****

**Access Now Submission to the United Nations Secretary General**

**on the Human Rights of Migrants**

12 May 2023

**Introduction**

Access Now welcomes this opportunity to provide relevant information to the United Nations (UN) Secretary General to inform the report on the human rights of migrants. Access Now, a UN Economic and Social Council (ECOSOC) accredited organization, routinely engages with the UN to support our mission to extend and defend digital rights of people and communities at risk around the world.[[1]](#footnote-1) Since its founding in 2009, Access Now monitors the abuse and misuse of new and emerging technologies that threaten fundamental human rights, including freedoms of expression, association, and peaceful assembly, as well as the rights to privacy and non-discrimination. We also closely monitor internet shutdowns and coordinate the global #KeepItOn coalition and campaign against internet shutdowns.[[2]](#footnote-2)

This submission addresses thecollection, processing, sharing, surveillance, and use of data of people on the movein the United States, Latin America, and the European Union contexts. This submission is divided into three sections. First, this submission provides a non-exhaustive overview of data protection under international law. Second, this submission delves into the context of the collection, processing, sharing, surveillance and use of data of people on the move through Mexico, Guatemala, Honduras and El Salvador to the United States. Third, this submission narrows in on the use of border surveillance technologies, particularly Artificial Intelligence (AI), in the European Union and its impact on people on the move and racialised groups. This submission concludes with recommendations to States, private sector actors, and international organizations. It is important to note that while this submission draws upon examples, these examples are non-exhaustive, and do not represent the lived experiences of all persons at risk. More information is required to take into full account the intersecting forms of oppression of those who are directly targeted.

**I. Data protection under international human rights law**

1. Sharing data may bring many benefits. For instance, in cross-border contexts, it is a common objective of States to share data regarding migration in order to strengthen the capabilities of their national security, and prevent organized crime. But it is not without risks. Data can easily be exploited to harm, and is especially dangerous for vulnerable individuals and communities, including people on the move, particularly those on the move who also identify as members of oppressed and marginalized groups. Data must therefore be strictly protected.
2. The international human rights law framework centers on the dignity of each person. It provides a clear basis for the promotion and protection of the right to privacy, which covers the collection, processing, sharing, retention, and use of personal data.[[3]](#footnote-3) No one shall be subjected to arbitrary interference with the right to privacy, which is closely linked to the right to data protection.[[4]](#footnote-4) Any restriction on these rights must be consistent with the principles of legality, necessity, and proportionality under international law.[[5]](#footnote-5) In practice, this also means that any collection or processing of individuals’ data should be fair, lawful, transparent, and subject to independent oversight, and that affected individuals should be provided with access to effective remedies. Further, the surveillance or interception of data must be subjected to the highest restrictions, if permitted at all.
3. Effective personal data protection frameworks should prevent data-driven discrimination-related harms and provide effective remedies in the case of the unlawful use of data to observe or infer information on the basis of race, ethnicity, sex, gender identity, immigration status, sexual orientation, religion, age, national origin, medical conditions, disability, genetic or biometric information, or any other characteristic protected by law. Therefore, cross-border data sharing agreements should not be used to circumvent existing protections for privacy and personal data protection at the national level, and should contain relevant safeguards to prevent risks to human rights and especially the safety, dignity and integrity of people and communities at risk — particularly people on the move — and the right to privacy.

**II. Collection, processing, sharing, surveillance and use of data of people on the move through Mexico, Guatemala, Honduras and El Salvador to the United States**

1. People on the move from Central America and Mexico to the United States (US) are constantly under surveillance. This is partly due to binding and non-binding cross-border data sharing agreements between the US and Mexico, Guatemala, Honduras and El Salvador that allows the sharing of personal data — including highly sensitive biometric data — collected with the support of a variety of technologies and private sector, state actors, and even humanitarian agencies.

1. The collection, processing, sharing, surveillance and use of data of people on the move is prone to potential human rights abuses. Bilateral and multilateral cross-border data sharing agreements are often used to allow for the deployment of different technologies that can then be used to assess and manage the migratory flow of people reaching the US, particularly at southern borders. Technologies like the US Custom Borders and Protection One application (CBP OneTM app) or the Automated Biometric Identification System (IDENT) can collect, store, and process personal data of millions of people on the move, including asylum seekers and migrants, and might assist the migratory authorities in decision making regarding their entry into, and ultimately their migration status, in the US. The mandatory nature and processing of such data criminalizes migrants by watching and treating this vulnerable population as suspicious simply for crossing international borders, or even for holding the lawful expectation of migrating, a violation of Article 13 of the Universal Declaration on Human Rights, affirming “the right to freedom of movement,” as well as human rights principles essential to realization of this right. [[6]](#footnote-6)
2. The implementation of tools that allow the mass surveillance of people on the move violates international human rights standards as it is neither necessary nor proportionate.[[7]](#footnote-7) Under these cross-border data sharing agreements, Central American and Mexican law enforcement agencies collaborate with their US counterparts by transferring vast amounts of personal data and records of their nationals and of people entering their countries, feeding the IDENT database, which might be used later as a tool for migratory decision making.[[8]](#footnote-8) Furthermore, government-developed applications, such as the US CBP One app, requires people on the move to register their biometric data, including facial images, in order to merely schedule an appointment with the border authorities. This creates severe barriers for migrants who do not have access to mobile devices or the internet, or cannot access or use the application if it cannot recognize their facial features due to discriminatory algorithms and assumptions or other circumstances. There is no legal justification for the processing, sharing, surveillance and use of data of people on the move occurring on these large movements of people in Central America and Mexico. The disproportionate amount of data that is collected and processed, and the legal infrastructure surrounding tech use in migratory governance results in an arbitrary intrusion on thousands of migrant’s private lives, and opposes several of the UN High Commissioner for Refugees’ *Principles and Guidelines on the human rights protection of migrants in vulnerable situations*, including principles 1, 2, 3, 5, 6, 16 and 19. [[9]](#footnote-9)
3. These cross-border data sharing agreements share a common objective among the signatory parties, which is to strengthen the capabilities of their national security, and the prevention of organized crime. However, in practice, national security is presented as the ultimate justification for potential human rights abuses, xenophobia, and discrimination. As the former United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance pointed out, the deployment of technologies that advance discriminatory ideas partly respond to the “widespread perceptions of refugees and migrants [seen] as *per se* threats to national security.”[[10]](#footnote-10)
4. There are many risks to people on the move’s safety, dignity, fundamental freedoms and human rights, including their right to privacy. Such risks include:
5. **Arbitrary access and uses of people on the move’s personal data:** Neither the US, Guatemala, Honduras, nor El Salvador currently have a data protection law that governs the processing of personal data. Yet, this has not stopped any of the involved countries from transferring migrants’ personal data across borders. Any abuse of such data processing will therefore ultimately fall under the interpretation of unspecialized authorities, jeopardizing the rights of the data owners.

A person on the move’s right to access, rectify, delete, and object to the status of their personal data also becomes harder to remedy without data protection law(s). This is particularly worrying in contexts where the collection of biometric data is mandatory at the borders, where consent is not necessarily informed, or transparent, or in the person’s native language. The US CBP One app is currently mandatory to request for asylum in the US, only became available in Spanish in June 2022, and remains unavailable in other languages often spoken by migrants.[[11]](#footnote-11) The US CBP One app also has access to a vast quantity of location data, purchased from private vendors,[[12]](#footnote-12) to help them improve their enforcement efforts by tracking people's movements at a large scale.[[13]](#footnote-13) It is unclear whether people on the move are genuinely aware of the transfer and uses of their personal data, both through CBP OneTM app collection, and through other mediums. Furthermore, even if people on the move are informed about their personal data processing, many are in a vulnerable position because some technologies, such as the CBP OneTM app, are the only option for people on the move, including asylum seekers, to enter the US.[[14]](#footnote-14) People on the move therefore need to use the CBP OneTM app to seek better life opportunities in another country for themselves and their families. This reality cautions against the use of consent as the legal basis for collection and processing of such sensitive data, and indeed against the requirement that asylum be conditioned on use of this application.

Moreover, the interoperable systems that allow the exchange of personal data of migrants, and other people on the move, are currently and presumably accessible to various State officers and authorities, where the collected data can be shared with other agencies as well. The burden lies with authorities to clarify what systems and data they have access to, under what legal authorities, and how permissions and access are limited accordingly. Personal data, particularly sensitive data, should be processed under higher standards of data protection to safeguard the privacy of individuals. Trespassing such standards is careless and dangerous, especially when individuals can be running away from criminal groups where their anonymity is crucial, and the level of corruption within certain authorities makes their integrity questionable and untrustworthy.[[15]](#footnote-15) This could lead to biased or incorrect data being collected by law enforcement agents, which could then be used to assist border authorities in making a decision on the individual's migratory status, or asylum application.

1. **Violation of the presumption of the innocence principle, the right to equality before the law, and the right to non-discrimination:** The vague language of the non binding cross-border data sharing agreements could enable the creation of profiling databases. The former UN Special Rapporteur on contemporary racism, racial discrimination, xenophobia and related intolerance was clear that such profiling systems are often biased and inaccurate.[[16]](#footnote-16) The lack of transparency from the authorities also prevents us from verifying whether they are implementing “predictive” systems, a type of technology that reinforces discriminatory assumptions around vulnerable people on the move. The cross-border data sharing agreement between El Salvador and the United States authorizes the collection of personal data from people who "might be planning to travel without authorization,” which goes beyond criminalizing migration itself, to criminalizing the mere intention of migrating.
2. **Prevention of free movement and asylum seeking:** Technologies that enable automated and semi automated decision making are often promoted, around the world, as a way to improve efficiency in borders. Once again, the lack of transparency and response from authorities prohibits us from understanding whether such technology is being implemented in the previously mentioned countries, but the agreements are broad enough to make it possible. When decisions of a migratory destination or situation are taken with little to no human intervention, it prevents people on the move from explaining their very specific and unique case, and from exercising their rights and to freedom of expression and opinion, and freedom of movement.
3. We are also deeply concerned about the data collection practices in migratory contexts by the United Nations High Commissioner for Refugees (UNHCR). In 2019, the US Department of Homeland Security signed a Memorandum of Understanding (MoU) with UNHCR to receive biometric and biographic data from asylum seekers.[[17]](#footnote-17) The MoU acknowledges privacy risks that are only partially mitigated, or that cannot be fully mitigated, such as the lack of knowledge by the individual of where their personal data is stored and with whom it can be shared. This is all particularly concerning in regards to a newer database technology that DHS is developing, called HART (Homeland Advanced Recognition Technology System), which is set to replace IDENT. HART allegedly has a much powerful potential to infringe individual's privacy, like migrants, refugees and asylum seekers, and the capability of feeding its database from more sources than IDENT, such as through social media scraping.

**III. The use of border surveillance technologies in the European Union and its impact on people on the move and racialised groups**

1. Artificial Intelligence (AI) systems and several types of surveillance technology are increasingly developed and deployed for purposes related to migration, asylum, and border control at and within the borders of the European Union. Access Now has been monitoring and denouncing the human rights risks and impacts that certain systems have on migrants, asylum seekers, refugees and undocumented people. Based on collaborative work with other human rights organizations, Access Now has developed a non-exhaustive analysis of AI-based systems used in the migration and border context.
2. The following systems are already deployed in the European Union:
3. **AI-based individual risk assessment and profiling systems**: AI-based risk assessment and profiling systems are used to assess individuals for risks to public security, irregular migration, public health, and also to predict people’s behaviour and likelihood to represent a risk. In the context of migration and border checks, these AI systems are then used to assess travelers on the basis of pre-defined risk categories, filtering legitimate from illegitimate travelers, with the ultimate goal of preventing the latter from entering, or residing, on EU territory. These systems assess and profile people based on predetermined risk indicators embedded in screening rules, parameters which are often opaque and not made public. They seriously threatened the right to non-discrimination, both directly and indirectly. One example is the “visa streaming algorithm” that the UK Home Office used to screen visa applications and that, in 2020, was suspended as it “entrenched racism and bias into the visa system,” according to the UK Home Office itself.[[18]](#footnote-18)
4. **Predictive analytic systems used to forecast migration:** Forecasting tools, built through predictive analytics techniques, can be used for border management and security purposes. We have deep concerns that the predictions could easily be used for the purpose of preventing migration, generating and exacerbating assumptions that particular groups present a ‘security risk’ or a threat of ‘irregular migration’, and encouraging punitive responses geared toward the interdiction of movement. In September 2022, Access Now published an open letter, endorsed by numerous civil society organizations and academics, demanding the withdrawal of the EUMigraTool from the EU-funded ITFlows project.[[19]](#footnote-19)
5. **AI Polygraphs and emotion recognition technology:** Emotion recognition technology is based on pseudo-science, AI polygraphs (‘lie detectors’) reinforce the automated suspicion in migration procedure. One infamous example of this is iBorderCtrl, an EU Horizon 2020-funded project that tested the use of an avatar that analyzes people’s non-verbal micro-gestures and verbal communication to determine the traveler’s intention to deceive.[[20]](#footnote-20) Because of the intrinsic bias of these technologies, Access Now calls for a full ban on emotion recognition technologies.
6. **Biometric categorisation systems in publicly accessible spaces and biometric categorisation systems that amount to phrenology**: AI-based systems that infer protected characteristics from biometric and biometric-based data (the way you walk, for example) violate a number of fundamental rights. In the migration context, there is a great appetite to use these systems, especially for flagging suspicious behavior, as in the case of the EU-funded Centaur project in refugee camps in Greek islands.[[21]](#footnote-21) Biometric categorisation systems have been used as part of administrative procedures, such as the dialect recognition system (DIAS) introduced in 2017 by the German Federal Office for Migration and Refugees (BAMF) for the examination of asylum applications.[[22]](#footnote-22) The system records two-minutes of a person describing a picture in their mother tongue; it then processes the voice data and calculates as a percentage how close the speech comes to a certain dialect. There is a growing interest in using these systems, especially within Frontex[[23]](#footnote-23) (check *Pronouncer* project).[[24]](#footnote-24)
7. **Remote Biometric Identification (RBI) systems in publicly accessible spaces**: RBI systems used in publicly accessible spaces amount to mass surveillance.[[25]](#footnote-25) These systems (which often use facial recognition technology, but are not limited to it) can have devastating effects if used in migration control, especially at the borders.[[26]](#footnote-26) There are already two cases in which Italy deployed RBI systems in areas considered to be frequently attended by people with an irregular migration status, with the twofold, and unrelated, purposes of reducing irregular migration and improving security measures. The first case is about the use of the SARI Real-Time facial recognition algorithm to monitor disembarkation operations,[[27]](#footnote-27) and the second is about the deployment of RBI by the municipality of Como in areas believed to be frequented by people with an irregular migration status.[[28]](#footnote-28) Both cases were deemed unlawful by the Italian Data Protection Authority.
8. **Non-remote biometric identification systems used for conducting ID checks**: The increased use of identity checks is a recurring feature in EU migration policy, in particular as part of a broader strategy to combat identity fraud and to increase the number of deportations. These systems include mobile biometric identification devices that can scan fingerprints or faces in the streets and automatically compare the biometric data against a database or a watchlist. The fundamental right to non-discrimination and the principle of proportionality are at great risk as race, ethnicity or skin colour is viewed as a proxy for an individual’s migration status, and racialized people (regardless of nationality and EU citizenship status) are more likely to be exposed to racial profiling practices. One example is the use of mobile fingerprint scanners by the Greek police, as part of the smart policing program.[[29]](#footnote-29)
9. **AI surveillance technologies used for border management**: AI systems are increasingly used in the migration context for generalized and indiscriminate surveillance at borders, including for the detection and recognition of human beings, both at land and at sea. They include the deployment of various AI-based technologies, including augmented reality (AR) systems, unpiloted vehicles and devices, intelligent detection platform and AI-assisted sensors. Examples include the use of drones to facilitate pull-backs to Libya in the Central Mediterranean,[[30]](#footnote-30) drones to detect human crossing borders between Turkey and Greece,[[31]](#footnote-31) or through a through-foliage detection platform for spotting people crossing borders passing via forests.[[32]](#footnote-32) The use of these surveillance technologies has the great potential to exacerbate violent practices and push-backs.
10. **AI-based systems used to examine asylum, visa, residence applications and to ascertain the veracity of the claim**: AI systems aimed at assessing the authenticity and veracity of evidence can utilize intrusive techniques with significant fundamental rights implications. One example is the data mobile extraction systems used by the German authorities to extract and analyze data from data carriers such as phones in order to check the stated origin and identity of the applicant.[[33]](#footnote-33)

**Recommendations**

1. **States**
2. Refrain from implementing border externalization practices that involve the personal data, particularly biometric data, of people on the move.
3. Refrain from cross-border agreements that allow the mass surveillance of the population, particularly in humanitarian contexts where such surveillance can further jeopardize vulnerable groups, like people on the move, internally/forcibly displaced persons, asylum seekers, and refugees, among others.
4. Expressly prohibit technologies that attempt to hinder migrants’ basic human rights, including, but not limited to, predictive technology, technology that takes automated or semi automated decisions, and remote biometric recognition. Specifically, call for a ban on the following:
	1. Remote Biometric Identification (RBI) systems in publically accessible spaces;
	2. AI-based individual risk assessment and profiling systems;
	3. Predictive analytic systems that can be used for the interdiction of border crossings;
	4. “Emotion recognition” and “sex/gender recognition” technologies;
	5. Biometric categorisation systems in publicly accessible spaces and biometric categorisation systems that amount to phrenology.
5. Provide information to stakeholders in a timely and appropriate manner, including answers to Freedom of Information Act (FOIA) requests.
6. Avoid the overuse of national security as a reasoning to justify any measure in borders, or the lack of transparency of the authorities.
7. Develop campaigns targeted to migratory authorities to debunk the criminal perception of migrants and other people on the move.
8. **Private sector** (applicable to both the private sector and investors of the private sector)
9. Avoid funding enterprises that develop or implement mass surveillance solutions in migratory contexts.
10. Conduct human rights due diligence, such as privacy impact assessments, to identify the potential privacy and security risks of connecting biometric data to the receipt of social services, engage with civil society and affected communities in developing and implementing due diligence policies, take steps to mitigate or prevent any identified risks, and ensure that such reporting and results are made public through transparency reports.
11. Participate in remedial processes to redress human rights harms caused or contributed by your technologies.
12. **International organizations**
13. Ensure that any “digital transformation” initiatives do not translate into more data harvesting and extraction, but rather better and more responsible use of data.
14. Protect people’s data, particularly biometric data, as a fundamental principle and operational necessity for the legitimacy and safety of its work and operation in the digital age.
15. Conduct an independent security and privacy audit as well as human rights due diligence for technologies before they are procured.

##### **Access Now (**[**https://www.accessnow.org**](https://www.accessnow.org)**)** defends and extends the digital rights of individuals and communities around the world. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact:* ***un@accessnow.org***

1. Access Now, About Us, 2023, available at <https://www.accessnow.org/>. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age. [↑](#footnote-ref-1)
2. Access Now, #KeepItOn, 2023, available at: <https://www.accessnow.org/keepiton/>. [↑](#footnote-ref-2)
3. United Nations Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. [↑](#footnote-ref-3)
4. United Nations General Assembly (UNGA), Resolution adopted by the General Assembly (2020), The right to privacy in the digital age, UN Doc. A/Res/75/176. [↑](#footnote-ref-4)
5. United Nations General Assembly (UNGA), Resolution adopted by the General Assembly (2020), The right to privacy in the digital age, UN Doc. A/Res/75/176, at OP4. [↑](#footnote-ref-5)
6. *See* United Nations Office of the High Commissioner for Human Rights, *International standards governing migration policy*, available at

<https://www.ohchr.org/en/migration/international-standards-governing-migration-policy>. [↑](#footnote-ref-6)
7. United Nations Office of the High Commissioner for Human Rights, *Spyware and surveillance: Threats to privacy and human rights growing, UN report warns,* 16 September 2022, available at: <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>. [↑](#footnote-ref-7)
8. National Immigrant Justice Center, *Consequences of Unreliable Transnational Gang Allegations*, 30 Septembe 2021, available at: <https://immigrantjustice.org/staff/blog/consequences-unreliable-transnational-gang-allegations>; Nextgov, *Fingerprint records reveals 825,000 immigrants with multople names, inconistent birth dates*, 23 August 2012, available at: <https://www.nextgov.com/cxo-briefing/2012/08/fingerprint-records-reveal-825000-immigrants-multiple-names-inconsistent-birth-dates/57620/>. [↑](#footnote-ref-8)
9. United Nations Human Rights Office of the High Commissioner and Global Migration Group, *Principles and Guidelines, supported by practical guidance on the human rights protection of migrants in vulnerable situations,* available at: <https://www.ohchr.org/sites/default/files/PrinciplesAndGuidelines.pdf>. [↑](#footnote-ref-9)
10. United Nations Human Rights Council (HRC), Report by the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, (22 September 2021), UN Doc. A/HRC/48/176. [↑](#footnote-ref-10)
11. US Customs and Border Protection, *CBP announces the Addition of a Spanish Option For I-94 Features in the CBP OneTM Mobile App*, (10 June 2022), available at: <https://www.cbp.gov/newsroom/national-media-release/cbp-announces-addition-spanish-option-i-94-features-cbp-onetm> [↑](#footnote-ref-11)
12. Wired, *The DHS Bought a “Shocking Amount” of Phone-Tracking Data*, (20 July 2022), available at <https://www.wired.com/story/dhs-surveillance-phone-tracking-data/> [↑](#footnote-ref-12)
13. Immigration Impact, *DHS Fails to Address Concerns about CBP One as the Agency Expands the App’s Use,* (13 January 2023), available at: <https://immigrationimpact.com/2023/01/13/concerns-cbp-one-app-dhs-expands/>; Amnesty International, *USA: Mandatory use of CBP One mobile applications violates right to seek asylum*, (8 May 2023) available at: <https://www.amnesty.org/en/latest/news/2023/05/usa-mandatory-cbp-one-violates-right-asylum/> [↑](#footnote-ref-13)
14. Immigration Impact, *DHS Fails to Address Concerns about CBP One as the Agency Expands the App’s Use,* (13 January 2023), available at: <https://immigrationimpact.com/2023/01/13/concerns-cbp-one-app-dhs-expands/> [↑](#footnote-ref-14)
15. See for e.g. WOLA, *Corruption Under the State of Emergency in El Salvador: A Democracy Without Oxygen*, (27 September 2022), available at: <https://www.wola.org/2022/09/corruption-state-of-emergency-el-salvador/>. [↑](#footnote-ref-15)
16. United Nations Human Rights Council (HRC), Report by the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial discrimination and emerging digital technologies; a human rights analysis,* (18 June 2020), UN Doc. A/HRC/45/57. [↑](#footnote-ref-16)
17. United States Department of Homeland Security, *United Nations High Commissioner for Refugees (UNHCR) Information Data Share*, DHS/USCIS/PIA\_081, (13 August 2019), available at: <https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf> [↑](#footnote-ref-17)
18. FoxGlove, *Home Office says it will abandon its racist visa algorithm - after we sued them*, (4 August 2020) available at: <https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/> [↑](#footnote-ref-18)
19. Access Now, *Open letter to the ITFlows Consortium: stop tech tools for predicting migration that can be repurposed to violate fundamental rights*, (27 September 2022), available at: <https://www.accessnow.org/press-release/open-letter-itflows-consortium/> [↑](#footnote-ref-19)
20. iBorderCtrl, *What is iBorderCtrl?* available at: <https://iborderctrl.no/#:~:text=iBorderCtrl%20is%20an%20EU%2Dfunded,into%20the%20EU%20more%20efficient> [↑](#footnote-ref-20)
21. BalkanInsight, *Asylum Surveillance Systems Launched in Greece without Data Safeguards,* (9 September 2020), available at: <https://balkaninsight.com/2022/09/09/asylum-surveillance-systems-launched-in-greece-without-data-safeguards/> [↑](#footnote-ref-21)
22. Vice, *Eine Software des BAMF bringt Menschen in Gefhr*, (20 August 2018), available at <https://www.vice.com/de/article/a3q8wj/fluechtlinge-bamf-sprachanalyse-software-entscheidet-asyl> [↑](#footnote-ref-22)
23. Frontext, *Frontext Law Enforcement Industry Days 17-18 May 2022 - follow up,* (2 August 2022), available at: <https://frontex.europa.eu/innovation/announcements/frontex-law-enforcement-industry-days-17-18-may-2022-follow-up-iMy0kZ> [↑](#footnote-ref-23)
24. PronounceR Europe, *Automated Native Language Identification*, available at: <https://frontex.europa.eu/assets/Invitations/Outcomes/2022_industry_days/Presentations_May_follow_up/Pronouncer.pdf> [↑](#footnote-ref-24)
25. Access Now, *Ban Biometric Surveillance*, available at: <https://www.accessnow.org/campaign/ban-biometric-surveillance/#signers> [↑](#footnote-ref-25)
26. Reclaim Your Face, available at: <https://reclaimyourface.eu/> [↑](#footnote-ref-26)
27. Statewatch, *Italy: Interior ministry’s facial recognition system is unlawful,* (21 April 2021), available at: <https://www.statewatch.org/news/2021/april/italy-interior-ministry-s-facial-recognition-system-is-unlawful/> [↑](#footnote-ref-27)
28. Privacy International, *How facial recognition is spreading in Italy: the case of Como*, (17 September 2020), available at: <https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como> [↑](#footnote-ref-28)
29. Human Rights Watch, *Greece: New Biometrics Policing Program Undermines Rights: Risk of Illegal Racial Profiling and Other Abuses*, (23 March 2020), available at: <https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights> [↑](#footnote-ref-29)
30. Human Rights Watch, *EU’s Drone is Another Threat to Migrants and Refugees*, (1 August 2022), available at: <https://www.hrw.org/news/2022/08/01/eus-drone-another-threat-migrants-and-refugees>. [↑](#footnote-ref-30)
31. Algorithm Watch, *Greece plans automated drones to spot people crossing the border*, available at: <https://algorithmwatch.org/en/greece-plans-automated-drones/>. [↑](#footnote-ref-31)
32. Foldout Solution, *Foldout Border Surveillance Technology,* available at: <https://foldout.eu/>. [↑](#footnote-ref-32)
33. Gesellschaft Für Friheitsrechte, *Freedom in the Digital Age,* available at: <https://freiheitsrechte.org/en/themen/digitale-grundrechte/refugee-daten>. [↑](#footnote-ref-33)