-has-civil-liberties-advocates-worried.

73. Ibid.

74. "Report to the CBSA with the ReportIn Application," CBSA, last modified Nov. 14, 2024, https://www.cbsa-asfc.gc.ca/security-securite/detent/ri-jmp-eng.html.

75. For a use case in the criminal justice context, see George Joseph and Debbie Nathan, "Prisons across the U.S. Are Quietly Building Databases of Incarcerated People's Voice Prints," *Intercept*, Jan. 30, 2019, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus/.

76. Nicholas Keung, "Canada Border Agency Has Launched Facial Recognition App to Track Migrants," *Toronto Star*, Dec. 20, 2024, https://www.thestar.com/news/canada/canada-border-agency-has-launched-facial-recognition-app-to-track-migrants/article_4ddd57ec-bbde-11ef-9f0d-ab0b80692041.html. See also Petra Molnar and Lex Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System* (International Human Rights Program, Faculty of Law, University of Toronto and Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, 2018), https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.

77. Amnesty International, *The Digital Border: Migration, Technology, and Inequality* (2024), https://www.amnesty.org/en/documents/pol40/7772/2024/en/. See also Johana Cabrera-Medina et al., "Crossing Digital Borders: Technology In The Migration Process Across The United States, Mexico, Honduras, and Chile," *Frontiers in Political Science* 6 (2024): 1487769, https://doi.org/10.3389/fpos.2024.1487769.

78. Aizeki et al., *Smart Borders*; Miller, *Empire of Borders*.

79. IDC, *Gaining Ground: Promising Practice to Reduce and End Immigration Detention* (2022), https://idcoalition.org/publications/gaining-ground-promising-practice-to-reduce-end-immigration-detention/.

80. Ibid.

81. Melissa Zumaeta and Lucía Solbes Castro, *Chile* (Case Compass, World Bank Group, 2022), https://www.case-compass.org/files/chile%20(gsl).pdf. See also Organisation for Economic Co-operation and Development (OECD), *OECD Justice Review of Peru: Towards Effective and Transparent Justice Institutions for Inclusive Growth* (2024), https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-justice-review-of-peru_de9fb54d/bb556518-en.pdf.

82. Comité Nacional para la Prevención de la Tortura, *Uso de Videocámaras y Sistemas de Grabación en Lugares de Detención* (Recommendation CNPT 1/21, Mar. 3, 2021), https://cnpt.gob.ar/2022/wp-content/uploads/2022/03/2021_01_Recomendacion-CNPT-1-21-Uso-de-videocamaras-sistemas-de-videovigilancia-y-grabacion-en-lugares-de-detencion.pdf.

83. Ramón Cruz Benzán, "Brazaletes Electrónicos Vigilan los Pasos de Más de 60 Reclusos," *Listin Diario*, Sep. 6, 2022, https://listindiario.com/la-republica/2022/09/06/737449/brazaletes-electronicos-vigilan-los-pasos-de-mas-de-60-reclusos.html.

84. Ibid.

85. Franco Giandana Gigena, "Alerta Migrante: Tus Datos Biométricos Pueden Estar Siendo Intercambiados con EEUU," Access Now, Jan. 10, 2023, https://www.accessnow.org/acuerdos-datos-biometricos-migrantes/.

86. Derya Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe* (Refugee Studies Centre, University of Oxford, 2023), https://www.hertie-school.org/fileadmin/2_Research/1_About_our_research/2_Research_centres/Centre_for_Fundamental_Rights/AFAR/Automating-immigration-and-asylum_Ozkul.pdf.

87. Chris Jones et al., *Europe's Techno-Borders* (Statewatch, Jul. 2023), https://www.statewatch.org/publications/reports-and-books/europe-s-techno-borders/.

88. Directorate-General for Migration and Home Affairs, "Pact on Migration and Asylum: Commission Report Assesses Progress and Next Steps Halfway through Implementation," European Commission, Jun. 11, 2025, https://home-affairs.ec.europa.eu/news/pact-migration-and-asylum-commission-report-assesses-progress-and-next-steps-halfway-through-2025-06-11_en.

89. "Commission Proposes a New Common European System for Returns," European Commission, Mar. 11, 2025, https://ec.europa.eu/commission/presscorner/detail/de/ip_25_724.

90. "New Returns Regulation Ushers in Dystopian Detention and Deportation Regime," Platform for International Cooperation on Undocumented Migrants (PICUM), Mar. 11, 2025, https://picum.org/blog/new-returns-regulation-ushers-in-dystopian-detention-and-deportation-regime/. See also "Proposal for an EU Return Regulation," European Council on Refugees and Exiles (ECRE), Mar. 13, 2025, https://ecre.org/proposal-for-an-eu-return-regulation/.

91. Antonella Napolitano and Hope Barker, "Europe's Digital Border Wars: How the EU's Facilitation Package Is Another Step in Europol's Unjustified Power Expansion," *Oxford Law Blogs*, Jan. 13, 2025, https://blogs.law.ox.ac.uk/border-criminologies-blog/blog-post/2025/01/europes-digital-border-wars-how-eus-facilitation. See also *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis; Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance*, U.N. Doc. A/HRC/44/57 (Jun. 18, 2020), https://docs.un.org/en/A/HRC/44/57; Molnar, *The Walls Have Eyes*.

92. Petra Molnar, *Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up* (European Digital Rights, Nov. 2020), https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf; Molnar, *The Walls Have Eyes*; "Press Release: NGOs on Samos Uncover a Covert Operation against Asylum Seekers and the Invasive Use of Technology in the Samos Closed Controlled Access Centre," I Have Rights, Jan. 21, 2025, https://ihaverights.eu/samos-border-tech/.

93. "Memorandum of Understanding: Commission Support for the Situation on the Greek Islands; Questions and Answers," European Commission, Dec. 3, 2020, https://ec.europa.eu/commission/presscorner/detail/sk/qanda_20_2284. See also Jones et al., *Europe's Techno-Borders*.

94. "Input by Civil Society Organisations to the Asylum Report 2024," European Union Agency for Asylum, Nov. 2023, https://euaa.europa.eu/sites/default/files/2024-02/greek_council_for_refugees.pdf.

95. Agapi Chouzouraki and Anne-Lise Dewulf, *"It Does Not Feel Like Real Life:" Children's Everyday Life in Greek Refugee Camps* (Greek Council For Refugees and Save the Children International, Oct. 2024), https://gcr.gr/wp-content/uploads/Children-in-Greek-refugee-camp-report-online-1.pdf. See also "Over 50 NGOs Pen Eleventh-Hour Open Letter to EU on Human Rights Risks in Migration Pact," PICUM, Dec. 18, 2023, https://picum.org/blog/open-letter-eu-human-rights-risks-migration-pact/; Jones et al., *Europe's Techno-Borders*; Molnar, *The Walls Have Eyes*.

96. Rudy Schulkind et al., *Every Move You Make: The Human Cost of GPS Tagging in the Immigration System* (Bail for Immigration Detainees, Medical Justice, and Public Law Project, Oct. 2022), https://publiclawproject.org.uk/content/uploads/2022/10/GPS_Tagging_Report_Final.pdf. See also "Immigration Bail Conditions: Electronic Monitoring (EM) Expansion Pilot (Accessible)," Home Office (UK), last updated Aug. 27, 2025, https://www.gov.uk/government/publications/offender-management/immigration-bail-conditions-electronic-monitoring-em-expansion-pilot-accessible.

97. "Immigration Bail Conditions."

98. "Stop GPS Tagging Migrants: Fighting the GPS Tagging of Migrants in the UK's 'Hostile Environment'," Privacy International, accessed Sep. 1, 2025, https://privacyinternational.org/campaigns/stop-gps-tagging-migrants. See also Monish Bhatia, "Racial Surveillance and the Mental Health Impacts of Electronic Monitoring on Migrants," *Race & Class* 62, no. 3 (2021): 18–36, https://doi.org/10.1177/0306396820963485.

99. Bhatia, "Racial Surveillance." See also Mary Bosworth, "Inside Immigration Detention," *Journal of Refugee Studies* 29, no. 3 (2016): 425–27, https://doi.org/10.1093/jrs/few003.

100. Rudy Schulkind et al., *Every Move You Make*.

101. Bhatia, "Racial Surveillance." See also Diane Taylor, "Shackles and Restraints Used on Hundreds of Deportees from UK," *Guardian*, Aug. 12, 2019, https://www.theguardian.com/uk-news/2019/aug/11/shackles-and-restraints-used-on-hundreds-of-deportees-from-uk.

102. "ICO Finds the Home Office's Pilot of GPS Electronic Monitoring of Migrants Breached UK Data Protection Law," Information Commissioner's Office (UK) (ICO), Mar. 1, 2024, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/03/ico-finds-the-home-office-s-pilot-of-gps-electronic-monitoring-of-migrants-breached-uk-data-protection-law.

103. Ibid.

104. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.

105. "ICO Finds;" Jo Hynes and Mia Leslie, *"Constantly on Edge:" The Expansion of GPS Tagging and the Rollout of Non-Fitted Devices; Annual Review of GPS Tagging in the Immigration System* (Public Law Project, Dec. 2023), https://publiclawproject.org.uk/resources/constantly-on-edge-annual-review-of-gps-tagging-in-the-immigration-system-2023/.

106. Holly Bancroft, "GPS Tagging of Asylum Seekers Is Ineffective, Government Report Finds," *Independent*, Jan. 13, 2025, https://www.independent.co.uk/news/uk/home-news/gps-tag-asylum-seeker-migrant-home-office-b2678445.html.

107. Rudy Schulkind et al., *Every Move You Make*.

108. "GPS Expansion Pilot Evaluation," Home Office (UK), published Jan. 13, 2025, https://www.gov.uk/government/publications/gps-expansion-pilot-evaluation/gps-expansion-pilot-evaluation.

109. ADL v. Secretary of State for the Home Department [2024] EWHC 994 (Admin), paras. 113, 145.

110. Ibid, para. 158.

111. "Immigration Bail (Accessible)," Home Office (UK), last updated Aug. 27, 2025, https://www.gov.uk/government/publications/offender-management/immigration-bail-accessible.

112. Ibid.

113. Monish Bhatia and Lucie Audibert, "From GPS Tagging to Facial Recognition Watches: Expanding the Surveillance of Migrants in the UK," Institute For Race Relations, Oct. 26, 2022, https://irr.org.uk/article/from-gps-tagging-to-facial-recognition-watches-expanding-the-surveillance-of-migrants-in-the-uk/.

114. "Immigration Bail: Digital Reporting," Home Office (UK), last updated Aug. 13, 2025, https://www.gov.uk/guidance/immigration-bail-digital-reporting.

115. Ibid.

116. Isobel Cockerell, "For Migrants under 24/7 Surveillance, the UK Feels Like 'an Outside Prison'," *Coda*, Sep. 13, 2023, https://www.codastory.com/surveillance-and-control/gps-ankle-tags-uk-migrants-home-office/.

117. "Biometric Identity Management System: Enhancing Registration and Data Management," UNHCR, accessed Sep. 1, 2025, https://www.unhcr.org/media/biometric-identity-management-system.

118. "Türkiye/Syria, 'Place Your Fingerprint Here and Stay Silent, or I Will Detain You and Your Family for a Month': Recent Testimonies on Mass Forced Deportations of Syrian Refugees from Türkiye and Racist Attacks on Them and Their Property following the 'Kayseri Incidents'," Syrians for Truth and Justice, Sep. 10, 2024, https://stj-sy.org/en/turkiye-syria-place-your-fingerprint-here-and-stay-silent-or-i-will-detain-you-and-your-family-for-a-month/.

119. "Verification of the Personal Data of Foreigners under International Protection and Temporary Protection," *Global Compact on Refugees*, accessed Sep. 1, 2025, https://globalcompactrefugees.org/good-practices/verification-personal-data-foreigners-under-international-protection-and-temporary.

120. Melvyn Ingleby et al., "Inside Turkey's EU-Funded Deportation Machine," *New Lines Magazine*, Oct. 12, 2024, https://newlinesmag.com/reportage/inside-turkeys-eu-funded-deportation-machine/.

121. ECRE, *AIDA Country Report on Türkiye: 2023 Update* (Aug. 2, 2024), https://ecre.org/aida-country-report-on-turkiye-2023-update/.

122. Sara Al-Sherif, *Digital Surveillance (Part II): Biometric Surveillance* (European Center for Not-for-Profit Law (ECNL), Jul. 2023), https://ecnl.org/sites/default/files/2023-07/Digital%20surveillance_Biometric%20surveillance_Open%20Rights%20Group.pdf.

123. *Report of the Special Rapporteur on Extreme Poverty and Human Rights on His Mission to Saudi Arabia*, U.N. Doc. A/HRC/35/26/Add.3 (Apr. 28, 2017), https://docs.un.org/en/A/HRC/35/26/Add.3.

124. Abdulla Rasheed, "UAE Develops Biometric Tech to Replace Physical Emirates ID Cards," *Gulf News*, Apr. 16, 2025, https://gulfnews.com/uae/government/uae-develops-biometric-tech-to-replace-physical-emirates-id-cards-1.500095753. See also "Bahrain First in Gulf to Launch Digital Travel-Enabled National ID Cards," *ID Tech Wire*, Mar. 5, 2025, https://idtechwire.com/bahrain-first-in-gulf-to-launch-digital-travel-enabled-national-id-cards/; Cathrin Schaer, "AI-Enhanced Identification: A Danger in the Middle East?," *Deutsche Welle*, Aug. 23, 2023, https://www.dw.com/en/ai-enhanced-identification-a-danger-in-the-middle-east/a-66602156.

125. "Saudi Arabia's Absher App: Controlling Women's Travel While Offering Government Services: Questions and Answers," HRW, published May 6, 2019, https://www.hrw.org/news/2019/05/06/saudi-arabias-absher-app-controlling-womens-travel-while-offering-government.

126. James Shires, "The Implementation of Digital Surveillance Infrastructures in the Gulf," Project on Middle East Political Science, accessed Sep. 1, 2025, https://pomeps.org/the-implementation-of-digital-surveillance-infrastructures-in-the-gulf.

127. "Libya: 'Registration Is a Right for Asylum Seekers and Refugees Wherever They Are'," UNHCR, Nov. 9, 2018, https://www.unhcr.org/blogs/registration-is-a-right-for-refugees/.

128. Ibid.

129. Law No. 6458 on Foreigners and International Protection, *Resmî Gazete* [Official Gazette] No. 28615, Apr. 11, 2013 (Türkiye).

130. Meltem İneli Ciğer, "The EU Support for Alternatives to Immigration Detention in Türkiye: A Curious Case at Odds with EU's External Migration Policy?," *EU Immigration and Asylum Law and Policy Blog*, Jan. 17, 2024, https://eumigrationlawblog.eu/the-eu-support-for-alternatives-to-immigration-detention-in-turkiye-a-curious-case-at-odds-with-eus-external-migration-policy/.

131. Ibid.

132. "A New Measure Is Being Prepared against Irregular Migration: Göçbil," *The Edge Eye*, accessed Sep. 1, 2025, https://theegeeye.com/a-new-measure-is-being-prepared-against-irregular-migration-gocbil/. See also "Düzensiz göçe yeni önlem: GÖÇBİL," *TRT Haber*, accessed Sep. 1, 2025, https://www.trthaber.com/videolar/duzensiz-goce-yeni-onlem-gocbil-74949.html. The app is available for download here: https://play.google.com/store/apps/details?id=tr.gov.goc.mobil&hl=tr&pli=1.

133. See, e.g., "Over 200 Turkish Lawyers Enhance Knowledge on Immigration Detention Standards," Council of Europe Programme Office in Ankara, Dec. 31, 2024, https://www.coe.int/en/web/ankara/-/over-200-turkish-lawyers-enhance-knowledge-on-immigration-detention-standards; Refugee Rights Türkiye, *A Pressing Need: The Lack of Legal Remedy in Challenging Material Conditions of Foreigners under Administrative Detention* (Jan. 2017), https://mhd.org.tr/wp-content/uploads/2025/01/9.-An-Urgent-Need-Judicial-Review-of-Conditions-in-Immigration-Detention-under-Turkiyes-new-Legal-Framework.pdf.

134. *Racial Discrimination and Emerging Digital Technologies*. See also Nanjala Nyabola, *Digital Identities and Border Cultures: The Limits of Technosolutionism in the Management of Human Mobility* (Atlantic Council, 2023), https://www.atlanticcouncil.org/wp-content/uploads/2023/08/Digital-Identities-and-Border-Cultures.pdf.

135. Deputy Chief Justice Moseneke, *Visit to Lindela Repatriation Centre, Krugersdorp* (Constitutional Court of South Africa, Apr. 2014), https://www.concourt.org.za/images/phocadownload/prison_visits/moseneke/Lindela-Report-(Final).pdf. See also Anthony Kaziboni, "The Lindela Repatriation Centre, 1996–2014: Applying Theory to the Practice of Human Rights Violations," *South African Crime Quarterly* 66 (Dec. 2018): 41–52, https://doi.org/10.17159/2413-3108/2018/i66a5623.

136. Lerato Mutsila, "Detention of Undocumented Migrants Should Be a Last Resort, Lawyers for Human Rights Tells Parliament," *Daily Maverick*, Feb. 11, 2025, https://www.dailymaverick.co.za/article/2025-02-11-detention-of-undocumented-migrants-should-be-a-last-resort-lawyers-for-human-rights-tells-parliament/.

137. "Home Affairs Launches Operation New Broom and Biometric Verification to Combat Illegal Immigration," Department of Home Affairs (South Africa), published May 21, 2025, https://www.dha.gov.za/index.php/statements-speeches/1904-home-affairs-launches-operation-new-broom-and-biometric-verification-to-combat-illegal-immigration.

138. "Kenya Court Extends Mobile Device IMEI Registration Ban over Privacy Concerns," Mobile ID World, published Mar. 24, 2025, https://mobileidworld.com/kenya-court-extends-mobile-device-imei-registration-ban-over-privacy-concerns. See also Beth Nyaga, "Prisoners, Border Residents to Benefit from ID Registration Drive, Bitok," *KBC News*, Mar. 13, 2025, https://www.kbc.co.ke/prisoners-border-residents-to-benefit-from-id-registration-drive-bitok/.

139. Shafiur Rahman, "UNHCR Defends Biometric Enrollment Push for Rohingya Refugees," *Diplomat*, Jun. 12, 2025, https://thediplomat.com/2025/06/unhcr-defends-biometric-enrollment-push-for-rohingya-refugees/.

140. "Automated Immigration Clearance Service (SES)," Korea Immigration Service, Ministry of Justice (South Korea), accessed Sep. 1, 2025, https://www.immigration.go.kr/immigration_eng/1859/subview.do.

141. Matthew Fennell, "Korea's Biometric Data Dilemma," Asia Society, Dec. 17, 2021, https://asiasociety.org/korea/koreas-biometric-data-dilemma.

142. "The NHRCK Made Recommendation on Improving Human Rights Situation in Immigration Protection Facilities (Immigration Detention Centers) following the On-Site Investigation," National Human Rights Commission of Korea, published Jul. 25, 2023, https://www.humanrights.go.kr/eng/board/read?boardManagementNo=7003&boardNo=7609366&menuLevel=2&menuNo=114.

143. International Federation for Human Rights (FIDH), *Out of Sight: Human Rights Violations in Thailand's Immigration Detention Centers* (Oct. 2024), https://www.fidh.org/IMG/pdf/out_of_sight_-_human_rights_violations_in_thailand_s_idcs.pdf.

144. Ida Lim, "EAIC Says Advised Immigration Dept to Put CCTVs at Detention Depots," *MalayMail*, Aug. 18, 2016, https://www.malaymail.com/news/malaysia/2016/08/18/eaic-says-advised-immigration-dept-to-put-cctvs-at-detention-depots/1185949. See also Choo Chin Low, "Reforming Malaysia's Deportation Regime: Digitalisation, Integration, and Militarisation," *Journal of International Studies* 20, no. 2 (2024): 65–94, https://doi.org/10.32890/jis2024.20.2.3.

145. Choo Chin Low, "Digitalization of Migration Management in Malaysia: Privatization and the Role of Immigration Service Providers," *Journal of International Migration and Integration* 22, no. 4 (2021): 1599–1627, https://doi.org/10.1007/S12134-021-00809-1.

146. "Malaysia Testing 'Artificial Intelligence' for Prisons," GovInsider, Oct. 30, 2015, https://govinsider.asia/intl-en/article/malaysia-testing-artificial-intelligence-to-monitor-prisoners.

147. Byler, *Terror Capitalism*.

148. Alfred Ng, "How China Uses Facial Recognition to Control Human Behavior," *CNET*, Aug. 11, 2020, https://www.cnet.com/news/politics/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/.

149. Evelyn Cheng, "China Releases Plans to Restrict Facial Recognition Technology," *CNBC*, Aug. 8, 2023, https://www.cnbc.com/2023/08/08/china-releases-plans-to-restrict-facial-recognition-technology.html.

150. See, e.g., Molnar, *The Walls Have Eyes*.

151. Immigration Control and Refugee Recognition Act, No. 319 of 1951, as amended, https://www.japaneselawtranslation.go.jp/en/laws/view/143.

152. Jefferson R. Plantilla, "Japanese Immigration Law in 2023: Changes and Issues," *Focus* 113 (Sep. 2023): 5–8, 15, https://www.hurights.or.jp/archives/focus/section3/2023/09/japanese-immigration-law-in-2023-changes-and-issues.html.

153. Memorandum of Understanding on the Determination of Measures and Approaches Alternative to Detention of Children in Immigration Detention Centers, B.E. 2562, https://asylumaccess.org/wp-content/uploads/2021/04/Eng-Version_MoU_ATD_Final.pdf.

154. Roz Keating and Louise Bloom, *Evaluation Report: Thailand Alternative to Detention Program* (IDC and HOST International, Jun. 2022), https://idcoalition.org/wp-content/uploads/2024/01/HOST-Thai-Evaluation-Report-2022.pdf.

155. As of June 2025, there were no children being held in immigration detention centers, less than five in alternative places of detention, and 33 living in the community under residence determinations: "Immigration Detention and Community Statistics Summary: June 2025," Department of Home Affairs (Australia), Jul. 31, 2025, https://www.homeaffairs.gov.au/research-and-stats/files/immigration-detention-community-statistics-30-june-2025.pdf.

156. Ariel Bogle and Christopher Knaus, "Labor to Pay $2.3Bn to Controversial US Prison Operator Subsidiary to Run Onshore Detention," *Guardian*, Dec. 11, 2024, https://www.theguardian.com/australia-news/2024/dec/11/secure-journeys-onshore-detention-operator-us-prisons-albanese-government-ntwnfb.

157. Behrouz Boochani et al., "Scale of Surveillance in Manus Island Detention Centre Laid Bare," *Guardian*, May 19, 2017, https://www.theguardian.com/australia-news/2017/may/19/scale-of-surveillance-in-manus-island-detention-centre-laid-bare.

158. Simon Taylor, "Incident at the Manus Island Detention Centre from 16 February to 18 February 2014: Submission," Parliament of Australia, 2014, https://www.aph.gov.au/documentstore.ashx?id=8064ead3-8aa9-4923-8a86-71379b58e486&subid=252120.

159. Ariel Bogle, "Revealed: The Secret Algorithm That Controls the Lives of Serco's Immigration Detainees," *Guardian*, Mar. 13, 2024, https://www.theguardian.com/australia-news/ng-interactive/2024/mar/13/serco-australia-immigration-detention-network-srat-tool-risk-rating-ntwnfb-.

160. Niamh Kinchin, "The Risk of Risk: Algorithms and Immigration Detention," *UNSW Law Society Court of Conscience* 18 (2024): 129–35. See also Australian Human Rights Commission, *Use of Force in Immigration Detention* (Oct. 23, 2019), https://humanrights.gov.au/our-work/asylum-seekers-and-refugees/publications/use-force-immigration-detention.

161. Kinchin, "The Risk of Risk." See also Commonwealth Ombudsman, *Immigration Detention Oversight: Review of the Ombudsman's Activities in Overseeing Immigration Detention; January to June 2019* (Feb. 2020), https://www.ombudsman.gov.au/__data/assets/pdf_file/0017/109700/immigration-detention-oversight-report_january-to-june-2019.pdf.

162. Ariel Bogle, "Flawed Immigration Detention Risk Assessment Tool Can't Be Upgraded as ABF Data 'Riddled with Errors'," *Guardian*, May 10, 2024, https://www.theguardian.com/australia-news/article/2024/may/10/flawed-immigration-detention-risk-assessment-tool-cant-be-upgraded-as-abf-data-riddled-with-errors.

163. Ariel Bogle, "Australian Immigration Detainees' Lives Controlled by Secret Rating System Developed by Serco," *Guardian*, Mar. 13, 2024, https://www.theguardian.com/australia-news/2024/mar/12/australian-immigration-detainees-lives-controlled-by-secret-rating-system-developed-by-serco.

164. Migration Amendment (Bridging Visa Conditions) Act 2023 (Australia).

165. NZYQ v. Minister for Immigration, Citizenship and Multicultural Affairs [2023] HCA 37.

166. YBFZ v. Minister for Immigration, Citizenship and Multicultural Affairs [2024] HCA 40.

167. Migration Amendment Act 2024 (Australia).

168. Paul Karp, "Coalition's Ex-Detainee Curfew Amendments Made Regime Unlawful, High Court Told," *Guardian*, May 31, 2024, https://www.theguardian.com/australia-news/article/2024/may/31/coalitions-ex-detainee-curfew-amendments-made-regime-unlawful-high-court-toldin-high-court.

169. Paul Karp, "Drones Used to Track Immigration Detainees Released after High Court Decision, Andrew Giles Reveals," *Guardian*, May 30, 2024, https://www.theguardian.com/australia-news/article/2024/may/30/drones-tracking-released-immigration-detention-detainees-andrew-giles.

170. Immigration (Fiscal Sustainability and System Integrity) Amendment Bill 2025 (New Zealand).

171. Gill Bonnett, "Criminologist Fears Electronic Tagging of Migrants 'Going to Get Huge'," *RNZ News*, Jul. 17, 2025, https://www.rnz.co.nz/news/political/567140/criminologist-fears-electronic-tagging-of-migrants-going-to-get-huge.

172. "Relief for RVJB as Fight Continues against Harsh New Laws for People Freed from Illegal Detention," Asylum Seeker Resource Centre (ASRC), Dec. 22, 2023, https://asrc.org.au/2023/12/22/relief-for-rvjb-as-fight-continues-against-new-laws/.

173. IDC, "Using Alternatives to Detention," 18–20.

174. Surya Mattu, "Meet SmartLINK, the App Tracking Nearly a Quarter Million Immigrants," *Markup*, Jun. 27, 2022, https://themarkup.org/the-breakdown/2022/06/27/meet-smartlink-the-app-tracking-nearly-a-quarter-million-immigrants. See also "The Alternative to Detention Is Freedom, Not Surveillance," American Friends Service Committee, Dec. 9, 2022, https://afsc.org/newsroom/alternative-detention-freedom-not-surveillance-0.

175. "Relief for RVJB."

176. See, e.g., Edwards, *Back to Basics*; Molnar, *The Walls Have Eyes*; Aizeki et al., *Smart Borders*.

177. ADL.

178. See, e.g., Roisin Pillay, *Unlocking Rights: Towards Ending Immigration Detention for Asylum-Seekers and Refugees* (UNHCR, Sep. 2024), https://www.refworld.org/policy/polrec/unhcr/2024/en/148655; UNHCR, *Detention Guidelines: Guidelines on the Applicable Criteria and Standards relating to the Detention of Asylum-Seekers and Alternatives to Detention* (2012), para. 43 (Guideline 5), https://www.unhcr.org/il/wp-content/uploads/sites/6/2020/11/UNHCR-Detention-Guidelines-English.pdf.

179. See, e.g., UNHCR, *Alternatives to Detention: Module 4; ATD Implementation Models* (Nov. 2018), 32, https://www.refworld.org/reference/manuals/unhcr/2018/en/122420.

180. See, e.g., UNHCR, *Detention Guidelines*; CMW, *General Comment No. 5*; Pillay, *Unlocking Rights*.

181. Anja Karadeglija, "CBSA Plans to Use Facial Recognition App to Track Deportations: Documents," *Global News*, Aug. 16, 2024, https://globalnews.ca/news/10701812/cbsa-facial-recognition-app-deportations/.

182. Anja Karadeglija, "CBSA to Use Facial Recognition App for People Facing Deportation Amid Privacy Concerns," *CBC News*, Aug. 16, 2024, https://www.cbc.ca/news/canada/windsor/cbsa-facial-recogntion-app-deportation-1.7296313.

183. See, e.g., Molnar, *Technological Testing Grounds*; Chris Jones et al., *Europe's Techno-Borders*.

184. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J. (L 119) 1 (European Union).

185. See, e.g., Garrett Hazelwood, "Securus Technologies Is Cashing in on Immigrant Detention," *Vice*, Jun. 12, 2020, https://www.vice.com/en/article/securus-technologies-is-cashing-in-on-immigrant-detention/.

186. Ryan Gallagher and Ludovica Jona, "We Tested Europe's New Lie Detector for Travelers and Immediately Triggered a False Positive," *Intercept*, Jul. 26, 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/.

187. See, e.g., Javier Sánchez-Monedero and Lina Dencik, "The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of iBorderCtrl." *Information, Communication & Society* 25, no. 3 (2022): 413–30, https://doi.org/10.1080/1369118x.2020.1792530.

188. Molnar, "Trump's Social Media Surveillance."

189. Robert Koulish and Kate Evans, "Punishing with Impunity: The Legacy of Risk Classification Assessment in Immigration Detention," *Georgetown Immigration Law Journal* 36, no. 1 (2021): 1–72, https://www.law.georgetown.edu/immigration-law-journal/wp-content/uploads/sites/19/2022/01/GT-GILJ210001.pdf.

190. Bogle, "Flawed Immigration Detention Risk Assessment Tool."

191. See *Racial Discrimination and Emerging Digital Technologies*; Molnar and Gill, *Bots at the Gate*.

192. Hope Baker et al., "Why the New Europol Regulation Is a Trojan Horse for Surveillance," *EU Observer*, Feb. 19, 2025, https://euobserver.com/migration/ar62dea65a. See also Molnar, *The Walls Have Eyes*.

193. See Miller, *Empire of Borders*; Todd Miller, "The Digital Border Wall: A Q&A with Journalist Verónica Martínez about the CBP One App," *Border Chronicle*, Apr. 26, 2024, https://www.theborderchronicle.com/p/the-digital-border-wall-a-q-and-a; Molnar, *The Walls Have Eyes*.

194. Department of Homeland Security, *Referrals from Nongovernmental Organizations: Second Quarter, Fiscal Year 2022* (Dec. 28, 2022), https://www.dhs.gov/sites/default/files/2023-03/U.S.%20Immigration%20and%20Customs%20Enforcement%20%28ICE%29%20%E2%80%93%20Referrals%20from%20Nongovernmental%20Organizations%2C%20FY%202022%20Q2_0.pdf.

195. See Molnar, *The Walls Have Eyes*; Miller, "The Digital Border Wall."

196. See, e.g., Eunice Hyunhye Cho, "Unchecked Growth: Private Prison Corporations and Immigration Detention, Three Years into the Biden Administration," American Civil Liberties Union, published Aug. 7, 2023, https://www.aclu.org/documents/unchecked-growth-private-prison-corporations-and-immigration-detention-three-years-into-the-biden-administration.

197. See *Report of the Special Rapporteur, E. Tendayi Achiume*.

198. See Molnar, *The Walls Have Eyes*.

199. See, e.g., Davy Tsz Kit Ng et al., "The Use and Impact of Digital Interventions on Mental Health and Wellbeing of Forced Migrants: A Systematic Review Of Empirical Studies," *Computers in Human Behavior* 172 (Nov. 2025): 108755, https://doi.org/10.1016/j.chb.2025.108755.

200. See, e.g., Ahmed Alrawi, "Immigrants Are Not Felons: A Legal Analysis of Immigrants' Civil Rights Chilling Effect Issues Caused by ICE's SmartLINK App Surveillance," *Journal of Information Policy* 13 (Dec. 2023): 85–113, https://doi.org/10.5325/jinfopoli.13.2023.0007.

201. Isabella Priestley et al., "The Impact of Immigration Detention on Children's Mental Health: Systematic Review," *British Journal of Psychiatry*, ahead of print, Apr. 10, 2025, https://doi.org/10.1192/bjp.2025.29.

202. Bosworth, "Inside Immigration Detention." See also Molnar, *The Walls Have Eyes*.

203. See, e.g., UNHCR Innovation Service, "Taking Innovation Global with Two-Way Communications with Refugees," Medium, published Feb. 27, 2025, https://medium.com/unhcr-innovation-service/taking-innovation-global-with-two-way-communications-with-refugees-8b4d51adef0b.

204. Jeffrey O'Brien, "Mobile Pathways Raises $1m to Transform Immigration Justice via AI," Mobile Pathways, published Feb. 6, 2025, https://www.mobilepathways.org/post/mobile-pathways-raises-1m-to-transform-immigration-justice-with-ai. See also Wang et al., *American Dragnet*.

205. "Our Services," Border Line Crisis Center, accessed Sep. 1, 2025, https://borderlinecrisis.org/servicios.

206. See, e.g., "Voices of Venezuela: Providing a Safe Space for Venezuelan Migrants in Colombia," Turn.io, accessed Sep. 1, 2025, https://www.turn.io/case-studies/voices-of-venezuela.

207. See, e.g., Molnar, *The Walls Have Eyes*. For a discussion of design justice principles more generally, see Sasha Constanza-Chock, *Design Justice: Community-Led Practices to Build the Worlds We Need* (MIT Press, 2020), https://doi.org/10.7551/mitpress/12255.001.0001. See also Afsaneh Rigot and Jessica Fjeld, *Design from the Margins: A Methodology to Deweaponize Our Tech; Discussion Draft* (De|Center, Feb. 2025), https://static1.squarespace.com/static/65c3888a0b958472b053a664/t/67ed8f90065c4360154e4371/1743622035643/discussion+draft+-+methodology+to+de-weaponize+tech+-+for+pub+-+apr+2+update.pdf.

208. Miller, "The Digital Border Wall."

209. See *Racial Discrimination and Emerging Digital Technologies*; Molnar and Gill, *Bots at the Gate*; Dragana Kaurin, *Space and Imagination: Rethinking Refugees' Digital Access* (UNHCR Innovation Service, Apr. 2020), https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Space-and-imagination-rethinking-refugees%E2%80%99-digital-access_WEB042020.pdf.

210. In Reach, "AsylumConnect Rebrands to InReach, Reflecting Growing LGBTQ+ User Base," *PR Newswire*, May 26, 2022, https://www.prnewswire.com/news-releases/asylumconnect-rebrands-to-inreach-reflecting-growing-lgbtq-user-base-301555329.html. See also "InReach: Global," World Justice Project, accessed Sep. 1, 2025, https://worldjusticeproject.org/world-justice-challenge-2022/inreach.

211. The "RefAid" app is available online at: "RefAid: About," RefAid, accessed Sep. 1, 2025, https://refaid.com/.

212. The "boniĝi" app is available online at: "Home: boniĝi," Boniĝi Monitoring, accessed Sep. 1, 2025, https://bonigi-monitoring.com/.

213. Alejandra Acebo et al., *Informe 2025: Las Personas Refugiadas en España y Europa* (Comisión Española de Ayuda al Refugiado, 2025), https://www.cear.es/wp-content/uploads/2025/06/CEAR_XXIII_INFORME_ANUAL_2025.pdf.

214. Ibid.

215. See Sampson et al., *There Are Alternatives*; IDC, "Using Alternatives to Detention."

216. See Rigot and Fjeld, *Design from the Margins*; Constanza-Chock, *Design Justice*.

217. "Home: Localization Lab," Localization Lab, accessed Sep. 1, 2025, https://www.localizationlab.org/.

218. "Homepage: The Engine Room," The Engine Room, accessed Sep. 1, 2025, https://www.theengineroom.org/.

219. "The De|Center | Justice, Human Rights, and Tech," De|Center, accessed Sep. 1, 2025, https://www.de-center.net/.

220. "Immigration Raids: Immigrant Defense Project," Immigrant Defense Project, accessed Sep. 1, 2025, https://www.immigrantdefenseproject.org/raids/; "People over Papers," Padlet, accessed Sep. 1, 2025, https://padlet.com/peopleoverpapers/people-over-papers-anonymous-anonimo-lf0l47ljszbto2uj.

221. The Migration and Technology Monitor is a project incubated and supported by the Refugee Law Laboratory, directed by one of the authors of this report: "Migration and Technology Monitor," Migration and Technology Monitor, accessed Sep. 1, 2025, https://www.migrationtechmonitor.com/.

222. "For Refugees in Jakarta and Medan, Uplifting Others Provides a Sense of Purpose," United Nations in Indonesia, published Feb. 12, 2024, https://indonesia.un.org/en/260363-refugees-jakarta-and-medan-uplifting-others-provides-sense-purpose.

223. See Constanza-Chock, *Design Justice*; Peter Wacnik et al., "Participatory Design: A Systematic Review and Insights for Future Practice," *Design Science* 11 (2025): e21, https://doi.org/10.1017/dsj.2025.10009.

224. "National Monitoring Mechanisms under the EU Pact on Migration and Asylum: Guidance for EU Member States," European Union Agency for Fundamental Rights, published Sep. 19, 2024, https://fra.europa.eu/en/news/2024/national-monitoring-mechanisms-under-eu-pact-migration-and-asylum-guidance-eu-member.

225. See, e.g., Daniel Ghezelbash, "Technology and Countersurveillance: Holding Governments Accountable for Refugee Externalization Policies," *Globalizations*, ahead of print, Mar. 28, 2022, https://doi.org/10.1080/14747731.2022.2051274.

226. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, 1465 U.N.T.S. 85.

227. International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3.

228. UNHCR, *Guidelines on International Protection No. 14: Non-Penalization of Refugees on Account of Their Irregular Entry or Presence and Restrictions on Their Movements in Accordance with Article 31 of the 1951 Convention relating to the Status of Refugees*, U.N. Doc. HCR/GIP/24/14 (Sep. 23, 2024), para. 36, https://www.refworld.org/policy/legalguidance/unhcr/2024/en/148632.

229. G.A. Res. 217A (III), Universal Declaration of Human Rights (Dec. 10, 1948).

230. CMW and CRC, *Joint General Comment No. 4 and No. 23*.

231. Ibid., paras. 5, 7.

From Surveillance to Empowerment: Advancing the Responsible Use of Technology in Alternatives to Detention

Daniel Ghezelbash
Kaldor Centre for International Refugee Law, UNSW Sydney

Petra Molnar
Refugee Law Lab, York University

In collaboration with International Detention Coalition (IDC)

September 2025

Kaldor Centre for International Refugee Law, International Detention Coalition, & Refugee Law Lab

UNSW SYDNEY

UNSW Kaldor Centre for International Refugee Law

refugee law lab

INTERNATIONAL DETENTION COALITION