



An arsenal of Surveillance



February 2026

privacyinternational.org



ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.



Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Photo by Fred Moon on Unsplash

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Table of Contents

Introduction	4
1. Mobile Phone Extraction	6
2. Drones	10
3. Facial Recognition Technology	14
4. Thermographic Cameras	18
5. Algorithmic Surveillance	20
6. IMSI Catchers	25
7. Biometric Scanning	29
8. SOCMINT	33
9. Digital Tracking and GPS Tagging	37
10. Bone and Dental Scanning	40
11. Automated Decision Making	42
12. Language Recognition Software	44
13. Other Technology	46

Introduction

Governments all over the world have been building [arsenals of technology to surveil and monitor migrants, asylum seekers and refugees at borders and within countries](#). By using technology spanning [GPS tagging](#), [social media intelligence \(SOCMINT\)](#), [facial recognition technology \(FRT\)](#), and [artificial intelligence \(AI\)](#); national and supranational immigration authorities have weaponised troves of invasive technologies against people on the move [in the name of 'security'](#) – but at the cost of these individuals' dignity and their rights to privacy, freedom of movement, freedom of expression, due process and myriad other human rights.

Governments are increasingly using this technology to create [data-driven systems](#) that collect and process [invasive](#), and [potentially inaccurate](#), information about migrants. These systems can influence life-changing decisions and [extend surveillance into daily interactions](#), impeding migrants' access to protection, justice, social services, and employment opportunities. Privacy International (PI) investigates and exposes how data and technology are used in the migration context, aiming to help organisations and advocates develop a clear, holistic understanding of the risks and threats migrants face at different stages of their journey.

In 2022, PI circulated a survey to immigration lawyers, advocates, and organisers from around the world, asking about the kinds of technologies they encounter in their practice. This guide is the result of our survey findings and aims to introduce the different technologies that are being used by immigration authorities to surveil and control migrants. We hope that mapping these technologies supports people on the move, and those working to defend migrants at a time when new technology is being ruthlessly deployed with insufficient consideration for human rights.

This list is not exhaustive, but is comprised of some of the most common technologies in use around the world. We expect the use of these and other technologies to become even more prolific as governments continue to enter

into procurement deals with artificial intelligence, defence, and surveillance companies. We need to be prepared.

We would like to acknowledge and thank the following organisations for contributing to this guide, and for their insight, engagement and continued advocacy in this space:

- Duncan Lewis Solicitors
- Carolina Sanchez Boe, Brown University in Paris
- SAMUEL HAVLÍK, ADVOKÁT
- Arthur Cox
- I Have Rights
- Human Rights Law Center
- Asociación Rumiñahui
- Irídia-Center for the defense of human rights
- TEDIC
- PLP
- Statewatch
- Detention Action
- Legal Centre Lesvos



Mobile Phone Extraction (MPE)

What is it?

Mobile phone extraction (MPE) is the seizure of mobile devices, such as those belonging to asylum seekers, journalists or activists, and [using extraction technology to view the contents of the device](#). MPE technology can [enable law enforcement to access deeply private and personal information stored on seized phones](#), such as photos, social media accounts, contact information (i.e., friends and family members they have been interacting with), and a wide range of other data. MPE could even reveal deleted contents and traceable [metadata](#) (i.e., where photos have been taken, who it was sent to, or how a device has been used). In some cases, this granular level of information-gathering from a device as personal as a mobile phone could reveal the journeys a person on the move has taken.

As the survey respondents have raised, intimate data extracted from mobile phones could potentially be shared among international bodies like Frontex, or even with national intelligence services. After all, we have seen large-scale information-exchange frameworks among European bodies such as Eurosur, where Member States can share a variety of surveillance data and real-time border patrol reports.

The highly personal nature of MPE data poses additional risks beyond surveillance. Not only does MPE infringe on individuals' right to privacy and data protection, but it also [strips people on the move of vital access to information on safe routes](#) and [ways to communicate with family and friends](#).

According to our survey, MPE has been deployed for a range of purposes, including to assess applications for protection and other claims for a right to stay/remain, determine their 'risk profile', prosecute individuals for unlawful entry or other immigration offences, [prosecute individuals and groups for people smuggling](#) or other criminal offences, and to [monitor individuals/organisations seeking to provide humanitarian assistance to migrants](#).

What are the risks?

Privacy: Law enforcement or intelligence agencies may extract intimate, personal data from mobile devices, including confidential data such as [journalistic material](#), or other protected categories of data.

Freedom of expression and self-censorship: As people crossing borders become increasingly aware that their phone might be seized, [individuals have begun to moderate or entirely restrict political speech that might be used against them](#).

Informed consent: [Under the Investigatory Powers Act \(2000\)](#), police authorities may extract mobile phone content without permission from individuals if they believe it will assist their investigation. Even if individuals can consent, due to the large repository of information stored by a device, the subjects themselves might not be aware of all the data accessible on their device, [such as deleted messages](#). The power asymmetry between authority and subject could also undermine actual meaningful consent.

Due process: Information extracted from mobile phones has also been increasingly used as a tool to [gather information about applicants](#) in asylum cases. However, this information might be out of context, out of date, or if someone is using a second-hand phone or a shared device, it might even be information associated with someone else entirely, raising serious concerns about the fairness and integrity of decision-making in these processes.

Are corporations involved?

Several private companies are reportedly involved in developing and selling MPE and data forensics technology for migration surveillance, including:

- **Cellebrite:** [Headquartered in Israel](#), the company offers a range of digital forensics tools, including its [Universal Forensic Extraction Device \(UFED\)](#) which, [according to its website](#), enables users to overcome encryption barriers and other locks including deleted content to access a wide range of digital data from smartphones, drones, SD cards, etc.
- **Atos:** [According to reports](#), German authorities have previously relied on [French IT company Atos](#), which further integrates mobile forensic services from Sweden-based [MSAB](#) and Austria-based [T3K-Forensics](#), to extract and analyse mobile phone data during asylum assessments.

Real world examples:

MPE has reportedly been deployed in various countries for the purposes of border control and surveillance, including:

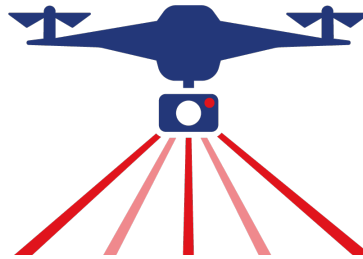
- **UK:** Deployed by [national immigration authorities and national border forces on small boat arrivals](#) in the southern English border. According to a survey respondent, this is also deployed by UK national immigration authorities and national border forces in detention centres to identify an individual's nationality or other characteristic or to determine their 'risk profile', among other reasons.
- **Spain:** According to a survey respondent, MPE has been used [by national immigration authorities, national border forces and police across all borders](#) in Spain, particularly maritime borders such as south of the Iberian Peninsula, the Canary Islands, the Balearic Islands. Used for the purposes of prosecuting people for people smuggling or unlawful entry, or to affect a pushback. Also deployed for in-country surveillance by national immigration authorities, national border forces, police, intelligence agencies and supranational forces (Frontex, Europol, Interpol) in arbitrary arrest scenarios and foreign detention centres for undocumented individuals, as reported in another survey response.
- **The Netherlands:** Deployed by national immigration authorities at

asylum seeker centres and detention centres to [assess applications](#) for protection or other claims for a right to stay or to justify the decision to detain a person, among other reasons.

- **Greece:** Deployed by national border forces and police at the [Aegean Sea border](#) to prosecute people for human trafficking, people smuggling or other criminal offences and to monitor individuals/ organisations seeking to provide humanitarian assistance to migrants. According to a survey respondent, this has also been used by police to monitor if an individual is complying with the conditions to which they were subject.
- **Poland:** Deployed by national officers [against journalists](#) documenting the hazardous border-crossing zone.
- **Germany:** Migration authorities utilise surveillance technology to [extract and analyse data from asylum seekers' smartphones](#).

Read more

- [Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps](#)
- [About Mobile Phone Extraction](#)
- [Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers](#)
- [A technical look at phone extraction](#)
- [What types of data can law enforcement extract from my phone?](#)
- [Privacy International and Article 19 intervention in Nabrdalik v Poland](#)
- [The US border surveillance expansion has global implications](#)
- [Privacy International intervention in R \(HM and MA and KH\) v Secretary of State for the Home Department](#)



Drones

What is it?

[Drones \(or unmanned aerial vehicles, UAV\)](#) are flown remotely by human operators from long distances or according to pre-programmed flight plans. In the [migration surveillance context](#), drones can be mounted with cameras and sensors to monitor border zones or to conduct in-country surveillance. The information gathered by drones enables a quick exchange of information to border or coast guards to intercept people on the move.

National immigration forces and national authorities, as well as intelligence agencies and supranational forces (e.g. Frontex) [reportedly deploy autonomous drones to carry out this invasive aerial surveillance](#). According to our survey findings, these deployments have been used for purposes including: prosecuting people for unlawful entry or other immigration offences, prosecuting people for human trafficking, people smuggling, or other criminal offences, to effect a push-back, and to monitor individuals/organisations seeking to provide humanitarian assistance to migrants.

What are the risks?

Privacy: Drone surveillance can [collect troves of data](#) about people on the move, such as their location, movement patterns and personal data.

Discrimination/profiling: In-country surveillance facilitated by drones has been shown to [target racialised migrant communities](#), raising concerns about discriminatory monitoring and profiling.

Due process: [Autonomous drones](#) can record and [surveil people on the move and their movement patterns](#) without their knowledge. The drones are AI-enabled, and are meant to adapt to changing conditions, and risk infringing upon the right to privacy and freedom of movement. Additionally, studies have found that aerial surveillance does not simply deter crossings, but pushes migrants into more dangerous areas and routes, raising the risk of injury or death.

Asylum: The right to seek asylum is [enshrined in international law](#). [Drones can facilitate pushbacks](#) to stop the movement of refugees and migrants and transport them back across the border, [which violates and frustrates their right to asylum](#). Also, the constant presence of drones overhead [has been reported](#) to induce psychological trauma, leading to feelings of anxiety, paranoia, and a diminished sense of security among affected individuals.

Are corporations involved?

Some private companies are reported to be involved in the development of drone systems, including

- [Indra](#): A Spain-based technology group that provides a range of drone-enabled services like defence and air traffic, including for [‘border protection’ of land and sea borders](#).
- [Elbit](#): Elbit Systems is a [defence technology company based in Israel](#) providing drone surveillance capabilities [for defence purposes](#). [Their UK branch also appears to provide border monitoring and surveillance technologies](#). One of their well-known drone systems is [Hermes](#).
- [Israel Aerospace Industries \(IAI\)](#): Israel-based IAI provides a suite of defence and ‘border protection’ tools, including real-time surveillance and intelligence services via unmanned aerial systems that they have previously marketed for [‘securing your borders from terrorists, smugglers and illegal immigrants’](#). One of their most well-known drones is the [Heron](#).

Real world examples:

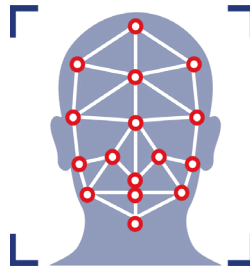
Drones have reportedly been deployed for both border surveillance and in-country surveillance. For example, reports and publicly available sources indicate it has been used in the following:

- **EU-wide:** EU member states [share information](#) among their immigration departments and supranational authorities like Frontex that was obtained through drone surveillance. This exchange is done through the [EUROSUR](#) and [EURODAC](#) databases. [Frontex also reportedly uses IAI's remotely operated Heron drones for aerial surveillance off the coast of Libya](#) to monitor small boat crossings. Frontex's contracting of IAI's Heron drone has been [announced to continue operating in the Mediterranean Sea for another four years](#) from the beginning of 2025.
- **Spain:** Drones have been deployed by national immigration authorities, border forces, police and supranational forces at [borders around Ceuta and Melilla](#), as well as at sea rescue scenarios around the Canary Islands and Andalusia.
- **Brazil-Argentina border:** Drone fleets have reportedly been deployed as part of [Brazil's 'Frenteira Tech' project](#), which 'promotes the use of digital technologies with a focus on public safety'. According to [research from TEDIC](#), these drones fly over the border 24 hours a day along the border with Argentina and are equipped with high-definition cameras for pattern recognition and license plate recognition.
- **Greek-Turkish border:** [Deployed around the Aegean Sea border](#) for a range of purposes including prosecuting people for people smuggling, pushing migrants away from and preventing them from crossing borders (effecting a pushback), search and rescue operations, and monitoring organisations providing humanitarian assistance. Information obtained via drone surveillance shared with Frontex via [Joint Operation Poseidon](#), with Europol via EURODAC.
- **UK:** The UK's Maritime and Coastguard Agency (MCA) had [reportedly signed a £990,000 contract](#) with Elbit Systems to test and develop

its unmanned aerial vehicles for 'coastal surveillance' back in 2020. The contract appears to have been intended for 'various scenarios' including search and rescue and surveillance. The UK is now [reportedly working with French authorities, who are rolling out 'millions of pounds' worth of drone surveillance.](#)

Read more

- [Satellite and aerial surveillance for migration: a tech primer](#)
- [About: Drone Surveillance](#)
- [The UK's Privatised Migration Surveillance Regime: A Rough Guide for Civil Society](#)



Facial Recognition Technology (FRT)

What is it?

[Facial recognition technology \(FRT\)](#) is a technology that recognises faces in images or video, processes that data, and then uses it to record something about the person sometimes in conjunction with other software. FRT can be used to verify, identify, and/or categorise an individual. Using it for verification purposes only involves a one-to-one comparison of two facial images usually presumed to belong to the same individual. When used for identification purposes, however, the system compares the image of an unknown person to a database of “known” faces to establish someone’s identity. FRT can occur live in real-time where an FRT camera captures biometric data in the form of a person’s face image and then processes this data instantly and [compares it to a reference image database](#), for example, a passport or immigration database. FRT could also occur retrospectively, which involves the capturing of individuals’ facial images and processing them at a later stage. For instance, law enforcement might compare and identify an image or other biometric data from a person captured in video footage from CCTV

In the migration context, according to our survey responses FRT has reportedly been used by national immigration authorities and police for a range of purposes, including effecting pushbacks at borders, assessing and determining applications for protection or other claims for a right to stay, to monitoring individuals/ organisations seeking to provide humanitarian assistance to migrants, and supporting prosecutions for unlawful entry or other immigration offences, human trafficking or other criminal offences.

What are the risks?

Privacy: FRT that involves capturing, processing and storing a person's biometric data results in the creation of biometric records into a database that might be held for later/other purposes down the line. It can involve trawling a range of databases [to search for a matching image](#), raising concerns about potential mission creep and the use of biometric data beyond its original purpose.

Mass surveillance and freedom of assembly: Mass, round-the-clock surveillance enabled by FRT [is in tension with individuals' right to freedom of](#)

[assembly](#), as asylum seekers or even other people on the move may not feel safe going to public spaces, events, or social gatherings, effectively creating a chilling effect on their freedom to participate in tension with.

Profiling/discrimination: FRT profiling could risk flagging individuals of certain [racial](#) or demographic groups more than others as ['threats' or 'more likely to commit crimes'](#), raising significant concerns about discriminatory targeting and the reinforcement of existing biases in law enforcement and migration control..

Inaccuracy and misidentification: Similarly, FRT algorithms [could be faulty and result in incorrect identification matches](#), which could contribute further to discriminatory outcomes. Previous research has shown that FRT algorithms exhibited bias and discrimination against certain demographics, [such as higher rates of misidentification of Black or East Asian faces](#), due to the lack of diversity and representation in training data.

Freedom of expression: Mass surveillance enabled by FRT – whether the stage of capturing biometric data or identification – could result in self-censorship and a chilling effect on freedom of expression, [as individuals may refrain from attending public events or spaces where FRT is reportedly present](#).

Are corporations involved?

Some private companies are reported to be involved in the development or provision of FRT technologies for migration surveillance use, such as:

- [Buddi](#): UK-based Buddi provides monitoring technologies for 'criminal justice' (live tracking GPS devices) and 'remote care' (alert clips and wristbands). While the company appears to supply mainly tags and wristband devices, Buddi had previously been reportedly [contracted by the UK Home Office to supply facial recognition smart watches for monitoring migrants](#)
- [G4S](#): G4S is a UK-based security technologies company that provides a range of services including facial recognition for ['identifying persons of interest, recognising known offenders or flagging individuals who do not carry the correct approvals'](#).
- [GEO Group](#): The GEO Group is a U.S.-based company that provides private prison and holding facilities to government bodies like [U.S. Immigration and Customs Enforcement \(ICE\)](#). The company is also reportedly behind the immigration enforcement app [SmartLINK](#).

Real world examples:

FRTs have been deployed at a global scale in places like airports (e.g., e-gate checkpoints), detention centres and across border zones. FRT is also being [increasingly utilised in public spaces by law enforcement](#).

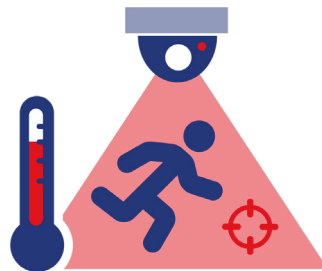
Some cases of FRT deployment include:

- **UK**: Reportedly deployed by national immigration authorities and police in London, such as in Heathrow Immigration Removal Centre (as reported by a survey respondent) and in surveillance of major events and [at airports](#).
- **USA**: Integrated into the [CBP One app](#) for individuals seeking to enter the US from Mexico and further used in other capacities by national immigration authorities and border forces; also reportedly deployed via the [SmartLINK App](#) to monitor newly arrived migrants; and by [ICE agents on mobile phones](#) to identify people and their immigration statuses.

- **Greece:** Allegedly deployed by the Ministry of Migration and national police in the Samos Closed Controlled Access Centre (CCAC) for monitoring and immigration control, as reported to us in our global survey.
- **Paraguay:** Reportedly deployed as part of the [SMARF system in Paraguay](#) in Asunción International Airport (initially deployed in the 'Triple Border Area' of Argentina, Brazil and Paraguay).

Read more:

- [About: Facial Recognition Technology](#)
- [Revealed: "Skyrocketing" scale of UK police's Secret Facial Recognition Searches of Passport and Immigration Databases](#)
- [Latest developments with facial recognition technology in the UK](#)
- [UK government announces tender for live facial recognition technology](#)



Thermographic Cameras

What is it?

[Thermographic cameras](#) capture heat-based images of persons and objects reflecting the infrared radiation they emit. [In the migration context](#), thermal imaging can be used to detect people on the move based on their body heat, which marks the person in a warmer colour (e.g., red) than surrounding backgrounds which reflect cooler tones. This makes it possible to, day or night, obfuscated environment or not, locate humans against their environment. Based on our survey responses, thermographic cameras have been deployed across borders to monitor and control crossings, detect people smuggling, and even effect push-backs.

What are the risks?

Privacy: Thermographic cameras can capture the movement of individuals [even when they are concealed](#), and often without their knowledge. This movement and thermal imaging data constitutes personal data that could [risk exploitation for surveillance purposes](#).

Informed consent: These cameras capture the movement of individuals and might store thermal images of individuals for tracking purposes without their consent.s

Are corporations involved?

Governments have reportedly entered contracts with certain private companies for the procurement of thermographic systems, including:

- [ClearView Communications](#): This UK-based company reportedly provides security services such as [thermal CCTV monitoring](#).
- [Teledyne FLIR](#): A US-based company that develops intelligent imaging technologies for several sectors including public safety and [defence](#). The company's [thermal imaging cameras](#) have been [deployed across the southwestern U.S. border for border security purposes](#)..

Real world examples:

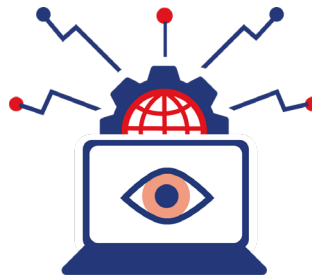
Thermal imaging technology is [typically used in conjunction](#) with other surveillance tools mentioned in this guide, such as drones and FRT.

Countries where thermal imaging is used to track people on the move include:

- **UK**: Use of thermal imaging has been [reported in the past](#) to monitor small boat crossings across the southern English Channel from France.
- **U.S.-Mexico border**: Border agents with the U.S. Department of Homeland Security reportedly utilise thermal camera systems to track migrants crossing through the U.S.-Mexico border. This [thermal camera system](#) allowed border agents to detect individuals in the early hours of the day and through agricultural fields and dense desert brush.

Read more:

- [About: Infrared temperature imaging](#)



Algorithmic Surveillance

What is it?

Algorithmic surveillance pertains to a range of technologies powered by algorithms that can detect, profile, track, or monitor individuals for in-country and [border surveillance](#). Algorithms have also been used to make and inform decisions, [such as to assess immigration cases and recommend case decisions in the UK](#).

Algorithmic surveillance can also be used alongside a range of tools like FRT [and drone surveillance to create an all-encompassing arsenal](#) for monitoring and tracking. In particular, algorithmic tools [integrated with advanced artificial intelligence \(AI\) systems](#) have been increasingly deployed across the EU and the U.S. to facilitate mass and automated surveillance for border control and security.

What are the risks?

Privacy and data protection: [Algorithms require large troves of data for training](#), refinement and even their deployment (i.e., an algorithm for processing immigration decisions). This raises concerns about how algorithms process and store vast amounts of personal and highly sensitive data, such as biometric data used for algorithmic identification and monitoring. Questions arise about how much data is collected (versus what 'needs' to be collected), the types of data collected ([e.g. health data allegedly used in algorithmic recommendations systems](#)), and the length of time data is retained.

Due process: Most algorithmic tools being used in the migration context are

highly secretive. It is unclear the extent to which human officers are involved in the decisions that these tools generate, how they operate, or whether individuals affected can meaningfully contest the outcomes. This opacity raises serious questions about [potential violations of due process rights that migrants are guaranteed under international law](#).

Transparency: There is a [lack of transparency](#) about what data is being collected, stored and processed about migrants and people on the move, as well as a lack of transparency about how long this data will be stored for and how it will be properly handled.

Bias and discrimination: Algorithms risk profiling and discrimination due to the data they are trained on, as well as continuing input data, which [may amplify and perpetuate societal biases against certain demographics](#). This could result in individuals of a certain demographic being profiled more than another, for instance.

Are corporations involved?

There have been reports of several private companies involved in the development of algorithmic surveillance tools sold in government procurement contracts. Such companies include:

- [Anduril](#): U.S. military technology company Anduril sells a wide range of defence tech from air to maritime to border technologies. The company's Sentry Towers have reportedly been used along [U.S. land and maritime borders](#) and the [southeastern UK border](#). [According to the company's website](#), 'Sentry uses artificial intelligence to detect, identify, and track objects of interest' [Migrants Rights Network](#) has previously reported these Sentry Towers' capability to algorithmically detect and track individuals and small boats.
- [Palantir](#) (e.g., Immigration OS): Palantir is a U.S.-based technology company that [provides a range of data tools and software for a variety of sectors like defence and life sciences](#). The company has historically partnered with U.S. government departments before as a supplier, such as providing U.S. Immigration and Customs Enforcement

- (ICE) with the [FALCON](#) surveillance tool to conduct workplace raids and the [Investigative Case Management \(ICM\) tool](#). Most recently, [it has been reported](#) that [Palantir is developing 'Immigration OS'](#), which aims to create an ['AI-driven profile of individuals that agencies can use to make faster and more efficient enforcement decisions'](#).
- [Babel Street](#) (e.g., Babel X): U.S.-based Babel Street is an 'AI-Driven Risk Intelligence' company that provides solutions for defence and law enforcement. Its [AI tool 'Babel X'](#) reportedly allows law enforcement to input a piece of data about a target, such as their name or email address, and get back troves of data about that person, such as their social media links, employment history and even advertising IDs on their mobile devices. [Both U.S. Customs and Border Protection \(CBP\) and ICE](#) have each reportedly contracted with Babel Street for its location data collection tools.
 - [Serco](#) (e.g., SRAT): Serco is a global company that provides technology and other solutions [for the immigration sector](#), such as asylum accommodation services. In Australia, the company has [reportedly been tasked](#) with running the country's immigration detention network and developed the ['Security Risk Assessment Tool' \(SRAT\)](#), which determines whether someone is low, medium, high or extreme risk for a range of factors including escape or violence.

We are also starting to see [private AI companies being contracted by governments](#) to develop bespoke surveillance capabilities for the purposes of border security ('defence'), such as [Claude Gov](#) from Anthropic. Governments themselves are also developing their own in-house tools for algorithmic surveillance, such as the [UK Ministry of Defence's 'ChatMOD'](#).

Real world examples:

Algorithmic surveillance has been reportedly used across various regions by national immigration authorities. The scope of algorithmic surveillance ranges from AI decision-making algorithms (e.g., [AI recommendations for immigration actions](#)) to [algorithmic detection software](#).

Specific examples of deployment within countries include:

- **EU:** Algorithmic surveillance has reportedly been deployed both among national immigration authorities and in [joint operations with international forces like Frontex](#) and foreign intelligence agencies. While algorithms introduce a wide range of risks and harms, [the EU AI Act notably does not expressly ban the harmful use of AI in the migration context](#).
- **UK:** The UK Home Office appears to have been using an [algorithmic AI tool 'Identify and Prioritise Immigration Cases' \(IPIC\)](#) that automatically identifies and recommends migrants for immigration decisions or enforcement actions. The UK also reportedly had a contract with U.S.-based Anduril Industries for [Sentry Towers using algorithmic surveillance](#) on the south-east coast of England to detect small boat crossings and people smuggling activities.
- **Australia:** Though [no longer in use](#), Australia's immigration system previously relied on Serco's [Security Risk Assessment Tool \(SRAT\)](#), an algorithm tool that assigns immigration detainees a low, medium, high or extreme risk rating, often without detainees' knowledge and allegedly riddled with inaccuracies.
- **U.S.:** US Customs and Border Protection (CBP) is reportedly using a range of algorithmic and AI tools like data-mining platform [Babel X](#) and [Palantir's Immigration OS](#) to monitor individuals and identify priority deportation cases.

Read more:

- [PI alerts regulator about the use of algorithms by the UK Government and their impact on migrants](#)
- [Automating the hostile environment: uncovering a secretive Home Office algorithm at the heart of immigration decision-making](#)
- [Privacy International issues complaint to the UK regulator regarding the deployment of two algorithms for immigration purposes](#)



IMSI Catchers

What is it?

[International Mobile Subscriber Identity catchers \(IMSI catchers\)](#), also called '[stingrays](#)', are devices that enable the locating and tracking of mobile phones that are switched on in a particular area. IMSI catchers [pose as legitimate mobile device antennas](#), prompting nearby mobile phones to connect to them and thereby revealing their unique IMSI numbers. IMSI catchers can then [intercept the data from these mobile phones](#) without the device holder's knowledge; once a mobile phone has been [tricked into revealing its unique IMSI number](#), the IMSI catcher can determine the phone's general location based on the strength of the phone's signal – thus enabling police to determine a more precise location of the device.

Some IMSI catchers have the capability to intercept text messages, calls and Internet traffic, even re-routing or editing communications data sent to and from a mobile phone. Other IMSI catchers could [block service](#) so that the individual can no longer use their mobile phone.

According to our survey findings, IMSI catchers in the migration context have reportedly been used in both border surveillance scenarios and within the country, such as in detention centres and airports.

What are the risks?

Privacy: The secretive nature of IMSI catchers may violate a person's right to privacy, as IMSI catchers can [covertly obtain a device holder's precise location](#),

[communications and other device traffic](#) to surveil them without the person even knowing their device has been captured. This could even lead to the surveillance of deeply personal messages and location data.

Informed consent: [IMSI catchers trick mobile phones into connecting with them](#), thus obtaining a device holder's [exact GPS location](#) without their consent or knowledge.

Lack of transparency: IMSI catchers operate covertly and undercover without a person's knowledge that their personal communications and device data and location may be revealed.

Free assembly: IMSI catchers have historically been deployed in areas with [dense groups of people](#), such as airports, detention centres, or even public events, which impact individuals' right to gather.

Freedom of expression: IMSI catchers might be used to deter people from engaging in protected political speech, and [create a chilling effect](#).

Are corporations involved?

Corporations are involved and reportedly manufacturing IMSI catchers explicitly for military and migration contexts, including:

- [L3Harris](#): L3Harris, a merger of L3 Technologies and Harris Corporation, are a U.S. defence contractor company that produces a range of defence electronics and surveillance products [which it says](#) are used by law enforcement for monitoring and intelligence programmes. One such surveillance tool is [Stingray cell-site simulators](#) to intercept mobile phones and extract data such as call metadata and location information.
- [Phantom Technologies](#): Phantom Technologies is an [Israeli defence technology](#) company. One of its offerings includes IMSI catchers deployed by law enforcement, intelligence and military units to conduct targeted or in-range surveillance, [such as for border protection](#).
- [Septier Communication](#): Israeli [Septier Communication](#) provides tactical and cellular security technology [such as for border security](#),

- including covert 'backpack' [IMSI catchers](#).
- [Octasis](#): Octasis is a Canadian firm that develops wireless communication technologies, including IMSI catchers that intercept mobile phone signals and extract user location information. Some law enforcement agencies in the U.S. have [reportedly been deploying Octasic's Nyxcell line of cell-site simulators](#).
 - [Kavit Electronics Industries](#): This is an Israel-based warfare technology company that also provides telecoms technology like [IMSI catchers](#) that can be used in law enforcement, national security and intelligence agencies to track and intercept mobile communications and data.

Real world examples:

IMSI catchers have reportedly been used in numerous countries to monitor and [locate](#) individuals for immigration-related charges. While the technology is not as commonplace as, say, FRT, IMSI catchers allow law enforcement authorities to capture a large breadth of intelligence from mobile phones in the surrounding area, often without the device holders' knowledge.

Examples of countries where IMSI catchers have been deployed include:

- **U.S.:** Allegedly used by U.S. Immigration and Customs Enforcement (ICE) [to apprehend and gather evidence on individuals, as well as to locate and arrest certain individuals](#). Despite organisations', like the ACLU's, determination to find out more about the technology, little information has been provided by ICE or Customs and Border Protection (CBP) about how the cell-site simulators work and in what circumstances they have been used.
- **Greece:** Survey respondents reported that IMSI catchers are deployed around the border areas of the Aegean Sea and in Evros, in addition to mainland Greece for in-country monitoring. [Greek authorities also have joint information-sharing operations with international bodies like Frontex, the European Border and Coast Guard Agency, and NATO.](#)

According to our survey respondents, the purpose of deployment appears to be for search and rescue operations and combatting people smuggling/human trafficking operations.

- **UK:** Our survey found that IMSI catchers were reportedly deployed at UK airports to identify an individual, their nationality or other characteristic; to justify the decision to detain an individual who arrived without immigration status; or to determine the conditions to which such an individual might be subject, including assessing their 'risk profile.' In 2016, law enforcement were [reported to have purchased IMSI catcher equipment](#) but have taken a 'neither confirm nor deny' position.
- **Spain:** Survey respondents report encountering deployments across all Spanish borders, especially maritime borders (i.e., southern Iberian Peninsula, Canary Islands, Balearic Islands, Mediterranean) and throughout randomized controls inside country borders such as in detention centres for undocumented individuals.

Read more

- [IMSI catchers: facilitating indiscriminate surveillance of protesters](#)
- [Explainer: IMSI Catchers](#)
- [IMSI catchers: PI's legal analysis](#)
- [Remember those IMSI catchers? UK authorities play hide and seek with use of intrusive surveillance technology](#)



Biometric Scanning

What is it?

Governments scan physical features like fingerprints, faces, or irises and store this information in new or existing databases which can then be used to identify individuals in border control contexts, and in registering and [verifying the identities of newly arrived migrants and asylum seekers](#).

Though this technology is not new – for example, [UNHCR has collected fingerprints for decades](#) – the use of biometric scanning has exploded, and the types of data being collected have grown more varied, [from gait analysis to voice recognition](#). Countries are increasingly issuing ‘[biometric passports](#)’, or passports with an Radio Frequency Identification (RFID) chip that contains information such as a person’s fingerprints, facial features, or iris scans.

What are the risks?

Privacy: Authorities collect and store unique identifying information about people – it is often unclear who can access this data, or who might be granted access to, under what circumstances and for how long – for example, [the UK has shared passport and immigration databases](#) with the Met Police.

Misidentification and exclusion: Biometric border control is not infallible – [bodies undergo changes over time](#) that can invalidate their usefulness as stable sources of information. For example, facial recognition is often inaccurate as a result of gender and skin-color changes, or fingerprints become damaged; and people’s gaits can change due to exercise, injury, or age. The varying accuracy and failure rates of the technology can lead to

misidentification, fraud and civic exclusion.

Informed consent: There are many scenarios when [migrants at the border may not be aware that their information is being collected, by whom, until when, and what it will be used for](#), thus undermining their right to give consent. Not only does this violate consent at the time of collection, but as biometric data can identify a person for their entire lifetime, this also violates consent far into the future, as individuals might not know for how long their registered biometric information is stored. This could carry implications in political change situations, a data breach, or the development of technologies that expand the use-cases for biometrics.

Transparency and accountability: Biometric systems are expensive, and the ways governments procure them is deeply opaque. It is often unclear how the systems work, how and why they fail, whether the government or the companies themselves manage and access the data, and whether there are contingencies should a company go out of business.

Are corporations involved?

There are many companies profiting from government use of biometrics, including:

- [Idemia](#): A French company that [provides biometric services](#) to over 350 air, land, and sea ports.
- [IBM](#): The technology giant has [contracted with the UK government](#) to provide biometric technology for immigration and law enforcement purposes.
- [Accenture](#): Headquartered in Dublin, Ireland, Accenture has provided biometric technology to countries and agencies around the world including the [U.S.](#), [EU](#), [Malawi](#), [Thailand](#), and to the [UNHCR](#).
- [WorldReach](#): Canadian software company WorldReach (which has since been [acquired by digital infrastructure company Entrust](#)), [provides a biometric app service to the UK](#) for its EU Settlement Scheme applications.
- [Thales Group](#): Defence tech company Thales Group provides biometric services [like its e-gates which have been deployed](#)

[worldwide.](#)

Real world examples:

Biometric scanning is used around the world in various immigration contexts:

- **Greece:** Survey respondents reported that authorities use biometric databases to assess if another member state is responsible for processing the asylum claim of an applicant, which would be the case if they had first registered somewhere else in the EU. According to our survey results, authorities also reportedly use biometric scanning supplied by Imperio in the Samos Closed Controlled Access Centre – an immigration detention facility – to track the entry and exit of migrants and employees. In 2021, the Hellenic Police [began using tools](#) that facilitate facial recognition and fingerprint identification during police stops that target undocumented migrants.
- **EU:** [EU agencies share data with one another, as do different countries](#) – in August 2025, the EU announced that they were planning to strike a deal that would [grant U.S. authorities](#) access to their immigration databases. [Frontex and Europol](#) use biometric scanning to determine the conditions to which an individual without immigration status is to be subject (including any anti-terrorism/national security conditions), such as assessing their “risk profile”. The European Asylum Dactyloscopy Database ([Eurodac](#)) collects and compares fingerprints of asylum seekers, and authorities plan to expand this database to include their faces. Additionally, survey respondents report that authorities use biometrics, to justify the decision to detain an individual who arrived in the country without immigration status (including both the initial decision and any subsequent decision(s) to maintain detention).
- **Spain:** Survey respondents reported that immigration authorities including [border forces](#) and police in (especially maritime) border areas and throughout the country use biometrics to identify people they suspect do not have legal status, and immigration officers employ the technology in detention centres to identify and track migrants and their

movements.

- **UK:** Our survey also found that UK authorities use biometric scanning in immigration detention facilities, as well as at the borders or when processing immigration applications [for identification purposes and for general immigration purposes, such as raising new records or processing existing cases](#). UK officials may also use retained biometric information to [assist with a prosecution and to assess an individual's "unresolved criminality"](#).

US: US authorities use biometric scanning at [borders](#) to record identities and immigration status, and in [ICE immigration enforcement contexts](#) to determine identities and whether a person has immigration status.

Read more

- [The EU, the Externalisation of Migration Control, and ID Systems: Here's What's Happening and What Needs to Change](#)
- [Explainer: Biometrics](#)
- [The rise of the Surveillance Databases](#)
- [The End of Privacy in Public](#)



SOCMINT

What is it

Social media intelligence (SOCMINT) [refers to the techniques and technologies](#) that allow companies or governments to monitor social media networking sites, like Meta and X (formerly Twitter). SOCMINT includes [monitoring content posted to social media sites](#) and might involve manually reviewing content as it is posted in public or private groups or pages, reviewing the results of searches and queries of users, and/or reviewing the activities or types of content that users post. SOCMINT can be carried out without human involvement through '[scraping](#),' the automated extraction of content from web pages to collect and structure the content in formats that make it searchable, analysable, or otherwise reusable outside the original platform environment, in ways that are directly accessible to the person gathering social media intelligence.

SOCMINT is [used for multiple purposes](#) in immigration contexts, including: to [assess and determine immigrant, asylum, and temporary visa applications](#) and to [monitor individuals](#).

What are the risks?

Bias and discrimination: Social media intelligence may allow immigration authorities to [selectively target individuals based on race, religion, political views, or other protected characteristics](#).

Privacy: [SOCMINT relies on information posted both to private and public accounts](#). Authorities obtaining information from these accounts, especially

accounts users think are private, violates a reasonable expectation of privacy.

Freedom of expression: People interacting with immigration authorities report [being less likely to express themselves on social media, especially their political views, in fear of retaliation](#) in the form of being denied or losing immigration status.

Informed consent: Individuals posting content to [private social media accounts](#) have not consented to their data being accessed, shared, and used by immigration officers. Even when individuals post content to public accounts, [there still remain significant privacy concerns when this data is being incorporated into mass databases](#).

Are corporations involved?

Corporations create software to automate the SOCMINT process, including:

- [Spokeo](#): Spokeo is an American SOCMINT company that [works with some agencies of the United States government](#), and touts its database that covers 'the entire US adult population'. It promises to assist governments to locate suspects, locate vehicles, uncover contact information, and identify relationships between people.
- [Palantir](#): Also discussed above, Palantir is a U.S.-based technology company that provides a [range of data tools and software for a variety of sectors like defence](#). In the context of SOCMINT, [Palantir contracts with immigration authorities and border control, and uses artificial intelligence and data mining to identify, track, and facilitate the deportation of non-citizens](#) in countries including the [US](#) and the [UK](#).
- [Shadow Dragon](#): Shadow Dragon produces the [SocialNet software](#) which scrapes over 200 social media platform, and uses this information to creates profiles of individuals of interest that map connections, track activities, and visualize relationships.
- [Babel Street](#): Also mentioned above, Babel Street is an American company that [markets its SOCMINT software for border screening](#). [According to its website](#), it promises to carry out social media analysis

on individuals and topics across languages; connects individuals with relevant names, addresses, and organizations and compare against databases and watch lists; and automate the analysis of bulk data sets.

Real world examples:

SOCMINT is rapidly being adopted all over the world, including in:

- **USA:** [Immigration authorities can use SOCMINT to monitor phones of advocates and migrant activists](#), and [may potentially use this information to decide whether to grant visas or asylum](#). The US now requires that applicants for certain visas provide all social media accounts one has used for the past five years, and the government reportedly considers political views when deciding whether to [grant](#) or [revoke](#) visas. Additionally, [Immigration and Customs Enforcement](#) uses SOCMINT to investigate, track, and arrest individuals who are suspected of being in the US unlawfully.
- **Ireland:** Our survey participants report that immigration officers in Ireland use SOCMINT when considering asylum claims, family reunification applications, and other claims for a right to remain, and when attempting to justify detention. According to a respondent, Ireland uses SOCMINT to 'verify' identities and stories of applicants.
- **Paraguay:** Our survey respondents report that SOCMINT is widely used by police with little to no oversight, and they are concerned that the technology is used by border officials and immigration officers..
- **Greece:** Greek and EU immigration officials as well as Greek police use SOCMINT to assess and determine application outcomes, age, nationality, and identity. The [Hellenic Coast Guard](#) has additionally contracted with a social media monitoring tool to surveil conversations on migration, and to predict migration flows towards Greece.
- **Spain:** According to survey respondents, national authorities use SOCMINT, especially in coastal regions, to determine identities

of newly arrived migrants, and people suspected to be in Spain unlawfully. A survey respondent also stated that this information can be used to arrest and justify the use of detention of newly arrived migrants, and border authorities and police use SOCMINT at checkpoints inside Spain, and in detention centres for undocumented people.

- **Germany:** Germany police [have advocated](#) for the 'intensive' use of open-source and social media investigations for visa applicants in order to assess them against subjective criteria, including the 'plausibility' of their stated reason for traveling, and their likeliness to leave the Schengen area.

Read more

- [Explainer: Social media intelligence](#)
- [Social Media Surveillance: When social media makes you a target](#)
- [Social media monitoring in the UK: the invisible surveillance tool increasingly deployed by government](#)



Digital Tracking and GPS Tagging

What is it?

In migration contexts, digital tracking [refers](#) to the remote monitoring of an individual through a fitted or non-fitted device like an ankle bracelet, smart watch, or cell phone. Certain immigration authorities view the practice as [“an alternative to detention”](#), however some regulatory bodies have also [disputed](#) these claims. People subject to digital tracking often have conditions associated with their release from custody such as a [curfew or requiring them to stay within a certain area](#). Additionally, some forms of digital tracking [allow immigration authorities](#) to see the wearer’s live location at all times.

What are the risks?

Privacy rights: Digital tracking allows immigration authorities to [track the location of individuals wearing the devices 24/7](#), potentially revealing information like an individual’s religion, health conditions, or sexual orientation.

Physical and mental health risks: Individuals subject to digital tracking [reportedly](#) experience re-traumatization, stress, difficulty sleeping, anxiety, and depression. Additionally, sometimes devices can [cause](#) bruises and blisters.

Informed consent: Research from our partner organisation [Bail for Immigration Detainees](#) shows that in many cases, governments do not communicate the conditions and implications of the tracking devices, and do not explain how to challenge the requirement that they be tracked.

Due process: Our previous research found that the accuracy of GPS tags appears to be [limited to around ten meters](#), and the technology can be

further affected by its surroundings. For instance, if the signal from one or more satellites bounces off a tall building, this can give rise to [an error of 100m or more](#). Even larger errors can arise [where the view of the sky is restricted](#). These inaccuracies could lead to misinterpretation of and thus risk unjust detention or deportation.

Transparency and accountability: Governments sometimes obtain FRT in opaque ways. For example, when we were first investigating Buddi, which was contracted to supply migrant tracking devices for the Home Office, [we were puzzled to see that company was marketing itself in the public consumer market as selling personal alarm wristbands for the elderly](#). It took further digging to connect the dots that this was the same company providing tracking devices to the UK government.

Are corporations involved?

Governments contract with corporations both to produce digital monitoring devices, and with other corporations to fit, administer, and manage them. Companies reportedly providing such devices in immigration contexts include:

- [Serco](#): [Serco administers](#) and fits GPS tags for the UK government, taking over from Capita in 2024. Its contract lasts until at least 2030.
- [G4S](#): [G4S manufactures technology](#) used to track the location of individuals through electronic monitoring. The company operates in countries around the world and signed a [new £175m contract](#) with the United Kingdom in 2023.
- [Airbus](#): European aerospace and defence company Airbus [has contracted with the UK government](#) to provide data and mapping infrastructure to the GPS tracking scheme, and processes and verifies the data transmitted from GPS tags.
- [Buddi](#): [Buddi](#) is a British company that manufactures smartwatches used to track migrants in the UK – its supplier contract has been [renewed for another year to April 2026](#).
- [BI Incorporated](#): [BI, Inc.](#), an American company and subsidiary of the UK-based GEO group (a private prison operator), designs, operates,

and manages the [SmartLINK electronic monitoring service](#) for U.S. Immigration and Customs Enforcement.

Real world examples:

Reports of GPS tagging migrants, especially newly arrived migrants, include:

- **UK:** [Many migrants in the UK](#) are fitted with GPS tags after being released on immigration bail. They monitor whether an individual is complying with the conditions, such as curfew, to which they are subject.
- **U.S.:** U.S. Immigration and Customs Enforcements monitors recently arrived asylum seekers who have crossed the US/Mexico border via the [SmartLink mobile application](#), and use SmartLink [and ankle monitors](#) to track the movements of people who have been released from immigration detention, or who have lost legal status.
- **Australia:** In November 2024, Australia passed [legislation](#) introducing ankle bracelets as a visa condition for persons who cannot be deported because they are stateless, owed non-refoulement obligations or for other reasons, including having been released from indefinite immigration detention. If the person leaves the country of Australia, they will not be permitted to re-enter.

Read more:

- [UK Justice and Home Affairs Committee publishes report on electronic monitoring](#)
- [ICO Complaint against the UK's GPS tagging of migrants](#)
- [Who profits from the UK's 24/7 tracking of migrants?](#)
- [Non-fitted devices in the Home Office's surveillance arsenal: Investigating the technology behind GPS fingerprint scanners](#)



Bone and Dental Scanning

What is it?

Immigration authorities [use bone and dental scanning](#) to determine the age of individuals, and to assess and identify newly arrived migrants. The main concern appears to be [identifying minors](#), who are entitled to additional resources and protections. Scans might include [dental x-rays, MRIs of the knees and clavicle, and x-rays of the wrists](#).

What are the risks?

Privacy: Subjecting individuals to bone and dental scans is an invasion of privacy and bodily autonomy.

Due process: Bone and dental scanning are [not scientifically sound methods](#) with which to determine age. Scanning for age determination relies on the incorrect assumptions that bone and teeth mature at a constant rate. This risks misidentifying a child as an adult, and denying them safety.

Invasive: Individuals, including children, are subject to unnecessary medical procedures, and are exposed to radiation.

Informed consent: Individuals who refuse medical tests such as x-rays can have their refusals [held as a negative factor against them](#) when authorities consider their asylum applications. As such, the power imbalance undermines migrants' right to consent if there may be potential negative consequences to not consenting.

Are Corporations Involved?

From our research, it is unclear the extent to which medical imaging manufacturers are aware that their devices are being used in migration contexts.

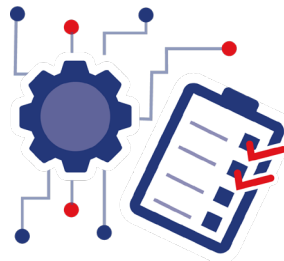
Real world examples:

Immigration authorities use bone and dental scanning in jurisdictions including:

- **Greece:** Our survey respondents report allegedly encountering immigration authorities and the police using bone and dental scanning at registration and identification centres when people first arrive to the country to attempt to determine age.
- **Czech Republic:** Survey respondents from the Czech Republic report that immigration authorities and the police have used bone and dental scanning to determine applicants' ages, and justify their detentions (in cases where detention is only mandated for adults).
- **UK:** [New legislation came into force in 2024 that allows the Home Office to use "scientific methods" like bone and dental scanning](#) verify the age of asylum seekers.

Read more:

- [Rights Groups Ask Court to Order Release of U.S. Government Info on Dental and Bone X-Rays of Migrant Children](#)
- [UK: Bone scans to be introduced for asylum seekers](#)



Automated Decision Making

What is it?

Automated decision-making, or ADM, refers to the practice of [using algorithmic tools to assess immigration or asylum applications](#). Personal data such as a person's age, nationality, and health conditions are used as parameters in [algorithmic systems that recommend or otherwise influence immigration case decisions](#), such as whether to detain or deport someone. Some algorithms may even make [recommendations about conditions which individuals on immigration bail are subject to](#).

What are the risks?

Bias and discrimination: These tools may make decisions about asylum and immigration claims by taking into account factors such as nationality, age, and prior interactions with criminal justice systems, thus opening the door to explicit and implicit discrimination based on race, ethnicity, gender, age, religion, and other [protected characteristics](#).

Lack of transparency: AI tools are [being deployed secretly and behind closed doors without minimum safeguards for transparency](#), which can [undermine procedural fairness for asylum applicants](#).

Informed consent: Individuals are [not necessarily told when their data is fed to an algorithm or that their case may be processed by an algorithm](#). As a result, they cannot meaningfully consent to being potentially subjected to automated decision-making – nor can they meaningfully consent to their application or data being processed by an algorithm..

Due process: Because the use of ADM is [secretive and poorly understood](#), and

because of the [biased](#) and [opaque nature](#) of automated decision-making, it is difficult to know whether individuals' immigration claims are [being given the consideration they are owed under international law](#).

Are corporations involved?

It is unclear which companies have been contracted to supply this software to governments. In the UK, the Home Office confirmed that [one of the several algorithms](#) they are using was [developed internally](#).

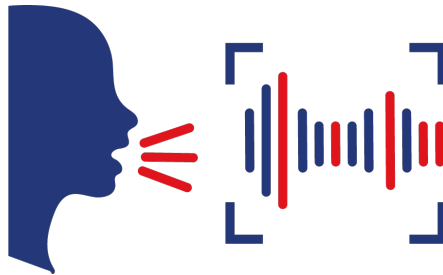
Real world examples:

Policy makers are quickly adopting ADM to aid in the assessment of applications [across government functions](#), such as applications for welfare and social security benefits, in addition to immigration applications. Jurisdictions where ADM has already been adopted in immigration contexts include:

- **UK:** [Immigration authorities](#) use ADM to determine immigration conditions, such as detention and electronic monitoring.
- **Greece:** Survey respondents report that immigration authorities use ADM to assess application materials to recommend an application outcome.
- **Canada:** [Canada](#) uses ADM at various stages of the visa application process. The ADM makes decisions about factors such as the completeness of applications, whether someone should be deemed a risk, and whether the basis for a visa application is truthful.

Read More

- [A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System](#)
- [PI alerts regulator about the use of algorithms by the UK Government and their impact on migrant](#)
- [Automating the hostile environment: uncovering a secretive Home Office algorithm at the heart of immigration decision-making](#)



Language Recognition Software

What is it?

Immigration authorities employ language recognition software to [identify the language and dialect someone speaks in an attempt to determine their country of origin](#). Software has reportedly been [used](#) to recognize Farsi, Dari, Pashto, and dialects of Arabic from Iraq, Egypt, the Maghreb, the Levant, and the Gulf.

What are the risks?

Inaccuracy: Critics argue that using voice recognition to determine nationality is [unreliable pseudoscience](#), as spoken dialects [do not always adhere to borders](#). For instance, Dari, primarily spoken in Afghanistan, and Farsi, primarily spoken in Iran are easily mistaken for one another.

Due Process: There are potential risks that country of origin determined by language and dialect recognition software can play a deciding role in the outcome of asylum applications. For example, [there have been reports that language recognition is used before an applicant's asylum interview](#), which means that the interviewer may already have an indication of where the applicant is from before hearing their testimony. This could potentially affect the procedural fairness of the process, [as some interviewers may hold unconscious biases or prejudices](#).

Informed Consent: Language recognition software may be employed without the interviewees' knowledge or consent – sometimes, individuals are simply asked to speak into a telephone like device without being told why.

Are corporations involved?

The German Federal Office for Migration and Refugees [internally developed](#) AI tools to recognise dialect, and [the European Union Agency for Asylum is exploring options, including using AI, to build upon its existing Language Assessment for the Determination of Origin \(LADO\) tool](#) that relies on human expertise, compared to Germany's machine learning equivalent. However, there are corporations that [manufacture](#) language recognition software that may be contracting with governments, but we have not been able to find publicly available information on this matter.

Real World Examples:

Language recognition is reportedly being used in:

The Netherlands and Sweden: Immigration practitioners from the Netherlands and Sweden who responded to our survey report that authorities have used language recognition software in interviews with their clients to corroborate or challenge their clients' countries of origin.

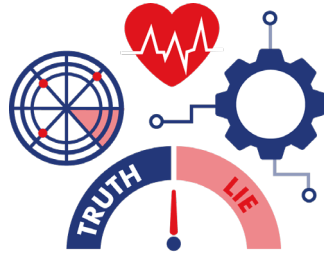
Germany: Germany has been using three separate AI equipped language recognition tools [since at least 2017](#). One of these tools, [DIAS \(Dialektidentifizierungsassistent\)](#), works by having an asylum seeker speak on a topic for about two minutes, after which the DIAS indicates the language and [regional dialect being spoken](#). This information is then provided to the relevant asylum officer conducting the asylum application interview.

EU: The EU is [reportedly building an AI-equipped language recognition software](#) that will standardize the use of this technology across EU member states. Ultimately, the EUAA plans to establish a centralized team of analysts to operate the software.

Read more

[Germany's controversial dialect recognition software](#)

[A European language detection software to determine asylum seekers' country of origin](#)



Other Technology

In survey responses, we received limited reports about border enforcement using:

- **Heartbeat Detectors:** [At EU borders, immigration authorities use heartbeat detectors to locate people who are hiding in vehicles and attempting to cross the border.](#) Just this year, [nearly 200 migrants were found using heartbeat detectors at the Kipi border crossing in Greece.](#) According to our survey findings, immigration authorities use heartbeat detectors to prevent people from crossing borders, and to prosecute unlawful entry, other immigration offences, human trafficking, and people smuggling.
- **Radar, helicopter, zeppelin, vessel detection:** [Greece has developed a system called 'Sea Border Awareness' involving radars and thermal cameras for observation of migrants in the Aegean sea.](#) Greece has been [accused of human rights abuses](#) involving forcing migrants off of their radar-identified vessels and leaving them adrift on life rafts. Like the use of drones and infrared cameras, these technologies risk privacy, freedom of association, freedom of expression, and due process rights.
- **Lie Detectors:** The [Automated Virtual Agent for Truth Assessment in Real-time \(AVATAR\)](#) aimed to create a virtual agent to detect 'potential anomalous behaviour' by analysing data from cameras, microphones, and eye tracking systems. Additionally, the [iBorderCtrl](#) aimed to create a 'decision support system' at borders that detected deception.



Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).