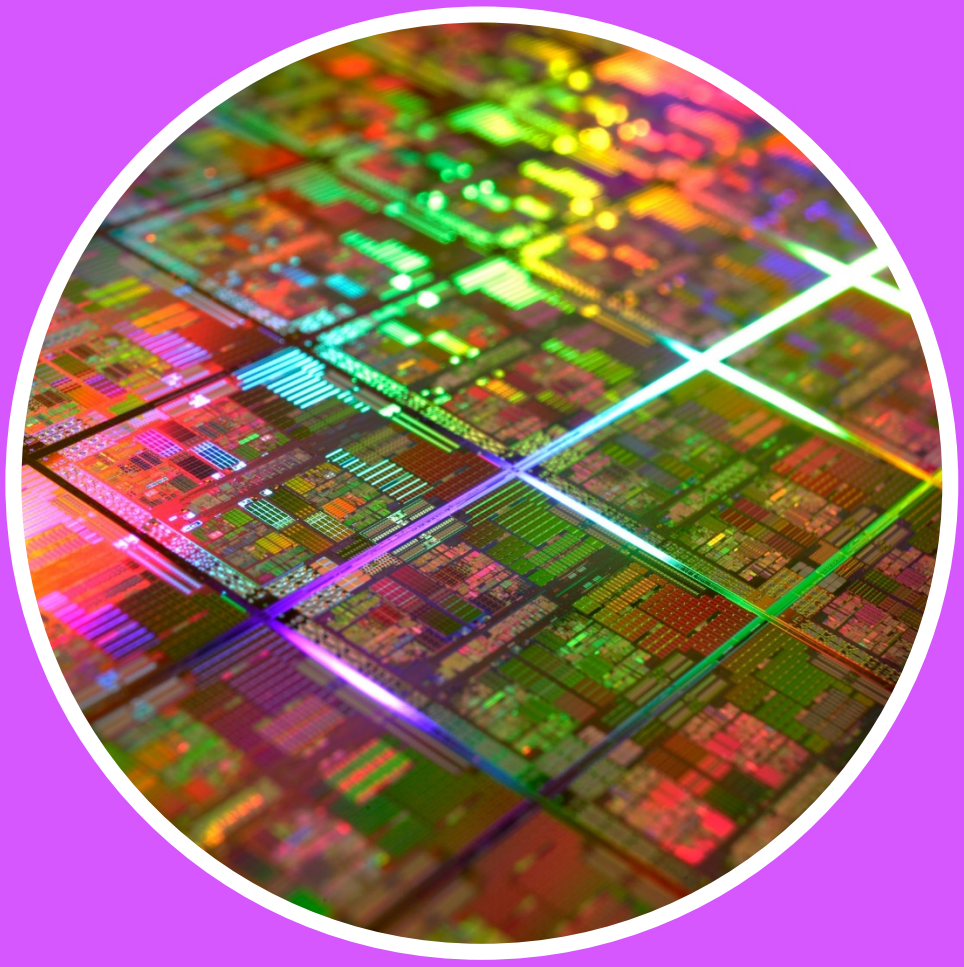
A clear and present danger

Missing safeguards on migration and asylum in the EU's AI Act



statewatch

Authors

Jane Kilpatrick, Chris Jones

Acknowledgements

The authors wish to thank Yasha Maccanico and Sarah Chander for their advice and comments.

Published by *Statewatch*, May 2022

statewatch.org

Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns for civil liberties, human rights and democratic standards. We began operating in 1991 and are based in London.

Registered UK charity number: 1154784. Registered UK company number: 08480724. Registered company name: The Libertarian Research & Education Trust. Registered office: c/o MDR, 88 Fleet Street, London EC4Y 1DH, UK.

Contents

Tables

Abstract

This briefing has been produced as a complementary document proposed amendments to the AI Act drafted by a coalition of human rights organisations (including *European Digital Rights*, *Access Now*, *Migration and Technology Monitor*, *Platform for International Cooperation on Undocumented Migrants* and *Statewatch*).[1]

It begins with key points and recommendations, which largely correspond with those in the proposed amendments. A short introduction follows, before an explanation of what the AI Act is, how it deals with migration, and the associated concerns of civil society over its "risk-based approach".

It goes on to examine the current development and deployment of AI systems by EU institutions and member states for asylum, border and migration control purposes, outlining key use cases, the risks these pose to fundamental rights, and how these would be regulated (or not) by the proposed AI Act.

The briefing then provides a snapshot of the extensive public funding that the EU has provided for the research and development of 'border AI', before giving an overview of the key actors and institutions involved in negotiations on the AI Act as it passes through EU institutions.

[1] 'Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act', *European Digital Rights*, 9 May 2022, https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf

Key points and recommendations

The Commission's proposed AI Act aims to address the risks of certain uses of AI and to establish a legal framework for its trustworthy deployment. In the context of asylum, migration and border control, the Act raises numerous concerns, which must be addressed in ongoing negotiations within Parliament, and by future campaigning and advocacy. On 20 April 2022, the European Parliament's committees on the internal market (IMCO) and civil liberties (LIBE) published a draft joint report on the Act , proposing some positive changes but continuing to overlook the risks of AI in the migration context.[2] It proposes certain exemptions that would prevent the use of AI for asylum, border and migration control being as closely controlled as for other high risk uses.

The major failures of the AI Act with regard to migration and border control are:

- A failure to include any reference to the need to uphold international obligations regarding migration and international protection
- The use of AI for individual risk assessments or profiling is not adequately considered by the Act, which should prohibit use of such systems in a migration context and ensure any other AI-systems for risk assessment or the assessment of information or evidence are classified as "high risk";
- A failure to encompass predictive analytics systems for migration, asylum and border control management, which should be included as "high risk" by the Act, and should be prohibited for purposes of interdicting, curtailing or preventing migration;
- The use of biometrics in asylum, border and migration management is not currently classified as "high risk" by the Act. AI polygraphs and emotion recognitions systems must also be prohibited in the migration management context;
- It does not take account of the fact that systems for border surveillance can underpin serious rights violations and should, therefore, be classified as high risk;
- Exclusions for large-scale IT systems: in its current form, the text will not apply to AI technologies used as part of the EU's large-scale IT systems for migration and border management if they were already on the market a year before the Regulation enters into force, unless their mandates are significantly changed in terms of design or purpose of the AI systems concerned;

There are also a number of more general shortcomings that may have implications for the use of AI in the asylum, migration and border control context:

- Limited indicators of inequality/vulnerability: the Act only refers to age and physical or mental disability as factors of vulnerability, rather than including all sensitive or protected characteristics as potential indicators of inequality (and therefore higher risk of vulnerability). These should include age, gender and gender identity, racial or ethnic origin, health status, sexual orientation, sex characteristics, social or economic status, employment status, migration status, and disability;
- The prohibition on remote biometric identification (RBI) contains numerous exemptions and only applies to law enforcement. There are three situations in which the ban would not apply, and as long as member states meet certain conditions and safeguards, they may

[2] 'Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised fules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts', COM2021/0206 – C9-0146/2021 – 2021/0106(COD), *European Parliament Committee on the Internal Market and Consumer Protection, Committee on Civil Liberties, Justice and Home Affairs,* 20 April 2022, https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_EN.pdf

fully or partially authorise the use of real time RBI. Retrospective RBI is not prohibited, nor is remote biometric categorisation;

- There are very limited obligations for users unless they modify an AI system themselves. Some obligations are placed on users of AI systems, but these are mainly procedural and do not go much further than requiring users to follow providers' instructions, and use their discretion to identify fundamental rights (and other) risks;
- In addition, it is urgent that the list of high-risk systems in the act can be modified to keep pace with developments in relevant technology and its deployment at borders or application to people on the move;

Finally, it is also urgent for campaigners and advocates to take account of the agencies, entities and institutions involved in AI knowledge and technology production, such as private companies, universities, research institutes, and arms-length government organisations, in order to better understand and engage with the development of new technologies that may pose a risk to rights at the earliest stage possible.

Introduction

The EU and its member states have long been keen to use advanced technology to control and manage migration. This tendency has accelerated in recent years, with a growing push to develop, adopt and implement technologies such as artificial intelligence, automated decision-making and biometrics in immigration and border control.[3] The potential functions for using these technologies are wide-ranging: automated systems to process citizenship and visa applications;[4] biometric 'corridors' in airports that use multiple identification technologies to shorten queueing times;[5] automated profiling systems to determine whether travellers may pose a security, health or irregular immigration risk;[6] and large-scale data analysis systems to inform humanitarian aid efforts for forcibly displaced people are all either in use or in the works – and this is just the tip of the iceberg.

In recognition of the growing use of various technologies deemed to employ "artificial intelligence", in April 2021 the European Commission published a proposal for an Artificial Intelligence Act (AIA). The proposed Act defines artificial intelligence as software that uses techniques or approaches based on machine learning, reasoning or modelling[7] that "can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."[8] The Act aims to address "the risks associated with certain uses of such technology" and develop "an ecosystem of trust by proposing a legal framework for trustworthy AI."[9] It seeks to propel the development of a domestic and export market for AI technologies that are in line with "European values"[10] – although quite how those

[3] 'Market Forces', *Statewatch, Transnational Institute* August 2017, https://www.statewatch.org/publications/reports-and-books/market-forces-the-development-of-the-eu-security-industrial-complex/ ; 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status', *Statewatch, PICUM* November 2019, https://www.statewatch.org/publications/reports-and-books/data-protection-immigration-enforcement-and-fundamental-rights-what-the-eu-s-regulations-on-interoperability-mean-for-people-with-irregular-status/; 'Automated Suspicion: The EU's new travel surveillance initiatives', *Statewatch* July 2020 https://www.statewatch.org/automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/; 'Deportation Union: Rights, accountability and the EU's push to increase forced removals', *Statewatch* August 2020, https://www.statewatch.org/deportation-union-rights-accountability-and-the-eu-s-push-to-increase-forced-removals/.

[4] 'Automating Society Report 2020; Finland', *Algorithm Watch* 2020 https://automatingsociety.algorithmwatch.org/report2020/finland/.

[5] Zach Whittaker, 'Princeton Identity debuts a new walkthrough biometric scanner – in a shipping container', *Techcrunch* October 2018, https://techcrunch.com/2018/10/09/princeton-identity-walkthrough-biometric-scanner-shipping-container; 'Emirates launches 'biometric' pathway for contact-less passage at Dubai airport', *Gulf News*, 23 October 2020, https://gulfnews.com/uae/emirates-launches-biometric-pathway-for-contact-less-passage-at-dubai-airport-1.74765654

[6] 'Automated Suspicion: the EU's new travel surveillance initiatives', *Statewatch* July 2020, https://www.statewatch.org/automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/

[7] 'Report on the JHA/law enforcement online workshop on the proposed AIA', 30 September 2021, p.5, contained in Council of the EU document 13329/21, 29 October 2021, https://www.statewatch.org/media/3068/eu-council-ai-act-report-law-enforcement-jha-workshop-13329-21.pdf

[8] 'Report on the JHA/law enforcement online workshop on the proposed AIA', 30 September 2021, p.5, contained in Council of the EU document 13329/21, 29 October 2021, https://www.statewatch.org/media/3068/eu-council-ai-act-report-law-enforcement-jha-workshop-13329-21.pdf

[9] Explanatory Memorandum to Commission proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, 1.1 Reasons for and objectives of the proposal

[10] "…the uptake of AI entails a number of potential risks and will bring about considerable socioeconomic changes. The EU must act as one, based on European values, to promote the development and deployment of AI." European Commission, 'How research and innovation contributes to AI policy', undated, https://ec.europa.eu/info/research-and-innovation/research-area/industrial-research-and-

values will be translated into the Act itself will be the subject of lengthy negotiations.

Defining artificial intelligence

Article 3 of the proposal for the AIA defines artificial intelligence as:

"software that is developed with one or more of the techniques and approaches listed in Annex I, and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

Annex I describes these techniques as:

"(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods"

A year after the proposal was published, the AIA has been the subject of substantial public and political attention as it passes through the EU's legislative process (see 'Policy discussions'). Ensuring that the law prevents, regulates and controls the myriad potentially harmful uses of AI for the purposes of immigration and border control is vital, particularly given that the Commission's proposal fell short of hopes it would provide protections against racism, discrimination and unequal power dynamics in the deployment of AI. The development and deployment of AI systems for immigration and border control purposes (such as the automation of control procedures at border crossing points, automated assessment and decision making systems, the use of language and emotion recognition to assess a person's credibility, or the use of extensive surveillance systems to inform predictive analytics) already shows how existing discriminations can be exacerbated through the use of supposedly sophisticated technology.

In November 2021, 114 civil society organisations published recommendations for the European Parliament and Council of the EU to use in their considerations of the Commission's proposal.[11] This briefing paper builds on that statement and analyses developments in relation to immigration and border control in order to inform advocacy on the Artificial Intelligence Act. It begins with a brief overview of the main provisions of the Act and highlights some of the shortcomings in relation to the use of AI for immigration and border control purposes. It goes on to examine border AI systems that are either already deployed or in development, assessing how they would be regulated (or not) under the AI Act, in order to highlight the limitations of the proposal. It also provides a snapshot of the border AI technology ecosystem that has been propelled by public research funding. Finally, it provides a brief overview of the key decision-making forums and sites of influence in the EU institutions, in order to clarify both where advocacy and campaigning on the AI Act could focus, and where other border AI initiatives are being discussed.

The proposed AI Act provides a significant opportunity to control and regulate technology in a policy area that puts people at a substantial risk of various rights violations. At the same time, whatever form the final legislation takes, the struggle for migration justice will continue, with potentially dangerous new technologies likely to come under increasing scrutiny. This briefing hopes to contribute to the effort to ensure an AI Act that provides meaningful and robust control over border, asylum and migration AI, at the same time as informing the struggles that will continue beyond the approval of the legislation.

innovation/key-enabling-technologies/artificial-intelligence-ai_en

[11] 'An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement', *EDRi* November 2021, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf.

The AI Act and migration

Managing risk to develop a market

The Act takes a "risk-based approach" to regulating artificial intelligence technologies, with the intention of boosting technological innovation and, thus, economic growth. The explanatory memorandum outlines the aspiration to support "socially and environmentally beneficial outcomes and provide key competitive advantages to companies in the European economy." According to the European Commission, the proposal is "based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them." Fundamental rights protections are, therefore, a vehicle for economic gain – or, in the worst case scenario, seen as a barrier to profit-making. As the following sections will show, when it comes to regulating AI technologies used for immigration and border control, and for home affairs purposes more broadly, upholding rights does not appear to be the first priority.

The proposal categorises AI systems by the level of risk they pose to health and safety and fundamental rights, with three different levels proposed: unacceptable (banned); high risk (use must meet certain requirements); and low risk, or "uses with specific transparency obligations" (permitted as long as they meet those transparency obligations). This of course also implies a fourth category, no risk, which is not addressed by the proposal.

There are also three different categories of users and providers of AI systems to which the Act will apply:

- providers who place on the market or put into use AI systems within the EU, whether or not those providers are established in the EU or elsewhere;
- users of AI systems located within the EU; and
- providers and users of AI systems that are located in a non-EU state, when the output of that system is used within the EU.

The rules will not apply to AI systems developed or used exclusively for military purposes,[12] although this does not preclude AI systems being used for military purposes alongside another purpose. Also excluded from the scope of the rules are public authorities of third countries or international organisations when they use AI systems "in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States."[13]

The proposal does not include particularly stringent obligations in relation to immigration and border control (it is noteworthy that there is no reference to the need to uphold international obligations regarding migration and international protection). AI technologies will be deployed within existing structures of discrimination, inequality, and bias, and without changes to the text, it will be possible to deploy systems that pose significant risks for individuals with limited safeguards, while those using these systems will be under no obligation to assess or even meaningfully understand how they function. It is vital that lawmakers, and the law itself, recognise this problem and impose limits and safeguards on the design and use of AI in high-risk settings – in this case, migration control – accordingly.

Unacceptable risk

The proposal lists four types of AI system deemed to pose an unacceptable risk and which should be prohibited:

- AI systems that use "subliminal techniques… in order to materially distort a person's behaviour in a manner that

[12] Commission Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Annex III, 'High-risk AI systems referred to in Article 2(3) and (4)'

[13] Article 2

causes… that person or another person physical or psychological harm";

- AI systems that exploit "vulnerabilities of a specific group of persons due to their age, physical or mental disability," in order to distort an individual's behaviour in way that causes them or another person physical or psychological harm;
- AI systems used to evaluate trustworthiness based on "social behaviour or known or predicted personal or personality characteristics" (social scoring), where this leads to:
    - detrimental or unfavourable treatment of people or groups in contexts other than those in which the data was originally collected; or
    - where it would be "unjustified and disproportionate";
- the use of real-time biometric identification systems in public places for law enforcement purposes.

There are numerous shortcomings with each of these prohibitions. The prohibition dealing with "subliminal techniques" fails to recognise that any and all distortion and exploitation of behaviour is harmful: any practice that undermines the essence of a person's autonomy causes harm.[14] The point regarding "vulnerabilities," meanwhile, only considers age and physical or mental disability as factors of vulnerability. As a starting point, the Act should consider all sensitive or protected characteristics as potential indicators of inequality (and therefore higher risk of vulnerability), including age, gender or gender identity, racial or ethnic origin, health status, sexual orientation, sex characteristics, social or economic status, employment status, migration status, and disability.[15] A more extensive list of factors indicating a risk of vulnerability is particularly crucial in the context of immigration and asylum proceedings.

The use of AI by or on behalf of public authorities to evaluate trustworthiness based on social behaviour only covers such systems where the "social score" leads to detrimental treatment in social contexts unrelated to the context in which the data was generated or collected, or otherwise unjustified or disproportionately detrimental or unfavourable treatment. Were such systems used in identity assessments, or decisions on a person's asylum claim (examined in 'Automated assessments and decision making', below), the information would be collected in the context for which it were used, yet could also lead to disproportionately detrimental or unfavourable treatment. Nor is it clear how it might be determined whether social scoring is "unjustified and disproportionate."

The prohibition on real-time biometric identification (RBI) in publicly-accessible spaces for law enforcement authorities, meanwhile, is not really a prohibition at all – there are three situations in which the ban does not apply. If considered "strictly necessary," real-time biometric identification can be used in a targeted search for potential victims of crime, prevention of threat to life or physical safety, or for finding and identifying a perpetrator or suspect of certain criminal offences.[16] The carve-out is extensive: member states may in fact "fully or partially authorise the use of 'real-time' remote biometric identification (RBI) systems in publicly accessible spaces for the purposes of law enforcement," for any of the three purposes outlined above, provided that they meet a number of conditions and safeguards set out in the proposal.

The broad exceptions to the prohibition, as well as the fact that retrospective RBI identification (for example, through the use of a system that runs CCTV footage against a facial recognition algorithm) is not prohibited despite being equally invasive, undermine the proportionality and

[14] 'An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement', *EDRi* November 2021, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf.

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 9, https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e2051-1-1.

[16] Article 5(d)

necessity principle set out in the EU Charter of Fundamental Rights. This principle requires any limitation on rights and freedoms to meet objectives of genuine interest or to protect the rights and freedoms of others.[17]

Furthermore, the partial prohibition on the use of remote biometric identification only concerns its use for law enforcement purposes, thus permitting its use for migration, asylum and border management, commercial or other reasons. With regard to risk assessments and profiling in the contexts of asylum and migration control, this poses high risks to the rights to non-discrimination and privacy, as well as procedural rights.

Furthermore, the preamble states that despite being subject to a general prohibition, AI systems "intended to distort human behaviour," or "whereby physical or psychological harms are likely to occur," can still be used for research purposes under certain conditions. Such research will be permitted if it "does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research."[18] If the use of such systems is to be prohibited in 'real life', it is unclear why there is a need to engage in such research.

Finally, the section on systems posing an unacceptable risk does not include a provision that would allow for the list of systems classified as such to be modified.[19] In the way in which the proposal is drafted, any AI system that is not explicitly mentioned is permitted. If there is no way to add to the text further systems or use cases that may be developed in the future, the Commission's claim to have produced a "comprehensive and future-proof"[20] text rings rather hollow.

High risk

The proposed AIA sets out a number of use cases across nine different areas in which the deployment of AI systems is to be considered "high risk". These include AI systems used to ensure the safety of machinery, vehicles and other products; for the real-time and retrospective biometric identification of people; for assessments and decision-making affecting students, employees, and recipients of public benefits and emergency services; and in the case of law enforcement, for emotion detection, crime prediction, and profiling, amongst other things.[21]

In the realm of migration, asylum, and border control, the proposal sets out four use cases to be considered high risk:

- systems to be used to detect the emotional state of individuals;
- systems for assessing "a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person" planning to enter or having entered the EU;
- systems for the verification and authentication of travel and other documents;
- systems to assist the authorities in assessing asylum, visa and residence permit applications.[22]

In order to mitigate the risks posed by these systems, the proposal sets out various obligations for providers and users.[23] The providers of AI systems must, amongst other things:

- establish and maintain a risk management system;
- ensure certain data quality requirements are met;

[17] Charter of Fundamental Rights of the European Union OJ C 326, Article 52(1), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT#d1e774-393-1
[18] Recital 16
[19] 'An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement', *EDRi* November 2021, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf.
[20] Explanatory memorandum to the proposal
[21] Annex III 'High-risk AI systems referred to in Article 6(2)', 6(a-g).
[22] Annex III 'High-risk AI systems referred to in Article 6(2)', 7(a-d).
[23] Title III

- produce thorough and up-to-date technical documentation;
- ensure that systems store logs of their functioning;
- ensure that users are able to "interpret the system's output and use it appropriately" and are provided with detailed and clear instructions;
- make meaningful human oversight possible;
- ensure "an appropriate level of accuracy, robustness and cybersecurity";
- register the system in an EU-wide database that will be set up; and
- meet certain standards and conformity assessment requirements.

Providers based outside the EU must appoint an authorised representative within the EU to ensure these requirements are met,[24] and certain obligations are also placed on importers[25] and distributors.[26]

Meanwhile, users of high-risk AI systems – for example, border control, visa, asylum and immigration authorities – are essentially ordered by the proposal to follow the providers' instructions, ensure that any data they enter into such a system is "relevant", and inform the provider or distributor of the system if they identify that its use may present a risk to health, safety or fundamental rights, or if they identify "any serious incident or any serious malfunctioning."

In relation to risks to health or fundamental rights, users would be required to inform providers and suspend use of systems when they have "reasons to consider that the use in accordance with the instructions… may result in the AI system presenting a risk."[27] However, it does not expand upon what may be included or excluded as a "reason to consider," and there is a precedent in EU border control operations for a very wide margin of appreciation on this matter. For example, EU border agency Frontex suspended its border control operations with Hungary at the start of 2021, following a judgement by the Court of Justice that Hungary's asylum legislation was in breach of EU law and fundamental rights obligations. In this case, the threshold for a "reason to consider" was a court judgement, despite years of criticism of Frontex's involvement at the border by civil society organisations, and "repeatedly expressed concerns about the fundamental rights situation in Hungary" by the agency's Consultative Forum on Human Rights.[28] Frontex continues to assist Hungary in deportation operations, despite the Court of Justice ruling that return operations from the state in 2020 were incompatible with EU law.[29]

Unlike the systems posing an "unacceptable risk", the list of "high risk" systems can be amended by delegated act.[30] This makes it possible to add further AI systems used in any of the above areas, if they pose a risk of harm to health and safety or an adverse impact on fundamental rights.[31] As it stands, the list does not refer to a number of potential or current uses of AI that could negatively affect a person's right to seek asylum, the principle of non-refoulement or the right to leave one's own country. This might cover the use of predictive analytics on migration trends to inform border control operations, or the analysis of "micro-gestures" or emotional reactions to assess the credibility of someone claiming asylum.

The proposal also excludes certain such high risk systems from its scope. In its current form, the text will not apply to AI technologies used as

[24] Article 25
[25] Article 26
[26] Article 27
[27] Article 29(4)
[28] "Frontex: the ongoing failure to implement human rights safeguards", *Statewatch* January 2022, https://www.statewatch.org/analyses/2022/frontex-the-ongoing-failure-to-implement-human-rights-safeguards/
[29] European Parliament, 'MEPs withhold discharge of EU border control agency Frontex's accounts', 31 March 2022, https://www.europarl.europa.eu/news/en/press-room/20220328IPR26301/meps-withhold-discharge-of-eu-border-control-agency-frontex-accounts
[30] A form of additional legislation used to update or amend the law when considered necessary. Delegated acts are drawn up by the Commission but can be revoked or objected to by the Parliament and Council. See: European Commission, 'Implementing and delegated acts', undated, https://ec.europa.eu/info/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_en
[31] Article 7(1)

part of the EU's large-scale IT systems if they were already on the market a year before the Regulation enters into force, unless their mandates are significantly changed in terms of the design or purpose of the AI systems concerned.[32]

Of the numerous systems in question, two – the Visa Information System (VIS) and the European Travel Information and Authorisation System (ETIAS) – will deploy AI systems for the purpose of individual risk assessment. Applications for a visa or travel authorisation are to be parsed by data mining tools that will trawl through previous applications, statistics on overstay and refusal of entry, information from national authorities on security risks, and epidemic disease risks identified by global health bodies, in order to generate "screening rules". These rules will then be used to identify individuals previously unknown to the authorities, but "assumed to be of interest for irregular migration, security or public health purposes due to fact that they display particular category traits."[33]

With no changes to the text, these and other systems that are part of the EU's policing and migration data complex[34] will be excluded from the obligations, safeguards and controls introduced by the AIA, leaving the data of potentially hundreds of millions of foreign nationals subject to practices that would otherwise be prohibited[35]

Low risk

The proposal considers that "AI with specific transparency obligations" – effectively, AI systems considered as low risk – should be permitted, but subject to information and transparency obligations.[36] This includes, for example, notifying humans that they are interacting with an AI system (for instance in the case of 'chatbots'), or that they are being subjected to emotional recognition or biometric categorisation. However, in both these cases the obligation to provide information does not apply if the system is being used to detect, prevent and investigate criminal offences.[37]

[32] Article 83

[33] 'Automated profiling of all travellers' in *Automated Suspicion: the EU's new travel surveillance initiatives*, *Statewatch*, July 2020, https://www.statewatch.org/automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/step-one-making-an-application/

[34] The individual information systems are: the Entry/Exit System (EES), Eurodac, the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN), the European Travel Information and Authorisation System (ETIAS), the Schengen Information System (SIS), the Visa Information System (VIS). However, these systems increasingly do not function as standalone databases – substantial parts of the data they hold is being merged and made available for cross-checking as part of the 'interoperability' initiative. This will see the development of a new biometric identity database (the Common Identity Repository, CIR), a shared Biometric Matching System (sBMS), a European Search Portal (ESP, to be used to query all the systems at once) and a Multiple Identity Detector (MID). Depending on how exactly they work, the sBMS and MID could be considered as AI systems under the proposed AIA, but would also be excluded from its scope if the text remains as it is.

[35] Annex IX, 'Union legislation on large-scale IT systems in the Area of Freedom, Security and Justice'

[36] Title IV

[37] European Commission, 'Shaping Europe's Digital Future', Ares(2021)5674926, 16 September 2021, https://www.statewatch.org/media/2795/eu-com-ai-expert-group-general-presentation.pdf

Technology development and deployment

While the Act does seek to impose limitations on the types of AI system that can be produced and used within the EU, it does so in order to stimulate a market and thus stimulate economic growth. While the passing of legislation on AI technology will prove something of a milestone, stricter regulation could imperil the modus operandi of the private companies, state agencies and research institutes that the AI Act seeks to empower – and which the EU has been helping to empower for some two decades, through its funding for the research and development of new security technologies.

In the realm of immigration and border control, there are a vast range of possible use cases for AI. The section below provides an outline of some existing deployments and developments of 'border AI'; it is followed by an overview of the companies and other institutions involved in the EU's budding border AI ecosystem.

Current initiatives

It appears to be the case that the AI Act is not, in fact, intended to place any substantial limits on the deployment of AI technologies for purposes of immigration and border control. As noted above, the EU's large-scale IT systems, which hold sensitive personal data on hundreds of millions of people, are excluded from the scope of the proposal. The Commission has said it aims to ensure that "not all AI applications are considered automatically high risk," in the area of home affairs, while, to "safeguard public security and the secrecy of investigations", the proposal provides limits on "disclosure and transparency of the AI applications" used by law enforcement and border security agencies.[38]

Perhaps most tellingly, in a presentation to the Commission Expert Group on Artificial Intelligence in the domain of Home Affairs,[39] the Commission declared that the aims of the AI Act in relation to home affairs are "to decrease administrative burden on home affairs authorities in order not to hamper innovation and in-house developments," and "to ensure that the implementation of the EU large-scale IT systems for migration, border management and security are not delayed,"[40] a clear reference to the fact that elements of those systems may end up being exempt from the Act's obligations. Elsewhere, the Commission has suggested that although the requirements of the AI Act will impose additional financial costs, in terms of legislative requirements "there will be virtually no impact on users" in the law enforcement sector.[41]

With this in mind, it is important to take into account the ongoing development and deployment of AI systems for the purposes of immigration and border control – such as ABC gates, automated assessment and decision-making tools, emotion recognition systems, and systems for predictive analytics and border surveillance – in order to identify the potential

[38] Article 70(2)

[39] The group is made up of national authorities, generally interior ministries and police forces, with the task of assisting and advising on the preparation and implementation of legal and policy initiatives on AI relating to home affairs. More information: 'EU: Artificial intelligence expert group in breach of rules of procedure', *Statewatch*, 12 October 2021, https://www.statewatch.org/news/2021/october/eu-artificial-intelligence-expert-group-in-breach-of-rules-of-procedure; European Commission, 'Commission Expert Group on Artificial Intelligence in the domain of Home Affairs (E03727)', undated, https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3727

[40] European Commission, 'Rules on law enforcement, migration and asylum in the AI proposal', Ares(2021)5674926, 16 September 2021, https://www.statewatch.org/media/2793/eu-com-ai-expert-group-presentation-lea-migration-asylum.pdf

[41] 'Report on the JHA/law enforcement online workshop on the proposed AI Act (AIA)', available in 'EU: Artificial Intelligence Act: justice sector and high-risk systems; internal security; migration and borders; comments and presentations', *Statewatch*, 26 January 2022, https://www.statewatch.org/news/2022/january/eu-artificial-intelligence-act-justice-sector-and-high-risk-systems-internal-security-migration-and-borders-comments-and-presentations/

risks of failing to regulate these technologies adequately through the AI Act.

It should be noted that some of the systems considered in this section would not be covered by the AI Act as they are not deployed in or by the EU or its member states, but are included here to illustrate the different types of systems available and the applicability of the AI Act to different technologies.

Automated border control (ABC)

ABC gates are designed to replace manual passport checks, and require a traveller to place their passport into a scanner, which captures an image of the passport's photo page. A 'live' photo is then taken of the traveller's face, the system compares the photo to the image in the passport, and when the algorithm finds a match the gate opens automatically. The gates are already a familiar fixture in airports in many technologically-advanced states around the world.

While the Commission does not classify ABC gates as AI systems, a report produced for Frontex by the RAND Corporation considers the biometric scanning, facial recognition and document authenticity validation functions of these gates as AI applications.[42] A presentation produced by the Commission states that real-time remote biometric identification at "fixed terminals" is considered AI, but identity checks conducted at borders by "bots" and "ABC-gates" are classified as "out of scope of the AI Regulation". It is unclear what justifies this distinction.[43]

In the EU, many ABC gates were first deployed as pilot projects, "intended to test their capability to improve the border crossing processes in aspects such as speed, security, automation, false rejection, reduction, etc.,"[44] before going on to be permanently installed either as private initiatives (for example, as a way for airports to woo business-class travellers, or under the auspices EU's 'smart borders' initiative[45]). Between 2014 and 2018, through the project ABC Gates for Europe (ABC4EU), funded under the EU's security research programme, Frontex assessed existing pilot projects and identified a variety of priority issues, in particular the harmonisation of e-passport management, biometrics, and interoperability of systems, among others.[46]

IDEMIA, a self-professed "global leader in Augmented Identity"[47] has developed 'ID2Travel', in which biometric identity checks are extended to the check-in as well as the border control process.[48] Going one step further, Frontex and the Border Service of Portugal began exploring a system that would both intensify and 'invisibilise' such checks. The 'Biometrics on the Move' project uses e-gates or "biometric corridors" to run facial recognition and touchless fingerprint scanning for passengers leaving the EU, supposedly giving border guards more time for security checks and speeding up the process for travellers.[49] In 2019, AI start-up SenseTime created a "smart security check-in system" for the new Daxing Airport in Beijing, in a move to improve efficiency.[50] The system has also been deployed at a number of other Chinese airports.[51] It uses AI-based facial

[42] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', March 2021, p.28, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

[43] European Commission, 'Rules on biometrics in the AI proposal' Ref.Ares(2021)567492, 16 September 2021, https://www.statewatch.org/media/2794/eu-com-ai-expert-group-presentation-biometrics.pdf

[44] 'ABC Gates for Europe', *CORDIS*, https://cordis.europa.eu/project/id/312797

[45] See 'Funding 'smart borders'' in 'Building the biometric state: Police powers and discrimination', *Statewatch*, February 2022, p.19, https://www.statewatch.org/media/3143/building-the-biometric-state-police-powers-and-discrimination.pdf

[46] 'ABC Gates for Europe', *CORDIS,* https://cordis.europa.eu/project/id/312797

[47] IDEMIA, https://www.idemia.com/our-journey

[48] IDEMIA, 'ID2Travel; facilitating airport passengers' journeys', https://www.idemia.com/id2travel

[49] "Frontex Testing "Biometrics on the Move Border Check Technology at Lisbon Airport', *Schengen Visa Info*, October 2019, https://www.schengenvisainfo.com/news/frontex-testing-biometrics-on-the-move-border-check-technology-at-lisbon-airport

[50] Bonnie Zhang, 'SenseTime's AI Technology Enables Intelligent Security Check-in System', *Pandaily*, January 2019, https://pandaily.com/sensetimes-ai-technology-enables-intelligent-security-check-in-system/

[51] 'SenseTime AI Serves International Travelers at the Newly-opened Beijing Daxing International Airport',

recognition for self-check-in, automatically linking facial features to a passenger's tickets, luggage and ID documents. Tests of the system had a 99% match success rate, using, "the latest IoT [Internet of Things] technology, intelligent photo recognition technology and automatic sorting technology" as well as "AI technology," although it is not clear what form of AI is involved.[52]

While passenger convenience and speed is often touted as the key motive behind e-border initiatives, it is certainly not the only one. In the USA, the long-delayed[53] Biometric Exit Programme aims to use biometric verification at all border crossing points "to identify foreign nationals that stay in the U.S. beyond their authorized periods of admission,"[54] in order "to support the identification of visa overstayers."[55] The EU's forthcoming Entry/Exit System has the same aim of enforcing immigration controls more efficiently.

The RAND report produced for Frontex noted that although facial recognition data used in entry/exit verification programmes could be accessed for law enforcement in breach of data protection regulations, such systems "would enable airport scans to support the identification of overstayers and illegal migrants more rapidly" than manual passport checks.[56]

A roadmap provided in the RAND study anticipates that ABC gates will become "more prominent" as technology is improved. Future such gates will integrate e-gate hardware with document scanning and verification, facial recognition and "other biometric verification", with the ability to alert border guards to "any potential issues of non-compliance" with pre-defined rules. The report sees current capabilities as too reliant on human border guards, recommending a "pathway to adoption" that includes acquiring high-quality images for facial recognition and advancing iris scanning and facial recognition models to "enable systems to function in non-perfect conditions". AI-based sensors and extraction algorithms are expected to lead to higher capability.

All AI-enabled systems that perform biometric identification should be covered by the Regulation so that the relevant safeguards can be applied. AI systems used in migration enforcement should be classified as "high-risk"[57]

SenseTime, 27 September 2019, https://www.sensetime.com/en/news-detail/3898?categoryId=1072

[52] Bonnie Zhang, 'SenseTime's AI Technology Enables Intelligent Security Check-in System', *Pandaily*, January 2019, https://pandaily.com/sensetimes-ai-technology-enables-intelligent-security-check-in-system/

[53] United States Government Accountability Office, 'Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain', 27 February 2017, https://www.gao.gov/products/gao-17-170

[54] United States Government Accountability Office, 'DHS Annual Assessment', March 2022, p.71, https://www.gao.gov/assets/gao-22-104684.pdf

[55] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', March 2021, pp. 97-8, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

[56] Ibid.

[57] 'Artificial Intelligence Act Amendments; Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act', *European Digital Rights*, 9 May 2022, https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf

Automated border control	
Use case	**Classification under AI Act proposal**
Generic ABC gates	Out of scope, although components of such a system may fall under the Act, e.g. automated verification of travel document authenticity would be considered high risk
ID2Travel	Out of scope
Biometrics on the Move	Could be considered as remote biometric identification but would not be considered as high risk if deployed for immigration and border control purposes
"Smart security check-in"	Out of scope, although components of such a system may fall under the Act, e.g. automated verification of travel document authenticity would be considered high risk

Automated assessments and decision making

The use of algorithms to aid decision-making on visa applications, requests for international protection, and immigration detention demonstrates the ways in which automated systems may be unable to deal with nuanced, complicated cases; can make it harder to appeal decisions; and create difficulties in determining responsibility for decision making. Even where systems include a 'human-in-the-loop', the outsourcing of initial impression-forming and the use of machine learning can influence officials' interpretations and ultimate decisions.

A "visa-streaming" algorithm used by the UK Home Office, while not making the ultimate decision on visa applications, categorised applicants based on nationality, placing certain nationalities in a "red" queue, for which applications were processed more slowly than the "green" and "yellow" categories, as well as prompting more intensive assessment.[58] The use of this algorithm was successfully challenged by the digital rights organisation *Foxglove* and the *Joint Council for the Welfare of Immigrants*. Threatened with judicial review, the Home Office agreed to suspend use of the algorithm "pending a redesign of the process and the way in which applications are allocated for decision-making".[59] As outlined by *Foxglove*, the algorithm was fed a "secret list of suspect nationalities", that it would then flag as "high risk", building a "feedback loop" in which "past bias and discrimination, fed into a computer program, reinforce future bias and discrimination."[60]

The EU's long-planned European Travel Information and Authorization System (ETIAS), the Central Unit of which will be managed by Frontex, will perform an electronic pre-screening of travellers exempt from visa requirements coming into the EU. It is part of the EU's interoperability initiative, and therefore connected to other identity databases, and will run a series of automated checks to flag "hits" to national authorities. Automated checks against databases, watch lists and profiling systems will determine whether to permit entry to the Schengen area, as well as checking for any orders for arrest or extradition, use of a lost or stolen passport, and previous visits to Schengen or visa applications.[61] The ETIAS Central Unit

[58] 'We won! Home Office to stop using racist visa algorithm', *JCWI*, August 2020, https://www.jcwi.org.uk/news/we-won-home-office-to-stop-using-racist-visa-algorithm

[59] 'UK: Threat of legal challenge forces Home Office to abandon "racist visa algorithm', *Statewatch*, August 2020, https://www.statewatch.org/news/2020/august/uk-threat-of-legal-challenge-forces-home-office-to-abandon-racist-visa-algorithm/.

[60] 'Home Office says it will abandon its racist visa algorithm – after we sued them', *Foxglove* August 2020, https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/

[61] Article 20, Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations

will access any application files producing "hits" for verification, consulting national authorities and Europol on any data they have supplied to EU databases. In these cases, decisions on applications must be made by officials, with national authorities granted a right of veto; those that do not lead to any "hits" will be processed automatically.[62]

As noted above (see 'High risk') both ETIAS and the Visa Information System (VIS) are to include automated screening and risk assessment processes. "Screening rules" will be used to identify individuals previously unknown to the authorities, but assumed to be of interest due to matching certain character traits deemed problematic. These traits are referred to as "risk indicators" and include age range, nationality, country and city of residence, destination, purpose of travel and occupation. They will be based on data collected and analysed not solely by computers, but by people as well. "Bias may be introduced at each step of the process,"[63] increasing the risk of unwarranted refusals of applications, discrimination or invasions of privacy.

AI-enabled "language biometrics" may also form part of the asylum assessment process, using software to analyse dialects and determine the "true" place of origin of individuals, in order to determine "the potential of false statements" being made by people crossing borders.[64] Automated text and speech recognition has been used by Germany's Federal Office for Migration and Refugees (BAMF) since 2017, using information from people's phones, tablet or laptop to check claims of country of origin.[65] Software designed by the firms Atos and MSAB presents an overview of content extracted, with a language analysis of text retrieved.[66] BAMF also uses software to identify "disguised dialects" by analysing a two minute recording of asylum applicants without an accepted form of identification, delivering a percentage chance of nationality of origin.[67]

To approach the issue of transliteration from Arabic name spelling, BAMF promoted the use of a web-based transcription service, TKS, to transcribe Arabic names "into a consistent Latin script".[68] As of 2018, BAMF has been working with "several European countries" on a pilot project for language and dialect recognition involving exchanges and analysis of speech recordings.[69] The 2022 German Agenda on Digitalisation also foresees the use of automated name transcriptions to forecast countries of origin, as well as the use of speech biometric analysis for Arabic dialects, biometric imaging and the extraction of information from smartphones to try to help identity and determine the country of origin of people requesting international protection.[70] A 2019 evaluation report of BAMF's language analysis noted that

(EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

[62] Articles 22-27, Regulation (EU) 2018/1240, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

[63] European Union Agency for Fundamental Rights, 'Preventing unlawful profiling today and in the future: a guide', 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

[64] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', *Frontex* March 2021, pp.98-99 https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

[65] Leo Thüer, Alexander Fanta and Chris Köver, 'Asylum Procedure: Cell Phone Search Has No Benefits', *Netzpolitik*, July 2018, https://netzpolitik.org/2018/asylverfahren-handy-durchsuchung-bringt-keine-vorteile/

[66] Anna Biselli, 'Software, die an der Realität scheitern muss', *Zeit Online*, March 2017, https://www.zeit.de/digital/internet/2017-03/bamf-asylbewerber-sprach-analyse-software-computerlinguistik; Anna Biselli, 'Eine Software des BAMF bringt Menschenin Gefahr', *VICE*, August 2018, https://www.vice.com/de/article/a3q8wj/fluechtlinge-bamf-sprachanalyse-software-entscheidet-asyl

[67] 'Automating Society Report 2020; Germany', *AlgorithmWatch*, 2020, https://automatingsociety.algorithmwatch.org/report2020/germany/

[68] 'Digitalising the asylum procedure', *Federal Office for Migration and Refugees*, 2020, https://www.bamf.de/EN/Themen/Digitalisierung/DigitalesAsylverfahren/digitalesasylverfahren-node.html

[69] Ibid.

[70] 'Further development of the Migration Asylum Reintegration System (MARiS)' in 'Überblick über die Digitalisie-rungsinitiativen', *BAMF*, 2022, https://www.bamf-digitalisierungsagenda.de/wp-content/uploads/2022/02/220216_Digitisation_initiatives_barrierefrei.pdf

"although more than 90 languages are recognised, not all existing languages are supported by the system… the system will recognise one of the most similar languages."[71] The training data set and algorithms for speech recognition have not been disclosed.

BAMF has analysed data from electronic devices (like mobile phones) since 2017, imposing a legal obligation to comply with requests for access to these devices. In 98% of cases, information found on devices and analysed by software – which checked the country codes of contacts, messages and calls, the country domains of websites accessed, language used in text messages and login names of apps – corresponded with the identities and countries of origin claimed by asylum seekers, but BAMF saw fit nonetheless to spend €11.2 million on the technology between 2017 and 2019. BAMF refused to disclose the algorithms used for this undertaking, making it impossible to verify the reliability and significance of findings.[72]

Based on the ratio of confirmation to contradiction found by the system, its use and invasiveness seems disproportionate to pursue the aim of preventing erroneous asylum grants. However, were the algorithm to incorrectly identify a contradiction, the individual in question would be distrusted by the authorities they came into contact with afterwards, jeopardising their asylum claim. Additionally, geo-data from smart devices (it is not clear which apps this information can be obtained from) and from photos on the device are used to plot points on a map, potentially allowing officials to establish migratory routes, which could be used to inform border control operations (see "predictive analytics" below). In 2021, the searching of mobile phones during asylum applications was deemed unlawful in a case put to the regional court in Berlin, which decided that BAMF had demanded access to mobile phone data too early in an individual's application, and had unnecessarily stored information obtained from it.[73]

The Horizon 2020 project TRESPASS,[74], which received almost €8 billion in public funding, claimed to be developing a similar system for border control purposes. It aimed to use "data fusion" and "risk analysis" services to analyse biometric information, sensor information, data from travel documents and applications, along with database scans to calculate a risk level for individual travellers at official border crossing points.[75] A research paper produced by project participants proposed "an algorithm to compute an abnormal behaviour score in real-time," that would be used to determine which individuals should be subject to closer scrutiny at border crossing points.[76] Three pilots of the model were run: at Schipol airport in Amsterdam; at a land border crossing point in Poland; and in Piraeus, Greece, to carry out risk-based screening of cruise travellers.[77]

Such algorithm-based risk assessments are used in the USA to make decisions about immigration detention, assessing risk of absconding during a review and return process based on variables including age, country of origin, and previous application history. The risk assessment software used by the USA's Immigration and Customs Enforcement (ICE) was amended to conform to the "zero-tolerance" stance on immigration adopted under the Trump administration, resulting in its automatic

[71] Anna Biselli, Lea Beckmann, 'Invading Refugees' Phones: Digital Forms of Migration Control in Germany and Europe', *Gesellschaft für Freiheitsrechte*, February 2020, https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf

[72] Ibid.

[73] 'Berlin court rules searching phone of asylum-seeker was unlawful', *Deutsche Welle*, June 2021, https://www.dw.com/en/berlin-court-rules-searching-phone-of-asylum-seeker-was-unlawful/a-57750301

[74] 'RobusT Risk basEd Screening and alert System for PASSengers and luggage', *CORDIS*, https://cordis.europa.eu/project/id/787120

[75] 'Technical Framework', *TRESPASS*, 2018, https://www.tresspass.eu/Technical-Framework

[76] S. Vora, M. Shahriari, Stelios C. A. Thomopoulos, L. Fischer, T. Hoch, 'A scoring algorithm for abnormal traveller behaviour in border crossing areas', *SPIE Digital Library*, 20 September 2020, https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11542/2573963/A-scoring-algorithm-for-abnormal-traveller-behaviour-in-border-crossing/10.1117/12.2573963.full

[77] 'Pilots', *TRESPASS*, 2018, https://tresspass.eu/Pilots

recommendation of detention for anyone apprehended crossing a border or in the country illegally.[78] While final decisions on detention are still made by a human deportation officer, the removal of the "release" recommendation was followed by a more than 300% increase in detainees.[79]

Automated individual risk assessment systems pose grave risks to the rights to privacy, non-discrimination, data protection and procedural rights and should be prohibited. Mobile device data extraction and analysis systems may also have substantial negative effects on those same rights, yet do not fall within the scope of the proposal; they should be classified as high-risk. Equally, it must be ensured that the exemption the proposal grants to the AI components of the EU's large-scale IT systems is not maintained in the final legislation, and that they be treated as a high risk to fundamental rights.

Automated assessments and decision making

Use case	**Classification under AI Act proposal**
"Visa streaming"	High risk
Profiling via ETIAS	Exempt (would otherwise be high risk)
Profiling via VIS	Exempt (would otherwise be high risk)
Dialect and accent recognition	High risk
Mobile device data extraction and analysis	Out of scope
TRESPASS	High risk
Detention risk assessment	High risk (if considered as an AI system intended to be used to assess individual risk)

Emotion recognition

iBorderCtrl, a €4.5 million Horizon 2020 research project, analysed "micro gestures" during interviews with travellers via an Automatic Deception Detection System (ADDS), intended to support risk assessments, though human border officials would be "involved" in the final decision on allowing or denying entry. Pilot projects saw automated lie detectors introduced temporarily at airports in Hungary, Greece and Latvia, flagging certain individuals for questioning by a human border officer. A journalist who was given the chance to test the system immediately triggered a number of false positives.[80] The same technology, analysing facial movements, speech and body language has also been pitched to verify an individual's vulnerability, the outcome of which would determine whether a person's application was expedited, or if they were referred to medical, mental health or other services, and would also influence decisions on detention.[81]

The project has by now become somewhat notorious, and the subject of substantial attention from human rights campaigners. A petition to the Greek parliament by *Homo*

[78] Mica Rosenberg, Reade Levinson, 'Trump's catch-and-detain policy snares many who have long called US home', *Reuters Investigates*, June 2018, https://www.reuters.com/investigates/special-report/usa-immigration-court/; Daniel Oberhaus, 'ICE Modified its 'Risk Assessment' Software so it Automatically Recommends Detention', *Vice*, June 2018, https://www.vice.com/en/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention

[79] Daniel Oberhaus, 'ICE Modified its 'Risk Assessment' Software so it Automatically Recommends Detention', *Vice*, June 2018, https://www.vice.com/en/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention

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

[81] *Deloitte & European Commission, Directorate-General for Migration and Home Affairs*, 2020, p. 24-26, https://data.europa.eu/doi/10.2837/1116.

Digitalis called for a data protection assessment of iBorderCtrl, pointing out the lack of transparency in the system.[82] Green MEP Patrick Breyer launched a legal challenge against the European Commission's Research Executive Agency over their refusal to release the project consortium's ethical assessments of the system, resulting in the release of some redacted documents.[83]

Aside from the technological developments sought by the project, a portion of its funding went towards lobbying for new legislation to allow its deployment following the research stage.[84] Commission publicity claimed that iBorderCtrl was a research project and did not envisage the piloting or deployment of a functioning system, but a redacted communications plan published by Patrick Breyer in 2021 details the research consortium envisaging ways to "foster such legal reforms" as were needed to create the statutory legal basis required to actually use so-called deception detection technologies at borders[85] – a clear attempt to try to overcome what the RAND report refers to as "barriers" to the adoption of AI technology. Such activities included various "dissemination activities" to members of parliament, border authorities, and the Commission. The documents also demonstrated the consortium's caution around public messaging due to ethical concerns, leaning towards lower public messaging as "a controversial public debate might also even hamper the implementation of policies required for iBorderCtrl."[86]

Meanwhile, Frontex is looking into automated, real-time "truth assessments" offered by the AVATAR system, which analyses eye movements, changes in voice, posture or facial gestures to identify "untruthful or potential risk individuals".[87] AVATAR has been piloted in Canada and Romania, where automated decision making was used to try to detect signs of lying in facial movements, increasing the complexity of questions asked to individuals the more "sceptical" the machine became, based on their answers, before referring those deemed suspicious to a human border officer (who will understand from the referral that this person is "suspicious").[88]

What is not clear, and seems unlikely given what is known of the bias built into automated decision making, is whether these algorithms consider communication differences across different cultures and languages, or whether they account for the impacts of trauma on memory and communication. Is it even possible for such a system to take cultural differences into account, given it could not "know" the cultural background of the person it is dealing with?

AI polygraphs in the migration context represent an unacceptable risk to rights to non-discrimination, with a high likelihood of

[82] 'ΑΝΑΦΟΡΑ', *Homo Digitalis*, November 2018, https://www.homodigitalis.gr/wp-content/uploads/2018/11/05.11_HomoDigitalis_Petition_iBorderCtrl.pdf

[83] 'Immigration, iris-scanning and iBorderCTRL', *EDRi*, February 2020, https://edri.org/immigration-iris-scanning-and-iborderctrl/; 'Automated technologies and the future of Fortress Europe', *Amnesty International*, March 2019, https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/; 'Homo Digitalis files a petition to the Greek Parliament concerning the use of the "IBORDERCTRL" system in the Greek borders', *Homo Digitalis*, November 2018, https://www.homodigitalis.gr/en/posts/3044

[84] Patrick Breyer, 'Big Brother "video Lie Detector": EU Research Funds Are Misused to Lobby for Legislative Changes', *Patrick Breyer*, April 2021, https://www.patrick-breyer.de/en/big-brother-video-lie-detector-eu-research-funds-are-misused-to-lobby-for-legislative-changes/

[85] 'P-003504/2021 Answer given by Ms Johansson on behalf of the European Commission', *European Commission*, September 2021, https://www.europarl.europa.eu/doceo/document/P-9-2021-003504-ASW_EN.html

[86] Patrick Breyer, 'Big Brother "video Lie Detector": EU Research Funds Are Misused to Lobby for Legislative Changes', *Patrick Breyer*, April 2021, https://www.patrick-breyer.de/en/big-brother-video-lie-detector-eu-research-funds-are-misused-to-lobby-for-legislative-changes/

[87] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', March 2021, p.100, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf; Jeff Daniels, 'Lie-detecting computer kiosks equipped with artificial intelligence look like the future of border security', *CNBC*, May 2018, https://www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-border-security.html

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

misinterpreting cultural signifiers and using problematic assumptions grounded in Western understandings of truthfulness or deception, and with unsubstantiated scientific foundations.[89] The use of emotion recognition systems risks undermining the right to privacy, freedom of thought, the right to asylum, a fair trial, effective remedy and other procedural rights. Emotion recognition and deception detection should be prohibited by the AI Act in the context of immigration, asylum and border control.

Emotion recognition	
Use case	**Classification under AI Act proposal**
iBorderCtrl	High risk
AVATAR	High risk

Predictive analytics

In the realm of immigration and border control, predictive analytics can be used to pre-empt migratory movements in order to predict future demand on states' asylum systems (for example by the EU Agency for Asylum, EUAA), inform border control operations (by agencies such as Frontex) or humanitarian or aid responses (by agencies such as the International Organization for Migration or UNHCR, the UN refugee agency).

The EUAA, when it was still known as the European Asylum Support Office (EASO), pursued this goal by feeding an algorithm with information from countries of origin and transit, data scraped from social media, real-time information on arrivals at the EU's external borders, and data on previous outcomes of asylum applications in the EU.[90] The aim was to provide predictions on likely numbers of asylum applications a month in advance, as well as medium-term scenarios. The European Data Protection Supervisor (EDPS) declared EASO's scraping of social media data as putting "individuals' rights and freedoms at significant risk," going beyond any individual's reasonable expectations of how their data might be used and compromising the principle of purpose limitation in a way that the data subjects "could not reasonably anticipate."[91] A 2022 academic paper on the same topic lists an EASO staff member as co-author, indicating that there is still interest in trying to predict the movement of asylum-seekers.[92]

Frontex has maintained a high interest in this controversial practice through its role in the research projects MIRROR and PERCEPTIONS. Even after the EDPS put a stop to EASO's social media scraping, Frontex showed MEPs visiting its headquarters how it monitored social media "in order to be aware of groups of persons organising in order to move towards the EU external borders," as part of its drive for "comprehensive situational awareness."[93] The agency's most recent work programme refers more obliquely to "media monitoring and reporting including open-source intelligence (OSINT)."[94]

The International Organisation for Migration (IOM), meanwhile, uses a 'Displacement

[89] 'Artificial Intelligence Act Amendments; Uses of AI in migration and border control', https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf

[90] Alexander Fanta, 'Data watchdog raps EU asylum body for snooping', *EUobserver*, December 2019, https://euobserver.com/migration/146856

[91] 'Formal consultation on EASO's social media monitoring reports (Case 2018-1083)', *European Data Protection Supervisor*, 2019, https://www.statewatch.org/media/documents/news/2019/dec/eu-edps-reply-easo-ssm-12-19.pdf

[92] Marcello Carammia et. al., 'Forecasting asylum-related migration flows with machine learning and data at scale', *Nature Scientific Reports*, 2022, 12:1457, https://www.nature.com/articles/s41598-022-05241-8.pdf

[93] 'Borders, budgets and beyond: LIBE report sheds new light on Frontex's priorities for implementing its new mandate', *Statewatch*, July 2020, https://www.statewatch.org/news/2020/july/borders-budgets-and-beyond-libe-report-sheds-light-on-frontex-s-priorities-for-implementing-its-new-mandate/

[94] Frontex, 'Single Programming Document 2022-2024', 16 December 2021, p.37, https://frontex.europa.eu/assets/Key_Documents/Programming_Document/2022/Single_Programming_Document_2022_2024.pdf

Tracking Matrix'[95] that "allows agencies to infer migration patterns via locatable mobile phone call records, IP addresses, or geotagged social media activity drawn from private-sector data sources."[96] UNHCR has also used biometric information of individuals in its datasets of over eight million individuals, sometimes "retrofitting" old data with newly obtained biometric information.[97]

EU research projects have also sought to advance the technology available for predictive analytics. ARESIBO (Augmented Reality Enriched Situation awareness for Border security), which has received nearly €7 million in public funding and is led by the multinational aerospace and military company Airbus, aims to "optimise the collaboration between human and sensors (fixed and mobile)", to use "deep learning techniques" to merge disparate data sets, and to provide "real time situation understanding and threat analysis for future actions."[98] The system would use augmented reality techniques to provide operators with a situational awareness picture for specific missions, with tests planned in Finland, Greece, Romania and Portugal.

AI-based predictive analytic systems must be classified as "high-risk" under the Act due to the risks posed to life, liberty and security of the person, non-discrimination, privacy, data protection and the right to asylum, and be subjected to the safeguards provided by the Act.[99] Additionally, the use of predictive systems in combination with wider surveillance infrastructure at borders poses the risk of their being used in the practice of pushbacks when deployed with the aim of combatting "irregular migration".[100]

As such, deployments of predictive analytic systems for certain purposes amount to an unacceptable risk to fundamental rights and therefore must be prohibited insofar as such systems are used to interdict, curtail or prevent movement.

Predictive analytics	
Use case	**Classification under AI Act proposal**
EASO algorithm	Low risk
MIRROR	Low risk
PERCEPTIONS	Low risk
Displacement Tracking Matrix	Low risk
UNHCR biometric identification system	Out of scope
ARESIBO	Low risk

Border surveillance

A key part of the fortification of borders in states across the globe in recent years has been through the widespread deployment of surveillance equipment: standard and thermal-imaging cameras, movement and heat sensors,

[95] IOM, 'Displacement Tracking Matrix', https://dtm.iom.int/
[96] Stefaan G. Verhulst and Andrew Young, 'The Potential and Practice of Data Collaboratives for Migration', *Stanford Social Innovation Review*, 29 March 2018, https://ssir.org/articles/entry/the_potential_and_practice_of_data_collaboratives_for_migration
[97] Petra Molnar, 'Technology on the margins: AI and global migration management from a human rights perspective', *Cambridge International Law Journal*, 8(2), pp.305-330, https://rai2022.umlaw.net/wp-content/uploads/2022/02/19_Technology_on_the_margins_AI_and_global.pdf
[98] 'AR for field and C2 activities', *ARESIBO*, https://aresibo.eu/; 'ARESIBO', *CORDIS*, https://cordis.europa.eu/project/id/833805
[99] 'Artificial Intelligence Act Amendments; Uses of AI in migration and border control', https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf
[100] 'Artificial Intelligence Act Amendments; Uses of AI in migration and border control', https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf

and other remote monitoring tools. In the EU, the connection of a variety of surveillance technologies to the European Border Surveillance System (EUROSUR) is, in part, intended to inform the type of predictive analytics discussed above. However, it can also be used to direct more immediate interventions – for example, when a drone spots a boat in distress in the Mediterranean and its location is provided to the so-called Libyan Coast Guard.[101] Intrusive surveillance systems and technologies are also a regular feature of immigration detention centres and other facilities used to house refugees and migrants.

A partly-automated surveillance system named 'Centaur' is planned for the Greek islands of Lesvos, Chios, Samos, Leros and Kos, where drones will be used to monitor the revamped 'hotspots' (now known as "closed controlled centres") in order "to detect incidents." Alarms and cameras will be placed at the camp perimeters, and control gates will be fitted with metal detectors, integrated cameras and x-ray machines.[102] The system will make use of "a motion analysis algorithm (AI Behavioral Analytics)," according to a Greek government presentation cited by *Algorithm Watch*.[103]

The use of integrated, interconnected surveillance technologies in the Greek hotspots is something of a microcosm of EUROSUR. Operated by Frontex, EUROSUR has evolved from a system justified as a way to help save lives a sea, to one promoted for its role in "combatting illegal migration and cross-border crime".[104] Data uploaded to EUROSUR by member state authorities and from surveillance activities by planes, boats and drones, *inter alia*, is combined with other sources to produce risk analyses and assessments to inform strategic decision making and operational activities.[105] The 2019 Frontex Regulation allows Frontex to also include data gathered within the EU, from hotspots and on "unauthorised secondary movements", in its "European situation picture".[106]

The deployment of new surveillance technologies, as with the construction of fences and barriers to block common migration routes, is intimately linked to increased danger and death for people on the move. At the US-Mexico border, constructions known as sentry towers or surveillance towers provided by the military and security contractor Anduril Industries make use of "fully unmanned integrated hardware and software surveillance systems," which runs "autonomous detection and classification of objects, contributing to threat analysis." This provides border authorities with "automated surveillance of border crossings for threats… [requiring] very little intervention from human operators".[107] This increase in surveillance has led to a higher number of people dying as they attempt to cross the border: "There is an increased correlation between this technology and more deaths, as desperate people try to find ways into country," Dinesh McCoy, a lawyer with *Just Futures Law*, told *The Washington Post*.[108]

Both the public and private sectors have long recognised the ways in which drones could massively boost border surveillance

[101] 'Drones for Frontex: unmanned migration control at Europe's borders', *Statewatch*, February 2020, https://www.statewatch.org/analyses/2020/drones-for-frontex-unmanned-migration-control-at-europe-s-borders/
[102] Carina Petridi, 'Greek camps for asylum seekers to introduce partly automated surveillance systems', *Algorithm Watch*, April 2021, https://algorithmwatch.org/en/greek-camps-surveillance; Marion MacGregor, 'Greece: Migrant camps surrounded by concrete walls', *InfoMigrants*, September 2021, https://infomigrants.net/en/post/32834/greece-migrant-camps-surrounded-by-concrete-walls
[103] Carina Petridi, 'Greek camps for asylum seekers to introduce partly automated surveillance systems', *Algorithm Watch*, April 2021, https://algorithmwatch.org/en/greek-camps-surveillance
[104] Preamble, paragraph 28, Regulation (EU) 2019/1896 on the European Border and Coast Guard
[105] Frontex, 'Situational awareness and monitoring', https://frontex.europa.eu/we-know/situational-awareness-and-monitoring/monitoring-risk-analysis/
[106] Article 26, Regulation (EU) 2019/1896 on the European Border and Coast Guard
[107] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', March 2021, p.115, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf
[108] Nick Miroff, 'Powered by artificial intelligence, 'autonomous' border towers test Democrats' support for surveillance technology', *Washington Post*, 11 March 2022, https://www.washingtonpost.com/national-security/2022/03/11/mexico-border-surveillance-towers/

capabilities.[109] One EU research project, ROBORDER, sought to develop a "fully-functional autonomous border surveillance system with unmanned mobile robots", to be deployed in the air, on the ground, and on and underwater.[110]

The project claims it will use "enhanced detection capabilities" to feed into a radar network accessible by border authorities and operational personnel via a control room, with "early identification of criminal activities at border and coastal areas" identified through thermal and optical cameras, radars, and a host of different sensors.[111] The project, which received almost €8 million in public funding, ended in August 2021.[112] According to the RAND report commissioned by Frontex, it still required further testing and investment in 2021.[113] A more recent border drone project, BORDERUAS, claims to be developing a "lighter-than-air" surveillance vehicle, for which it has received almost €7 million in public funding.[114] It is due to complete its work in November 2023.

In a similar futuristic vein, the FOLDOUT project promised to "[fuse] information from multiple heterogeneous sensors (including ground and airborne)" to provide "through-foliage" surveillance in order to detect "illegal cross-border activities" at the EU's external borders.[115] This continues an initiative previously pursued by Frontex, which in 2014 commissioned a study into "under-foliage detection."[116] FOLDOUT claimed it would combine data "from various sensors to give a complete situation threat assessment combined with suggested reaction scenarios," with pilots and demonstrations at sites in Bulgaria, Greece, Finland, Lithuania and French Guiana.[117]

In its roadmap for the deployment of surveillance towers, the RAND report suggests that the "pathway to adoption" rests upon "testing and refinement of the technology," in order to develop towers that are "better integrated with sensors" for comprehensive, fully autonomous situational awareness.[118] This would include Frontex testing such technologies in "a European context", considering "any regulatory issues to address to allow testing".[119] RAND's roadmap for small unmanned aerial systems (sUAS) foresees the integration of AI technologies to provide real-time automatic target detection and geolocation to border guard patrols, with sUAS operating autonomously through AI-enabled technology.[120] The roadmap for geospatial data analysis aims for a future scenario in which AI enables an "integrated real-time tracking and threat identification system that can improve planning and logistics in border security."[121] How the word "threat" should be interpreted, and how such threats might be dealt with, is not discussed in the report.

Given the elevated risk of violation of fundamental rights and the broader structural injustices and inequalities that surround their use, all AI systems that are part of border surveillance systems should be classified as

[109] 'Eurodrones, Inc', February 2014, pp.30-32, 65-73, https://www.statewatch.org/media/documents/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf
[110] 'ROBORDER', https://roborder.eu/
[111] *Border Security Report* 27, September/October 2021, https://border-security-report.com/wp-content/uploads/2021/09/BSRSepOct2021.pdf
[112] 'ROBORDER', *CORDIS*, https://cordis.europa.eu/project/id/740593/results
[113] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', March 2021, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf
[114] 'BORDERUAS', *CORDIS*, https://cordis.europa.eu/project/id/883272
[115] FOLDOUT, 2022, https://foldout.eu/
[116] 'Seeing through trees: Frontex commissions study on "solutions for under-foliage detection"', *Statewatch*, 17 February 2014, https://www.statewatch.org/news/2014/february/seeing-through-trees-frontex-commissions-study-on-solutions-for-under-foliage-detection/?aid=33257
[117] 'FOLDOUT', *CORDIS*, https://cordis.europa.eu/project/id/787021
[118] Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', *Frontex* March 2021, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf, p. 112
[119] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', March 2021, p.112, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf
[120] Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', p. 121
[121] Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', p.137

“high-risk” and subject to the accompanying fundamental rights impact assessments and transparency obligations.

Border surveillance	
Use case	**Classification under AI Act proposal**
Centaur	Low risk
EUROSUR	Low risk
Sentry towers	Low risk
ROBORDER	Low risk
BORDERUAS	Low risk
FOLDOUT	Low risk

Summary of recommendations

Type of system	Recommendation
Automated border control (ABC)	All AI-enabled systems that perform biometric identification should be covered by the Regulation, and relevant safeguards applied. Such AI systems used in migration enforcement, like e-gates and any remote biometric recognition as discussed above, should be classified as "high-risk".
Automated assessments and decision making	The fact that dialect and accent recognition, and mobile device data extraction and analysis are out of the scope of the Act is a major issue which will have negative impacts on people's rights to private and family life, non-discrimination, data protection and procedural rights. They should be included, along with other forms of risk profiling in the context of migration, in the list of prohibited practices under Article 5.
Emotion recognition	AI polygraphs in the migration context represent an unacceptable risk to rights to non-discrimination, with a high likelihood of misinterpreting cultural signifiers and using problematic assumptions grounded in Western understandings of truthfulness or deception, and with unsubstantiated scientific foundations. The use of emotion recognition systems risks undermining the right to privacy, freedom of thought, the right to asylum, a fair trial, effective remedy and other procedural rights. Emotion recognition and deception detection should be included in prohibited uses of AI.
Predictive analytics	AI-based predictive analytic systems must be included as "high-risk", for the risks posed to life, liberty and security of the person, non-discrimination, privacy, data protection and the right to asylum, and be subjected to the safeguards provided by the Act for high-risk systems. Additionally, the use of predictive systems in combination with wider surveillance infrastructure at borders, posing the risk of their being used in the practice of pushbacks when deployed with the aim of combatting "irregular migration". As such, deployments of predictive analytic systems for certain purposes amount to an unacceptable risk to fundamental rights and therefore must be prohibited insofar as such systems are used to interdict, curtail or prevent movement.
Border surveillance	Given the elevated risk of violation of fundamental rights and broader structural injustices, all AI systems that are part of a border control and management system should be classified as "high-risk", with the accompanying fundamental rights impact assessments and transparency obligations.

A publicly-funded border AI ecosystem

No matter what form the final Act takes, its approval will only mark the beginning of a longer struggle over the control and regulation of AI technologies in sensitive areas such as asylum, migration and border control. The RAND report cited in the previous section correctly refers to the widespread and serious human rights and ethical concerns regarding AI technologies in these areas. However, it goes on to argue for "incentivising informed public debate" on the increased use of AI "to further address public concerns and lack of trust in AI and its applications in border security and law enforcement,"[122] whilst calling for the removal of the protections intended to protect rights and uphold ethics: "Legislations and regulations appear to be the barriers that technology developers will need to overcome to ensure the use of their AI-based solution."[123]

There is already extensive corporate lobbying on the AI Act,[124] and the further development of novel and potentially invasive technologies is likely to spur further calls from the private sector for regulatory and legal changes. It is thus vital that campaigners and advocates are aware of ongoing research and development into new technologies, and the institutions and funding streams driving these processes.

As noted in the section above, a number of EU research projects have sought to advance the use of AI technology for immigration and border control purposes. The EU is the largest provider of public research funding in the world, with the current programme, Horizon Europe (2021-27), worth a total of €93 billion. A small but substantial element of the programme, worth €1.4 billion, covers 'civil security', which includes topics such as policing, critical infrastructure protection, cybersecurity and border control. It is through this security research programme that these projects have been provided with funding, and over the last decade-and-a-half the programme has provided hundreds of millions of euros for this purpose.

[122] RAND Europe, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', March 2021, p.57, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

[123] Artificial Intelligence-Based Capabilities for the European Border and Coast Guard; final report', p.51

[124] Alina Yanchur et. al., 'Computer says No: How the EU's AI laws cause new injustice', *EUobserver*, 23 August 2021, https://euobserver.com/investigations/152695

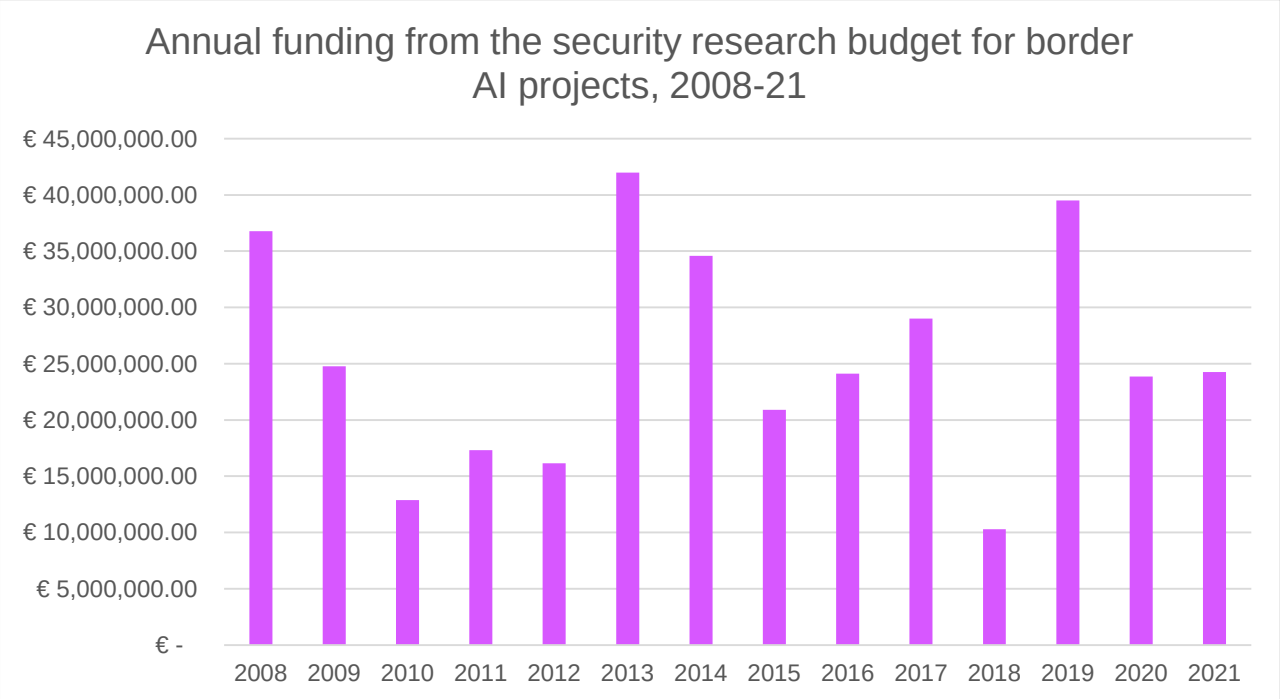
Overview

An analysis of the data on security research funding from 2007 to 2020 carried out by *Statewatch* shows that just over €341 million in public funding has gone towards a total of 51 projects seeking to develop new technologies for the purposes of immigration and border control that involve some element of 'artificial intelligence'. These include autonomous border control robots, biometric identification and verification technologies and automated data-gathering and analysis systems.

Of the total of €341 million dedicated to border AI projects, just over €181 million was distributed under the Seventh Framework Programme for Research & Development (FP7, running from 2007 until 2013), and just over €160 million as part of Horizon 2020 (H2020, 2014 until 2020). The current research programme, Horizon Europe (2021-27) is set to continue the trend for the development of novel immigration and border control technologies, with the first work programme for Horizon Europe offering some €55 million for "border management" topics.[125]

EU research funding for border AI from FP7 (2007-13) and H2020 (2014-20)

Institution type	Total funding €	Number of participations	Funding %
Private companies	€162,627,520	187	48%
Research institutes	€78,403,180	66	23%
Higher education institutions	€54,391,797	62	16%
Public bodies	€39,522,887	62	12%
Other	€6,220,481	6	2%
Total	**€341,165,865**	**383**	**100%**



[125] European Commission, 'Horizon Europe Work Programme 2021-2022 – 6. Civil Security for Society', C(2021)9128, 15 December 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf

Geographic distribution

The geographic distribution of funding also shows that 'frontline' southern EU member states are some of the biggest recipients of security research funding for border AI: Spain is home to institutions that have received a total of €44.3 million since 2007; Italy, €38.3 million; and Greece, €35.9 million. While the border politics of EU member states cannot be seen as a determinant of how much funding they receive under the research programme, the data may be indicative of enthusiasm amongst institutions in those member states to contribute to the development of new border security 'solutions'. The substantial increase in funding awarded to Greek institutions during the Horizon 2020 period (2014-20), during the 'migration crisis', provides further weight to this hypothesis.

Top 10 countries by total amount of border AI research funding received

Country	Funding FP7	Funding H2020	Funding total
Spain	€34,687,558.13	€9,625,575.06	€44,313,133.19
France	€25,346,752.54	€16,399,881.09	€41,746,633.63
Italy	€24,171,382.77	€14,177,213.56	€38,348,596.33
Greece	€15,089,971.83	€20,783,446.78	€35,873,418.61
Germany	€12,994,081.76	€14,317,003.19	€27,311,084.95
UK	€9,406,066.31	€10,978,682.46	€20,384,748.77
Finland	€9,952,994.83	€6,868,715.50	€16,821,710.33
Portugal	€7,475,537.76	€9,211,839.69	€16,687,377.45
Belgium	€4,536,718.80	€ 10,431,216.52	€14,967,935.32
Austria	€4,875,762.35	€6,839,551.25	€11,715,313.60

Private companies

According to data published by the EU, the majority of funding for the projects examined for this briefing has gone to private companies, who received almost €163 million (48% of the total). This is consistent with other areas of security research,[126] and suggests that – at least within the network of organisations funded by the EU's research programmes – the private sector has consolidated its leading role in the development of border AI technologies. However, many of these companies are also closely tied to public authorities: Spain's state-owned holding company owns almost 19% of the shares in Indra, and was recently authorised to increase that to 28%;[127] Isdefe is owned by the Spanish state;[128] the Italian state owns 30% of shares in Leonardo (formerly Finmeccanica);[129] while according to *Corporate Watch*, Israel Aerospace Industries "is the largest state owned defence and aerospace company in Israel."[130]

Top 20 private company recipients of EU security research funding for border AI projects

Institution	Country	FP7 projects	H2020 projects	Total funding
Indra Sistemas	Spain	ABC4EU MOBILEPASS PERSEUS SCIIMS SEABILLA		€ 7,965,160
Ingenieria de Sistemas para la Defensa de España (Isdefe)	Spain	CLOSEYE OPARUS PERSEUS	PROMENADE	€ 7,388,556
Naval Group	France	I2C PERSEUS	CAMELOT COMPASS2020 EFFECTOR	€ 5,610,240
Vision Box	Portugal	ABC4EU	iMARS Smart-Trust	€ 5,106,097
Leonardo	Italy	FIDELITY SUNNY	MARISA PROMENADE RANGER	€ 3,292,592
Engineering – Ingegneria Informatica	Italy	PERSEUS	ANDROMEDA EFFECTOR MARISA	€ 3,278,814
Israel Aerospace Industries	Israel	OPARUS TALOS		€ 2,965,049
Gscan	Estonia		SilentBorder	€ 2,844,875
Veridos	Germany	FASTPASS MOBILEPASS	D4FLY PROTECT	€ 2,741,780
Satways	Greece	PERSEUS	ANDROMEDA EFFECTOR MARISA	€ 2,661,162

[126] 'Market Forces: The development of the EU security-industrial complex', *Statewatch/Transnational Institute*, August 2017, http://statewatch.org/marketforces/

[127] Alfonso Muñoz Fernández, 'El Gobierno autoriza a la SEPI a incrementar su participación en Indra hasta el 28%', *El Español*, 22 February 2022, https://www.elespanol.com/invertia/empresas/tecnologia/20220222/gobierno-autoriza-sepi-incrementar-participacion-indra/652185177_0.html

[128] 'Información corporativa', *Isdefe*, undated, https://www.isdefe.es/informaci-n-corporativa?language=es

[129] 'Shareholders base', *Leonardo*, undated, https://www.leonardo.com/en/investors/stock-info/shareholders-base

[130] 'Israel Aerospace Industries company profile', *Corporate Watch*, 12 December 2014, https://corporatewatch.org/israel-aerospace-industries-company-profile/

Institution	Country	FP7 projects	H2020 projects	Total funding
			PROMENADE	
ITTI	Poland	FASTPASS MOBILEPASS TALOS	FOLDOUT iBorderCtrl PROTECT	€ 2,459,745
Atos	Spain	ABC4EU	BODEGA	€ 2,367,744
CS Group	France		RANGER	€ 1,973,209
Hipersfera Doo Za Razvoj i Primenjenu Tehnologija	Croatia		BorderUAS	€ 1,727,564
BMT Group	UK	SUNNY		€ 1,646,142
TTI Norte	Spain	SEABILLA SUNNY TALOS		€ 1,563,746
Marine & Remote Sensing Solutions Limited	UK	SECTRONIC		€ 1,499,529
GMV Aerospace and Defence	Spain		ANDROMEDA MARISA PROMENADE	€ 1,435,446
Exus Software	UK		ANDROMEDA RANGER	€ 1,262,188
Exodus Anonymos Etaireia Pliroforikis	Greece		CAMELOT FLYSEC	€ 1,260,496

Academic institutions

While the border security industry, governments and state agencies are frequent targets of migrant and refugee rights activists, the prominent role of research and higher education institutions in the EU's border complex arguably merits closer attention. Over €54 million has been awarded to universities for their role in border AI projects over the last 15 years, with 16 institutions receiving over €1 million each for their work.

The issue of academic complicity in the EU's border regime was brought to a wider public late last year when an academic at Turin Polytechnic University, Michele Lancione, denounced a company owned by the university for planning to assist EU border agency Frontex in the production of maps for its "risk analysis" work.[131] Although students, staff and supporters of Lancione's stance did not succeed in having the contract withdrawn, Lancione was undeterred: "I am more and more convinced that continuing to fight Frontex at all levels is very necessary. It is not time to retreat, but time to scale up," he said.[132] As border control methods become increasingly reliant on advanced technologies, the involvement of educational institutions is likely to become further entrenched.

Top 20 higher education recipients of EU security research funding for border AI projects

Institution	Country	FP7 projects	H2020 projects	Total funding (FP7 and H2020)
University of Reading	UK	EFFISEC FASTPASS	D4FLY FOLDOUT PROTECT	€3,707,124.25
Laurea University of Applied Sciences	FI	AB4EU EU CISE 2020 PERSEUS	AI-ARC ANDROMEDA MARISA RANGER	€3,493,531.50
Gottfriend Wilhelm Leibniz University Hanover	DE	SMART	CRITERIA iBorderCtrl MIRROR SMART	€2,222,287.25
Alma Mater Studiorum – University of Bologna	IT	FIDELITY INGRESS	iMARS MARISA PERCEPTIONS	€2,138,612.79
University of Antwerp	BE		BorderSens PERCEPTIONS	€2,004,107.50
Catholic University of Leuven	BE	BEAT FASTPASS FIDELITY	iMARS	€1,910,866.61
Gjøvik University College	NO	FIDELITY INGRESS		€1,752,084.00
Norwegian University of Science and Technology	NO	INGRESS	D4FLY iMARS SMILE	€1,731,571.94

[131] '"Not alongside Frontex": academics speak out against border collaboration', *Statewatch*, November 2021, https://www.statewatch.org/news/2021/november/not-alongside-frontex-academics-speak-out-against-border-collaboration/

[132] 'Resisting co-optation by Frontex: Italian academia and a Swiss referendum', *Statewatch*, January 2022, https://www.statewatch.org/news/2022/january/resisting-co-optation-by-frontex-italian-academia-and-a-swiss-referendum/

Institution	Country	FP7 projects	H2020 projects	Total funding (FP7 and H2020)
Autonomous University of Barcelona	ES		BorderSens ITFLOWS	€1,373,567.00
Munster Technological University	IE		AI-ARC CAMELOT ITFLOWS	€1,324,037.50
University of Malta	MT	SMART WIMAAS	CRITERIA MIRROR	€1,289,730.40
University of Groningen	NL	INGRESS SMART	CRITERIA MIRROR	€1,288,185.00
National Inter-University Consortium for Telecommunications	IT	SEABILLA SUNNY	ROBORDER	€1,218,533.30
Darmstadt University of Applied Sciences	DE	FIDELITY	iMARS	€1,202,574.14
Queen Mary University of London	UK	SUNNY	SafeShore	€1,067,763.86
University of Tartu	EE		SilentBorder	€1,010,125.00
National and Kapodistrian University of Athens	EL		ARESIBO ROBORDER	€918,125.00
King Juan Carlos University	ES	ABC4EU	PERCEPTIONS	€845,585.38
Dresden Technical University	DE		RANGER	€823,125.00
Sheffield Hallam University	UK		PERCEPTIONS ROBORDER	€810,312.50
Technical University of Crete	EL	SUNNY	BorderUAS	€777,305.89
Polytechnic University of Valencia	ES		CAMELOT	€755,312.50
University of Vienna	AT	SMART	MIRROR	€749,443.50

Research institutes

Publicly-funded research institutes, many of them intimately-connected to the state – if not effectively part of the state itself – are key actors in the EU's border AI complex. A Greek organization – KEMEA, the Center for Security Studies – is the single largest recipient of funding from the EU's security research programmes for border AI. The institution – which describes itself as "the think-tank of the Ministry of Citizen Protection" as well as "a scientific, consulting and research organization" overseen by that same ministry – has participated in 14 border AI projects since 2007, receiving almost €11.4 million for its work. Other state or state-connected research institutes feature prominently in the top ten recipients of border AI research funding: Isdefe (Spain), the Fraunhofer Institute (Germany), the Austrian Institute of Technology, National Center for Scientific Research 'Demokritos' (Greece) and Teknologian tutkimuskeskus VTT Oy (Finland).

Top 20 research institute recipients of EU security research funding for border AI projects

Institution	Country	FP7 projects	H2020 projects	Total funding
Kentro Meleton Asfaleias (KEMEA)	Greece	EWISA PERSEUS SNOOPY SUNNY	ANDROMEDA BODEGA BorderUAS CAMELOT EFFECTOR FOLDOUT iBorderCtrl iMARS PERCEPTIONS PROMENADE	€11,370,782
Fraunhofer Institute	Germany	AMASS ARGUS 3D FASTPASS FIDELITY MOBILEPASS WIMAAS	AI-ARC ARESIBO D4FLY E2mC MARISA ROBORDER SMILE	€ 6,757,620
Teknologian Tutkimuskeskus	Finland	EFFISEC FASTPASS TALOS	ARESIBO BODEGA D4FLY FOLDOUT ROBORDER	€ 6,107,623
Austrian Institute of Technology	Austria	FASTPASS MOBILEPASS	BODEGA FOLDOUT	€ 6,082,883
National Center for Scientific Research "Demokritos"	Greece	EU CISE 2020 PERSEUS SUNNY	D4FLY FLYSEC	€ 4,312,780
Totalforsvarets Forskningsinstitut (Defence Research Institute)	Sweden	EFFISEC FIDELITY SEABILLA WIMAAS	MIRROR	€ 3,471,553
Office National d'Etudes et de Recherces Aerospatiales	France	I2C OPARUS TALOS	FOLDOUT	€ 3,233,002

Institution	Country	FP7 projects	H2020 projects	Total funding
Ethniko Kentro Erevnas Kai Technologikis Anaptyxis	Greece		ARESIBO CRiTERIA ITFLOWS MIRROR ROBORDER SMILE	€ 3,179,545
Siec Badawcza Lukasiewicz – Prezemyslowy Instyut Automatyki I Pomiarow (PIAP)	Poland	TALOS	CAMELOT	€ 3,093,908
TNO (Nederlanse Organisatie Voor Toegepast Natuurwetenschapp Elijk Onderzoek)	Netherlands	SEABILLA	COMPASS2020 D4FLY MARISA	€ 2,284,439
Institute of Communication and Computer System	Greece		ANDROMEDA EFFECTOR iBorderCtrl RANGER	€ 2,174,979
EU Joint Research Centre	Belgium	EFFISEC FASTPASS I2C SEABILLA WIMAAS		€1,399,896
Fondation de l'Institut de Recherche (IDIAP)	Switzerland	BEAT	CRITERIA	€ 1,362,562
Institut Po Otbrana	Bulgaria		ARESIBO CAMELOT FOLDOUT ROBORDER	€ 951,596
Inesc Tec	Portugal	SUNNY		€ 926,229
Centre Suisse d'Electronique et de Microtechnique SA – Recherche et Developpement (CSEM)	Switzerland	INGRESS	ROBORDER	€ 923,668
Commissariat a l'Energie Atomique et aux Energies Alternatives	France	BEAT	BODEGA	€ 908,575
Deutsches Zentrum für Luft –und Raumfahrt	Germany	OPARUS	SilentBorder	€ 907,226
Fundación Centro de Tecnologias de Interacción Visual y Comunicaciones (Vicomtech)	Spain		BorderUAS	€ 757,708
RISE Research Institutes of Sweden			AI-ARC	€ 749,375

Public institutions

Public institutions – ministries, police forces and border agencies – are also prominent participants in the EU's border AI research projects. As noted above, the presence of numerous institutions Mediterranean states with external borders is noteworthy – as is the presence of three defence ministries, from Italy, Greece and Portugal. The fact that defence ministries have participated in multiple border AI projects gives a clear indication of both the type of technology that is being developed, and provides backing for longstanding critiques regarding the militarization of Europe's borders.

Top 20 public institution recipients of EU security research funding for border AI projects

Institution	Country	FP7 projects	H2020 projects	Total funding
MINISTERO DELLA DIFESA	Italy	CLOSEYE EU CISE 2020	ANDROMEDA MARISA	€4,817,831
MINISTERIO DEL INTERIOR	Spain	ABC4EU CLOSEYE EU CISE 2020 EWISA MOBILEPASS	MARISA PROMENADE	€4,589,830
MINISTRY OF NATIONAL DEFENCE, GREECE	Greece	EU CISE 2020 PERSEUS	ANDROMEDA ARESIBO CAMELOT EFFECTOR MARISA RANGER ROBORDER	€3,062,159
MINISTRY OF THE INTERIOR	Finland	EU CISE 2020 EWISA FASTPASS		€2,151,706
MINISTERIO DA DEFESA NACIONAL	Portugal	SUNNY	ANDROMEDA ARESIBO CAMELOT EFFECTOR MARISA	€1,801,547
MINISTERIO DA ADMINISTRACAO INTERNA	Portugal	ABC4EU CLOSEYE PERSEUS	CAMELOT ROBORDER	€1,348,865
INSPECTORATUL GENERAL AL POLITIEI DE FRONTIERA	Romania	ABC4EU EU CISE 2020 EWISA FASTPASS MOBILEPASS	BorderSens BorderUAS CAMELOT CRITERIA iMARS ROBORDER SafeShore SMILE	€1,309,790
MINISTRY OF MARITIME AFFAIRS AND INSULAR POLICY	Greece	EU CISE 2020	ANDROMEDA EFFECTOR PROMENADE	€1,005,274
GUARDIA CIVIL ESPANOLA	Spain	PERSEUS		€915,825

Institution	Country	FP7 projects	H2020 projects	Total funding
EUROPEAN UNION SATELLITE CENTRE	Spain	CLOSEYE EU CISE 2020	AI-ARC PROMENADE	€792,030
RAJAVARTIOLAITOS	Finland		ARESIBO BODEGA FOLDOUT	€741,003
DIRECAO-GERAL DE POLITICA DO MAR	Portugal	EU CISE 2020		€653,040
Força Aérea Portuguesa	Portugal	PERSEUS		€627,400
DE FEDERALE OVERHEIDSDIENST JUSTITIE - LE SERVICE PUBLIC FEDERAL JUSTICE	Belgium		BorderSens	€612,500
DIRECCAO GERAL DA AUTORIDADE MARITIMA	Portugal		COMPASS2020	€606,750
ORSZAGOS RENDOR - FOKAPITANYSAG	Hungary		iBorderCtrl ROBORDER SMILE	€547,500
BUNDESKRIMINALAMT	Germany	FIDELITY	iMARS	€544,018
SERVICIUL DE PROTECTIE SI PAZA	Romania		ARESIBO ROBORDER SafeShore SMILE	€541,500
Secrétariat général de la mer	France	EU CISE 2020	EFFECTOR	€520,295
HOME OFFICE	UK		BorderSens COMPASS2020 D4FLY PROTECT	€465,261

Policy discussions

The Commission's proposal for an AI Act was published in April 2021. At the time of writing, both the Council and the Parliament are yet to reach their respective positions on the text. After they do so, they will enter secret "trilogues" negotiations, in which the Commission also participates. The text that emerges will then go back to the Council and Parliament for plenary votes. The Parliament expects to adopt its position in November, after which lengthy negotiations with the Council will begin - Dragoș Tudorache, one of the two MEPs responsible for the file, expects that could take up to 18 months.[133]

Within the Parliament, there was a struggle over which committee – and which MEP – should get the lead role for determining the Parliament's position and taking part in negotiations with the Council. In December 2021, the Conference of Committee Chairs agreed that Brando Benifei (Socialists & Democrats, S&D) would take on the role of *rapporteur* in the Committee for Internal Market and Consumer Protection (IMCO), while Dragoș Tudorache (Renew, liberals) would act as *rapporteur* in the Committee on Civil Liberties, Justice and Home Affairs (LIBE).

IMCO and LIBE will act as joint lead committees for the file, with a host of other committees also involved. Of those, JURI (Legal Affairs) will have exclusive competence over articles on transparency and information to users, human oversight, transparency obligations for certain systems, and codes of conduct. [134] ITRE (Industry, Research and Energy) will have exclusive competence over articles dealing with accuracy, robustness, cybersecurity and measures for small-scale providers and users.[135]

One of the most likely contentious points in the proposal is the question of whether or not to ban the use of remote biometric identification systems, such as facial recognition, in public spaces. It is precisely because of this topic that Tudorache thinks negotiations will drag on so long. Benifei supports such a ban, a stance that is in line with the majority of other MEPs – a July 2021 resolution called for "a ban on any processing of biometric data, including facial images, for law enforcement purposes that leads to mass surveillance in publicly accessible spaces."[136] Tudorache, however, is against absolute bans.[137]

A European Parliament resolution on artificial intelligence in criminal law approved in July 2021 considers that any use of AI where there is "potential to significantly affect the lives of individuals" must be automatically categorised as high risk, especially given the fast pace at which technology and its application develops, and calls for strict necessity and proportionality testing.[138] The report expresses particular concern over the potential for repurposing technologies, calling for strict democratic control and independent oversight of any AI-enabled technology used by law enforcement or judicial authorities, and demanding a ban if they have capacity for mass surveillance or profiling, as these can never fulfil necessity and proportionality requirements.

The issue of assigning legal responsibility and liability for potential harm caused through the development or deployment of artificial

[133] Foo Yun Chee, 'Europe's bid for AI standard faces long road, EU lawmakers say', *Reuters*, 16 February 2022, https://www.reuters.com/world/europe/europes-bid-ai-standard-faces-long-road-eu-lawmakers-say-2022-02-16/

[134] Articles 13, 14, 52 and 69

[135] Articles 15 and 55

[136] 'Resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters', *European Parliament*, 13 July 2021, https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

[137] Melissa Heikkilä, 'AI: Decoded: Meet Parliament's second AI man — France on the AI Act — Uncovering hidden physical laws', *Politico Europe*, 19 January 2022, https://www.politico.eu/newsletter/ai-decoded/meet-parliaments-second-ai-man-france-on-the-ai-act-uncovering-hidden-physical-laws-2/

[138] 'Resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters', *European Parliament*, 13 July 2021, https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

intelligence is also considered. The report says a "clear and fair regime for assigning legal responsibility and liability for the potential adverse consequences produced by these advanced digital technologies" must be created, residing with a natural or legal person, which in itself required transparency of corporate structures producing and managing AI systems. While the AI Act includes exceptions to obligations in cases of law enforcement, LIBE considers that a compulsory fundamental rights impact assessment must be conducted prior to the use of any AI system for law enforcement purposes, given the high risk associated. The likelihood of discriminatory outcomes of classifications, assessments and predictions based on algorithmic systems and datasets is emphasised throughout the report. Given the risks for fundamental rights, these recommendations should also be taken to apply in the contexts of migration, asylum and border control.

The Parliament's Special Committee on Artificial Intelligence in a Digital Age (AIDA) produced a report in March 2022 that emphasised the risks to democracy posed by the power wielded by large technology corporations, and the threats to fundamental rights, in particular the right to privacy.[139] Rather than regulating AI as technology, however, AIDA concludes that regulatory intervention should be "proportionate to the type of risk associated with using an AI system in a particular way," especially considering risks of mass surveillance "and other unlawful interference" and concerns about military research. The final text – which has no binding force – was something of a political compromise by members of the committee, with the spokespersons Axel Voss and Dragoş Tudorache emphasising innovation and competition, and rules and values, respectively.

Within the Council of the EU, the Working Party on Telecommunications and Information Society (TELECOM WP) has responsibility for dealing with the proposal. However, the standing committee on internal security (COSI) has also shown significant interest in the text. Indeed, in September 2021 the Slovenian Presidency of the Council organised a day-long workshop that aimed to "address the remaining concerns raised by the law enforcement and internal security communities of the Member States".

It was at this workshop that, as noted above, the Commission said that the AI Act will make "virtually no impact" on users of AI for law enforcement or security purposes. Nevertheless, despite attempts by the Commission to reassure national officials, "several Member State representatives expressed their concerns and found the proposal restrictive and not in line with the practical needs of law enforcement."[140] Elsewhere, the Commission has gone even further, claiming that one objective of the proposal in relation to home affairs is "to decrease administrative burden on home affairs authorities in order not to hamper innovation and in-house developments,"[141] and a further aim is to "ensure that the implementation of the EU large-scale IT systems for migration, border management and security are not delayed".[142] It is nevertheless evident that there is significant disquiet amongst the home affairs and internal security "community" about the proposal.

However, that same community has also enjoyed a rather privileged position in the decision-making process, as well as broader initiatives on the use of AI in home affairs. In July

[139] 'Artificial intelligence: the EU needs to act as a global standard-setter"', *European Parliament*, 22 March 2022, https://www.europarl.europa.eu/news/en/press-room/20220318IPR25801/artificial-intelligence-the-eu-needs-to-act-as-a-global-standard-setter

[140] 'Report on the JHA/law enforcement online workshop on the proposed AI Act (AIA)', available in 'EU: Artificial Intelligence Act: justice sector and high-risk systems; internal security; migration and borders; comments and presentations', *Statewatch*, 26 January 2022, https://www.statewatch.org/news/2022/january/eu-artificial-intelligence-act-justice-sector-and-high-risk-systems-internal-security-migration-and-borders-comments-and-presentations/

[141] 'European Commission: Artificial Intelligence Act aims "to decrease administrative burden on home affairs authorities in order not to hamper innovation"', *Statewatch*, 28 September 2021, https://www.statewatch.org/news/2021/september/european-commission-artificial-intelligence-act-aims-to-decrease-administrative-burden-on-home-affairs-authorities-in-order-not-to-hamper-innovation/

[142] European Commission, 'Shaping Europe's Digital Future', Ares(2021)5674926, 16 September 2021, https://www.statewatch.org/media/2795/eu-com-ai-expert-group-general-presentation.pdf

2020 the Commission convened the first meeting of the Expert Group on Artificial Intelligence in the domain of Home Affairs, which was established to assist the Commission prepare "legislative proposals/policy initiatives concerning Artificial Intelligence in the domain of Home Affairs," and to boost cooperation and exchanges between the Commission, EU member states and "stakeholders". Its membership is primarily made up of representatives of police forces, immigration services and interior ministries.

As well as discussing the AI Act, the group has examined numerous other issues, including:

- the RAND Europe study on artificial intelligence opportunities for Frontex and national EU border agencies;
- a study on a "forecasting and early warning tool for migration based on artificial intelligence technology";
- the use of AI for advanced surveillance and behavioural analysis technologies;
- detecting and classifying online hate crime; and
- crime forecasting.

A consistent topic throughout the group's meetings has been that of a "security data space for innovation". The creation of "data spaces" is a political priority of the highest order, called for by the European Council in March 2021; such spaces would involve "a common data platform, including the national components and a communication infrastructure, with trusted datasets to train, test and validate algorithms aims to create sufficient quantity of data to research, innovate and develop AI technologies."

The "security" aspect of the project involves creating "a data ecosystem specific for the needs of the security and immigration stakeholders," which would include private companies if they are participating in EU-funded research projects. The call notes that: "Particular attention must be given to reducing potential bias in algorithms to be used by law enforcement." The Commission is offering up to €8 million for the first steps towards creating this data space,[143] along with a further €500,000 to create initial datasets.[144]

It is evident that there a vast number of ongoing AI initiatives that seek to boost the powers of border, policing and security agencies – who also have a vested interest in ensuring that the AI Act has as little effect as possible on their development and deployment of new technologies. It is therefore vital for reinforced efforts to ensure that the AI Act upholds the values of a just and democratic society, and does not advance the interests of the state's repressive agencies to the detriment of broader social interests

[143] 'Data space for security and law enforcement', https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cloud-ai-02-sec-law;

[144] 'Call for proposals on data sets for the European Data Space for innovation', 20 January 2022, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-tf1-ag-data_en.pdf

Institutions involved in negotiations on the AI Act and other AI policy discussions

Institution	Committee/Working Party/Unit	Role
European Parliament	Internal Market and Consumer Protection (IMCO)	Lead committee (joint)
	Civil Liberties, Justice and Home Affairs (LIBE)	Lead committee (joint)
	Environment, Public Health and Food Safety (ENVI)	Committee for opinion
	Industry, Research and Energy (ITRE)	Committee for opinion
	Transport and Tourism (TRAN)	Committee for opinion
	Culture and Education (CULT)	Committee for opinion
	Legal Affairs (JURI)	Committee for opinion
Council of the EU	Working Party on Telecommunications and Information Society (TELECOM WP)	Lead working party
	Standing Committee on Operational Cooperation on Internal Security (COSI)	Has maintained an interest in the internal security and home affairs aspects of the AI Act.
European Commission	Directorate-General for Communications Networks Content and Technology (DG CNECT)	Lead DG for preparing the proposal.
	Commission Expert Group on Artificial Intelligence in the domain of Home Affairs[145]	"To assist DG HOME in the preparation of legislative proposals/policy initiatives concerning Artificial Intelligence in the domain of Home Affairs; to establish Cooperation/coordination between the Commission and Member States or stakeholders on questions relating to the implementation of Union legislation, programmes and policies in the field of Artificial Intelligence in the domain of Home Affairs; and to bring about an exchange of experience and good practice in the field of Artificial Intelligence in the domain of Home Affairs."
	Commission Expert Group on Artificial Intelligence (AI) and Data in Education and Training[146]	"- Assist the Commission in relation to the implementation of existing Union legislation, programmes and policies - Coordinate with Member States, exchange of views"
	Expert group on Artificial Intelligence and Digitalisation of Businesses[147]	"- Assist the Commission in relation to the implementation of existing Union legislation, programmes and policies - Coordinate with Member States, exchange of views"

[145] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3727
[146] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3774
[147] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3795

Members of the European Commission Expert Group on AI in the Domain of Home Affairs

State	Authority/Authorities
EU member states	
Austria	EKO COBRA / Direktion für Spezialeinheiten
Belgium	Coordination of Strategic Analysis - Directie politionele informatie & ICT, Federale politie
Bulgaria	Communication & Information Systems Development and Projects Department, Communication and Information Systems Directorate, Ministry of Interior
Croatia	Department for IT, Ministry of Interior
	Organized Crime Unit, General Police Directorate, Ministry of Interior
Cyprus	Police CY
Czech Republic	Police Presidium of the Czech Republic, Department of Informatics and Operation of Information Technologies, Directorate for Service Support
Denmark	Danish National Police - Police Directorate - National Aliens Centre
Estonia	Justice and Home Affairs Counsellor - Permanent Representation of Estonia
	Strategy and Development Department, Ministry of the Interior
Finland	Police Department of the Minister of Interior
France	Permanent Representation of France to the EU, Ministry of Interior Sous-Direction de l'Innovation à la Organisation de la direction du numérique (DNUM) COL ST DGGN - coordination of AI for the whole French national Gendarmerie
Germany	Central Office for Information Technology in the Security Sector Permanent Representation of the Federal Republic of Germany to the EU “Projektgruppe Polizei 2020” of the German Federal Ministry of the Interior, Building and Community
Greece	Police of Greece
Hungary	Ministry of Interior Deputy State Secretariat for Informatics
Ireland	Cyber Security Policy, Criminal Justice, Department of Justice Department of Justice & Equality
Italy	Italian Ministry of Interior - Public Security Department/ Police Forces Coordination and Planning Office /International Relations Service – EU Affairs Division Italian Postal and Communications Police Italian Ministry of Interior – Italian State Police
Latvia	Integrated Systems Division of the Information Centre of the Ministry of the Interior Information Office of the Central Criminal Police Department of the State Police Support Unit of the Criminal Investigation Board of the State Border Guard
Lithuania	Criminal Police Bureau State Border Guard Service Activity analysis and control board of Police department under the Minister of Interior Ministry of Foreign Affairs of the Republic of Lithuania
Luxembourg	Ministère de la Sécurité intérieure Police Luxembourg
Malta	Permanent Representation of Malta to the EU Malta Police Force
Netherlands	Ministry of Justice and Security/Department for Police and Security Netherlands Police

State	Authority/Authorities
Poland	Ministry of Internal Affairs and Administration Polish Border Guard Headquarters Office for Foreigners IT and Communication Bureau, National Police Headquarters Chancellery of the Prime Minister Police Headquarters
Portugal	The Portuguese Immigration and Borders Service (SEF) National Republican Guard (Guarda Nacional Republicana - GNR)
Romania	National Romanian Police - Central Intelligence Analysis Unit
Slovakia	Ministry of Interior - Acquisitions and Innovation Department, Police Presidium
Slovenia	Ministry of Interior - General Police Directorate Slovenian Police JHA Council RP
Spain	Ministry of Interior Permanent Representation of Spain to the EU
Sweden	Division for Police issues - Ministry of Justice Swedish National Forensic Centre – Swedish Police Authority
Schengen Associated Countries	
Liechtenstein	EU/EEA at the Office of Information technology Amt für Informatik Liechtensteinische Landesverwaltung Police Service
Norway	Legislation Department, Ministry of Justice and Public Security Norwegian Business School
Switzerland	Federal Police EDA Département fédéral des finances DFF Administration fédérale des douanes AFD Centre de situation et d'information CSI

statewatch.org