

AUTOMATING AUTHORITY

ARTIFICIAL INTELLIGENCE IN EUROPEAN POLICE
AND BORDER REGIMES

APRIL 2025

STATEWATCH

WRITTEN BY:
Chris Jones
Romain Lanneau

SUPPORTED BY:
European
Artificial Intelligence
& Society Fund

Publication information

About this report

Authors: Chris Jones, Romain Lanneau

Research support: Samaya Anjum, Eloisa Griffiths

Thanks to: Nidžara Ahmetašević, Hope Chilokoa-Mullen, Sara Chitseko, Riccardo Coluccini, Caterina Rodelli, Niovi Vavoula

This report was supported by the European AI & Society Foundation.

Published by Statewatch, April 2025

About Statewatch

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.

statewatch.org

(+44) (0) 203 393 8366

**MayDay Rooms, 88 Fleet Street,
London EC4Y 1DH, UK**

Support our work

Support our work to expose state power and inform dissent by making a donation. And join our mailing list to stay informed and help spread our work.



Scan the QR code above or visit:

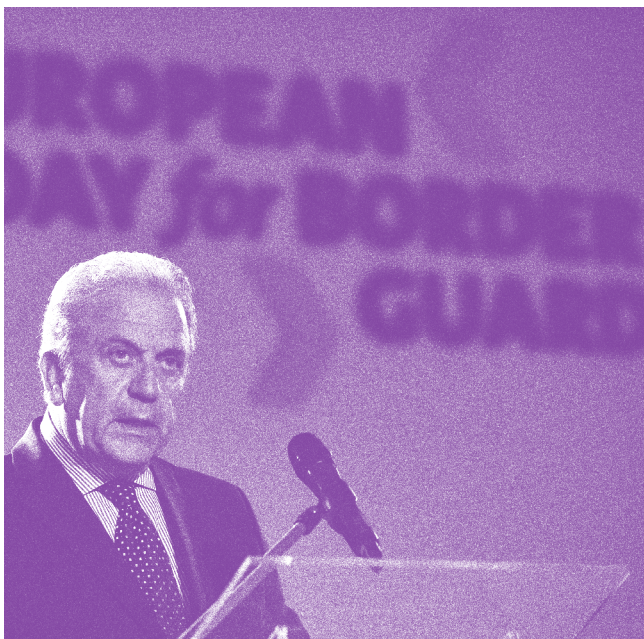
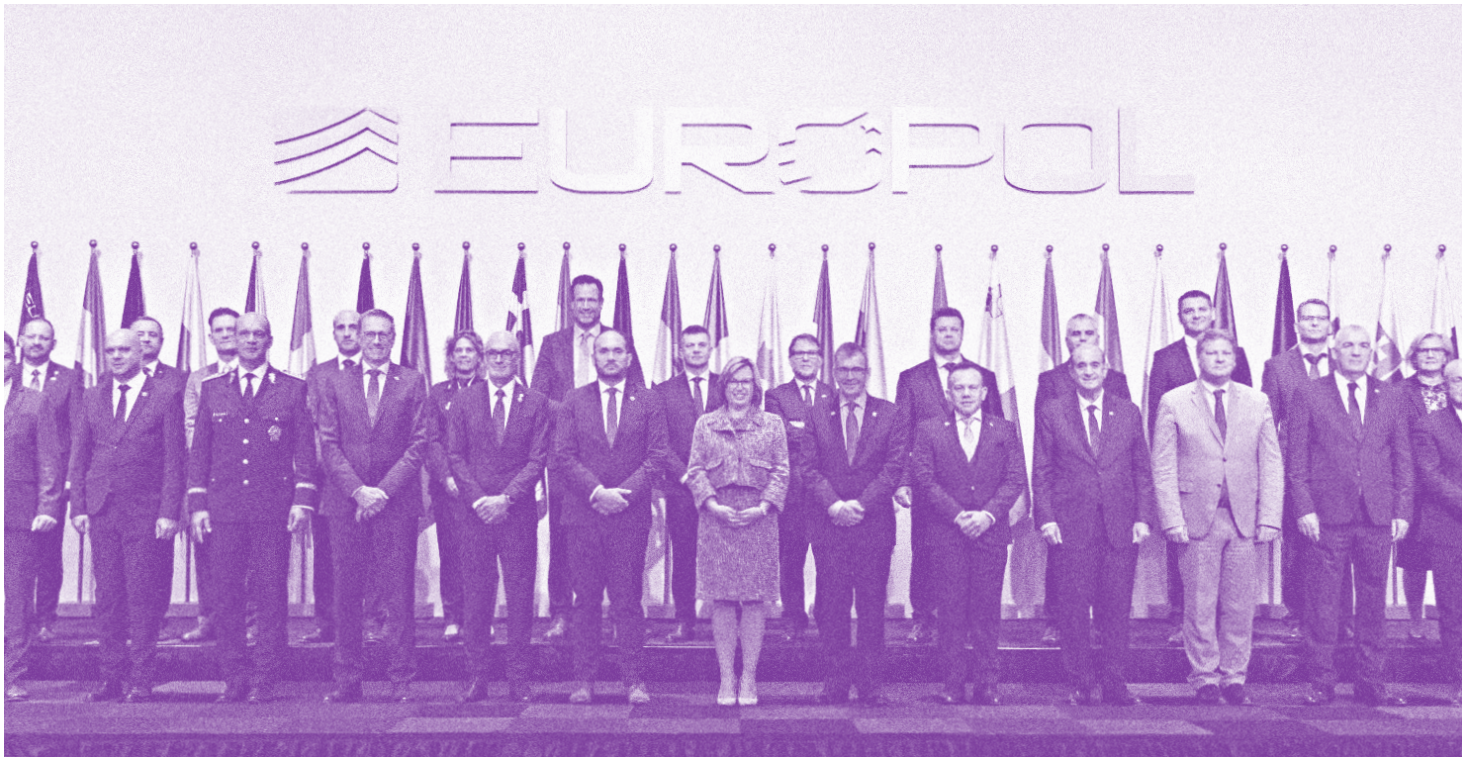
- [Donation page](#)
- [Mailing list sign-up](#)

Registered UK charity number:
1154784

Registered UK company number:
08480724

Registered company name: The Libertarian Research & Education Trust

Registered office: 88 Fleet Street,
London EC4Y 1DH, UK.



Intro

Artificial intelligence (AI) technologies are being embedded into everyday life by powerful actors, primarily motivated by profit. Police, border and criminal justice agencies are also looking to take advantage of the new powers AI offers for “security” policies, at both national and EU level. The EU is creating new infrastructure, away from the public eye, to allow the swift development and deployment of “security AI.” This will also reinforce the existing discrimination, violence and harm caused by policing, border and criminal justice policies. **Exposing and understanding this emerging security AI complex is the first step to challenging it.**



***Today's plan mainlines
AI into the veins of this
enterprising nation...***

UK Government



Mainlining AI

Artificial intelligence (AI) is big business. Since the release of the generative AI chatbot, ChatGPT, in November 2022, the hype and hubbub surrounding AI technologies has reached fever pitch, and it seems unlikely to die down anytime soon.

Businesses are adopting AI to automate all manner of tasks. They are inserting the technology into everyday tools such as web searches, whether people like it or not. Governments hail AI's supposed ability to improve public services, working conditions and education, amongst other things.

The UK government has promised – or, perhaps, threatened – to “mainline AI into the veins” of the country.¹

This phrase, perhaps unwittingly, represents the overall strategy of the companies behind the technology: insert AI into as much public and private infrastructure as possible, and thus guarantee an ongoing flow of profit.



Supranational AI

The repressive agencies of the state also form part of this picture. Police and border forces across Europe and beyond are already investigating or using various forms of AI.

The German authorities are interested in “biometrics and face recognition.” The Czech Republic is aiming for “prediction of crime.” Norway hopes to enable “fraud detection in the immigration directorate.” Its neighbour, Sweden, has tested “facial recognition... at some borders.”²

These trends are reflected in EU institutions and agencies, which have long seen new technologies as “solutions” to a wide range of social issues.

As *Statewatch* has previously analysed, the bloc’s immigration, border control and policing systems are being extensively digitalised.³ Introducing “artificial intelligence” is the next step in this process.

Europol, the EU’s policing agency, stores vast amounts of data sourced from police forces, private companies, or retrieved from the web. It is adopting advanced technologies to process and analyse that data. These include machine learning ([section 3.2.2](#)) and upgraded facial recognition systems ([section 3.2.3](#)).

The border agency, Frontex, is deploying new surveillance technologies at the EU’s borders and beyond, and developing new systems for the collection, consolidation and analysis of data ([section 3.3.1](#)).

Like Europol, it now also has a role in determining the EU's priorities for its technological research and development programme, Horizon Europe. This means the agencies can influence the development of new technologies.

The EU agency for managing policing and migration databases, eu-LISA, is building tools to algorithmically profile and assess travellers ([section 3.1.1](#)). The EU Asylum Agency is developing a tool to help identify the nationality of asylum seekers based on the way they speak ([section 3.4.1](#)). Eurojust, the judicial cooperation agency, is also slowly incorporating AI tools into its systems and processes ([section 3.5](#)).

This is just the start. Many other potential uses of AI have been identified in lengthy studies carried out for EU institutions (see Annex III). Some of the potential uses would be incredibly invasive. They include:

- the police using AI to detect “irregular travelling patterns,” through analysis of plane and other traffic;
- using AI to monitor “the level of success in integration” achieved by individual migrants, and for migrant groups as a whole; and
- using AI for “assigning individuals seeking asylum to detention centres.”

To the best of our knowledge, AI is not currently being used for these purposes. It will take concerted political and legal challenges and change for things to stay that way.

***This is just
the start.***



FILM THE POLICE

NO RACIAL PROFILING



Security AI: exclusion and discrimination

These uses of AI – for policing, border, immigration, asylum and criminal justice purposes – are referred to in this report as “security AI.” Like other forms of AI technology, security AI systems receive certain data as inputs, and use it to produce various different “outputs.” These include predictions, profiles, risk assessment and suggestions.

These outputs can, in turn, be used to influence all manner of decisions:

on criminal investigations and border interrogations, covert surveillance operations, visa decisions, and many more. This raises multiple questions for protecting the rights to liberty, security, non-discrimination, assembly, freedom of movement and effective remedies, amongst others.

However, the effects of these systems will not be evenly felt: marginalised and racialised people will bear the brunt of them.

The EU's plans will mean millions of people travelling to the EU 'legally' are profiled by algorithms.

Refugees, forced to travel 'illegally', already have to take dangerous and deadly journey to seek safety, due to border control and surveillance measures. Enhancing and increasing that surveillance with AI will only compound those risks.

Police forces and the criminal justice system are beset by racism and other forms of discrimination.⁴ “Racist comments, more frequent stops and even violence - this is how people of different ethnic backgrounds experience policing in Europe,” says the EU’s Fundamental Rights Agency.⁵ A 2018 study of the criminal

justice system in 12 EU member states found that “disparities exist for people of various ethnic, racial, and national origins, at least at some stages of their criminal justice systems and in some form.”⁶

Reinforcing these systems with AI technologies may provide a veneer of technical objectivity and fairness. This is why there is such concern amongst officials about “debiasing” AI systems. **However, this approach does nothing to address the structural dynamics of exclusion, subjugation and discrimination that shape the role and actions of police, immigration and other state agencies.**



“

Racist comments, more frequent stops and even violence—this is how people of different ethnic backgrounds experience policing in Europe

EU Fundamental Rights Agency



Security AI complex

Discussing these issues is difficult for many reasons. One of those is secrecy: **the development of security AI remains largely hidden from public view and excluded from political debate.** This report seeks to alter that situation, to encourage democratic discussion, and to support work towards accountability.


There are no smoking guns or big “reveals.” This is not that kind of story. Rather, it is the tale of an ongoing attempt by politicians and officials to develop new institutional, technical and legal infrastructure for the swift development, testing and use of security AI.

Over the past five years, these efforts have varied in their scale and ambition. Some appear to be slowly embedding themselves in the EU’s institutional landscape, such as the Innovation Hub for Internal Security ([section 4.1.2](#)). Others, like the plan to create a “centre of excellence” for AI at eu-LISA, the policing and

migration database agency ([section 4.1.1](#)), have fizzled out – though of course, they may be revived.

Nevertheless, all these initiatives show an intended direction of travel, and it is one that merits far greater scrutiny than it has so far received. By exposing and analysing this emerging “EU security AI complex”, we aim to inform meaningful public and political debate and decision-making.

The development of supranational security policies and powers should not be left in the hands of agencies and institutions that remain invisible or unaccountable to the public or their elected representatives. This is particularly important in light of the path dependencies created by these policies and powers. Their existence makes certain future policy choices more likely than others, precluding possible alternatives.



***There are no smoking guns or big “reveals.”
This is not that kind of story.***



EMERGENCY
USE ONLY

The AI Act: exceptions, exemptions and loopholes

The first substantive section of the report analyses the AI Act. The Act provides the legal framework that will govern the use of AI – including security AI – in the EU for the years to come ([section 2](#)).

The Act achieves two key things. First, it establishes conditions for increased development and use of AI systems. Second, it ensures that security AI systems are subject to extremely limited accountability, oversight and transparency measures.

The Act includes:

- the possibility to use mass biometric surveillance, AI-powered risk assessments and emotion recognition systems for immigration, asylum and border control purposes;
- a total exemption from the law until 2030 for large-scale EU databases and information systems;
- a self-assessment process that allows providers of high-risk AI systems to exclude their systems from the safeguards the Act imposes on high-risk systems;
- widespread secrecy over the testing and use of security AI; and
- the exclusion of people outside of the EU from the Act's protections, despite a number of the EU's own AI systems explicitly targeting such people.

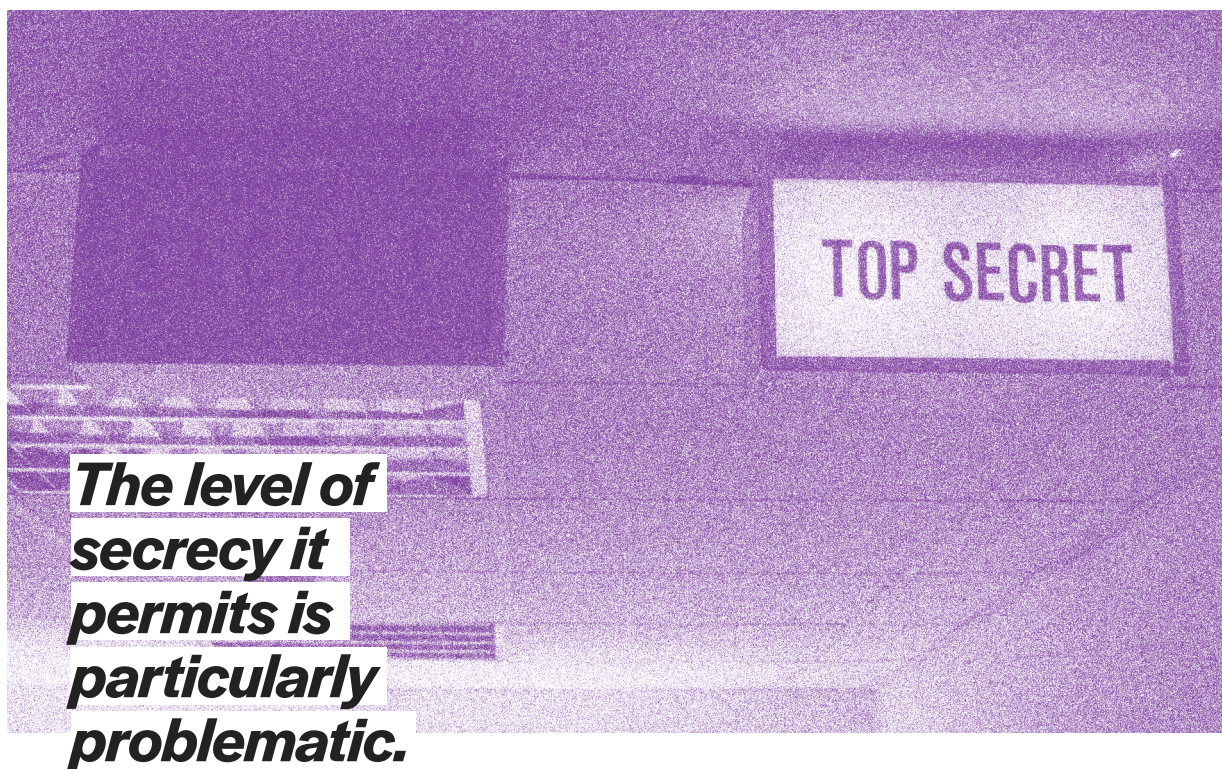
The report examines provides a summary of each exemption ([section 2.2](#)), and then examines them in detail ([section 2.3](#)).

The law presents formidable challenges to understanding, scrutiny and accountability of security AI. The level of secrecy it permits is particularly problematic: turning the techniques used to detect and investigate crime, or to control migration, into state secrets simply increases impunity.

Legal experts have already taken a dim view of many of these exemptions and exceptions. The Act itself says it is “without prejudice” to a host of EU and national legal requirements. However, on the face

of it, it clashes in a number of ways with the EU Charter of Fundamental Rights, jurisprudence from the Court of Justice of the EU, and existing laws.

These clashes cover topics ranging from the scope of a “national security” exemption, to the right for people to receive explanations about AI-informed decisions, and the powers of independent supervisory authorities. There will likely be a substantial amount of litigation in the years to come as authorities, companies and individuals seek to have aspects of the law clarified, and potentially strengthened in favour of protecting peoples’ rights.



The exception is the rule: the security AI imaginary

In a more ideological sense, the Act also contributes to a very particular ‘imaginary’ of AI. It invokes claims of urgency and emergency to justify restrictions on rights and safeguards. This is a familiar story, particularly for anyone who has lived through the growth, normalisation and bureaucratisation of the “war on terror.”⁷

What is more novel is the way these exceptions align with the visions put forward by some proponents of AI technologies.⁸ Bypassing normal procedures in the name of urgency rests upon an idea that there already



are, or will be, AI systems that are so effective or powerful that they will be able to protect society from various exceptional ‘threats.’

The law does not go into any details about what kind of AI system might be involved in such a situation. It is highly doubtful that any such AI system exists or will be built ([section 2.3.5](#)). This ideological role, however, fits neatly into a long, deeply-embedded history of techno-solutionism in EU policy-making.⁹



The police lobby: watering down safeguards

Part of the reason the law contains so many loopholes and exceptions is the result of lobbying by the police themselves. The police have also been working to develop tools for self-regulation, promoted as a way for security agencies to comply with the Act.¹⁰ Weakening the law in secret, whilst publicly calling attention to your efforts to comply with it, is hardly a demonstration of trustworthiness.

This was the public face of a broader, secret effort to undermine any potential protections in the law.

In May 2022, the European Police Chiefs Convention issued a public statement on the AI Act, calling for specific exemptions for police forces.¹¹ This was the public face of a broader, secret effort to undermine any potential protections in the law.

EU governments worked hard to water down safeguards in the Act, with the French authorities playing a key role.¹² Internal security officials in the Council also kept a close eye on proceedings. This was part of a

broader push to have “internal security needs” recognised in digital policies.¹³

Backing up this work was an obscure and secretive body called the European Clearing Board (EuCB, [section 4.1.3](#)). This is an informal group set up by senior EU member state police officers. The EuCB’s Strategic Group on AI worked extensively to weaken safeguards in the AI Act. One document obtained for this report says the EuCB’s lobbying:

...triggered important changes in the Council position on the AI Act, including on the definition, classification of systems, remote biometrics, use of dactyloscopy [fingerprinting] and exceptions for law enforcement (mandatory publishing of AI-systems in use or that are developed by law enforcement agencies).¹⁴

The EU treaties do not foresee a formal role for police agencies in negotiating new legislation, though it is hardly surprising that they engage in lobbying. **It is certainly unfortunate, however, that the EU’s secretive and opaque law-making system makes it essentially impossible for the public to be aware of it.**¹⁵



“Cutting-edge products for the security of citizens”

...formally accountable only to police and interior ministry officials.

The European Clearing Board (EuCB) is part of another new piece of institutional infrastructure: the Europol Innovation Lab. The Lab is based at Europol’s HQ in the Netherlands, and was set up to implement a December 2019 decision by EU interior ministers. The EuCB provides the Lab’s connection to national agencies and authorities.

The Lab, in turn, is a member and host of the EU Innovation Hub for Internal Security ([section 4.1.2](#)). The Hub brings together representatives of all the EU’s justice and home affairs agencies, covering “law enforcement, border management, criminal justice and the security aspects of migration and customs.”¹⁶

The Innovation Hub is supposed to “support the delivery of innovative cutting-edge products for the security of citizens in the EU,” through “the use and development of advanced

and emerging technologies.”¹⁷

It has yet to acquire the budget and staffing hoped for by officials, but has nevertheless coordinated a number of joint projects. In relation to AI, these include systems for profiling travellers to the EU, and research on biometric technologies for border and immigration control.¹⁸

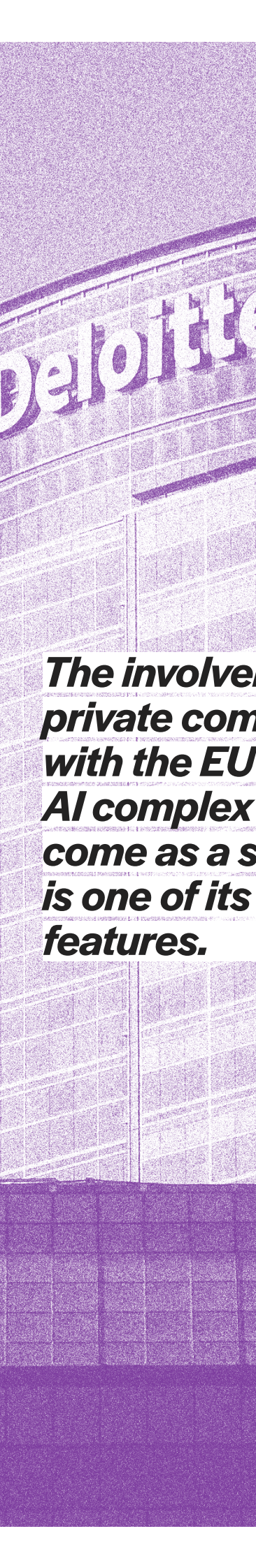
More recently, the Hub has been reorganised and is now based around a number of “clusters”, including one dedicated to AI. This was launched in spring 2024. It remains to be seen how the work of the cluster and the EuCB will develop. Doing so will be difficult without ongoing monitoring and investigation. They do not publish the agendas and minutes of their meetings, and are formally accountable only to police and interior ministry officials.



A “centre of excellence” for security AI?

On the opposite side of Europe, in Estonia, another EU agency has also been trying to build up institutional infrastructure for security AI. The agency, eu-LISA,¹⁹ is primarily responsible for the operation of the EU’s growing collection of large-scale policing, migration and criminal justice databases.²⁰

In October 2021, eu-LISA produced a “roadmap” setting out all “planned & potential, near to



medium/long term” AI initiatives. Amongst these was the development of a “Centre of Excellence for Artificial Intelligence in the Justice and Home Affairs Domain” ([section 4.1.1](#)).

Responsibility for developing this idea further was given to the multinational consultancy company Deloitte. It conducted a study that said the Centre of Excellence (CoE) would coordinate “the strategy for AI within the JHA domain.” The CoE would also set up “frameworks for future projects to speed up the adoption of AI.”²¹ Deloitte proposed the “strategy, purpose, requirements and operating model” for the CoE.

The agency did not give direct responses to questions from *Statewatch* on this topic, though it seems that the CoE

The involvement of private companies with the EU’s security AI complex should not come as a surprise: it is one of its defining features.

plan has been dropped, for now. If member states and the European Commission “consider that the creation of a Centre of Excellence for AI is necessary, the Agency will take the necessary steps to do so,” eu-LISA’s press office said. Currently, the agency is preparing an AI strategy to “serve as an umbrella for organising the internal governance on AI initiatives and ensuring compliance with the AI Act.”²²

Despite its fate, the CoE initiative is noteworthy for two reasons. Firstly, it may be indicative of future proposals to facilitate the development and use of security AI. Secondly, it is a remarkably wide-ranging initiative that was undertaken with no democratic scrutiny or oversight.

Based on the paper trail examined for this report, the very idea to set up a Centre of Excellence was first mooted in a report by Deloitte, itself based on interviews with EU officials. The idea was then adopted by EU institutions and agencies. This close involvement of private companies with the EU’s emerging security AI complex should not come as a surprise: it is one of its defining features.

Public-private partnership

The drafting of EU policy studies is often outsourced by the Commission to consultancy companies.²³ In the field of security AI, more and less well-known companies such as E&Y, Unisys, PwC, RAND Europe and Deloitte have all been involved in this kind of work. The aim of these studies is usually to set out policy options and explore their political, financial and institutional implications.

In practice, they largely seem to be a way to provide a veneer of independence and impartiality to proposals that are already more-or-less settled. At a minimum, it can be said they largely reflect the views of Commission and EU member state officials, as these tend to be the people interviewed for the studies. In this regard, they reflect the undemocratic nature of law and policy-making in the EU.²⁴

Public-private cooperation extends much further than this, however. The databases and information systems managed by eu-LISA are already a public-private endeavour.

Billions of euros have been awarded to multinational technology and consulting companies to set up, operate and maintain them,²⁵ making public institutions structurally dependent on the private sector.

This dependency is likely to increase as AI, alongside other digital technologies, becomes further embedded in security policies and structures. This is actively invited by the EU's justice and home affairs agencies, which regularly hold "industry days" where companies can market their products.

Then there is the EU's security research programme, which since 2003 has provided billions of euros for security and surveillance technologies.²⁶ These research projects are used to develop new forms of security AI. Both Europol ([section 4.2.2](#)) and Frontex ([section 4.1.4](#)) now have a structural, agenda-setting role in the programme, giving them influence over technology research and development.²⁷

The influence of the private sector on the public sector can also be considered from other angles. One internal Europol document says the agency's work on AI aims for "value creation at speed" – a term which, at least in part, recalls the Silicon Valley motto of "move fast and break things."²⁸



From institutional to technical infrastructure

Alongside new institutional infrastructure, the security AI complex also requires technical infrastructure: hardware and software that can process vast amounts of data. Two separate, but parallel, initiatives are underway in this area.

The first of these is part of a broader EU plan to create an array of “common European data spaces” ([section 4.2.1](#)). These will be made up of interconnected, but separate, datasets held by different organisations and institutions. The data will be used to train AI systems. Around 20 data spaces have so far been announced in sectors such as health, agriculture, finance, mobility, energy, public administration, and security.

The “Security Data Space for Innovation” (SDSI) will initially target law enforcement agencies. Border, immigration, criminal justice and customs agencies will later have access. Technologies of interest include automated image recognition and video analysis.

However, the plan has had a rocky start. There have been problems finding contractors to develop the SDSI. After scaling back the ambition of its initial plans, the Commission provided €1 million for a project to carry out “preparatory work needed for the creation of high-quality large-scale shareable data sets for innovation.”²⁹

The result was the TESSERA project. Amongst other things, it will map the types of datasets that could be shared through the SDSI, including:

- photos;
- videos;
- voices samples;
- unstructured text, such as that on web forums;
- unstructured hybrid data, for example scraped from websites or emails;
- structured data, such as telecommunications metadata.^{30,31}





Europol: AI sandbox

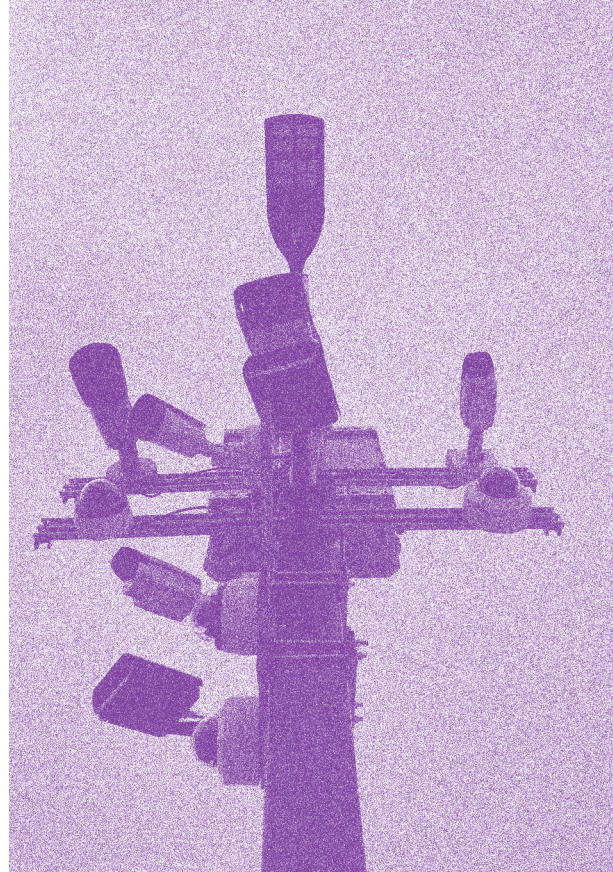
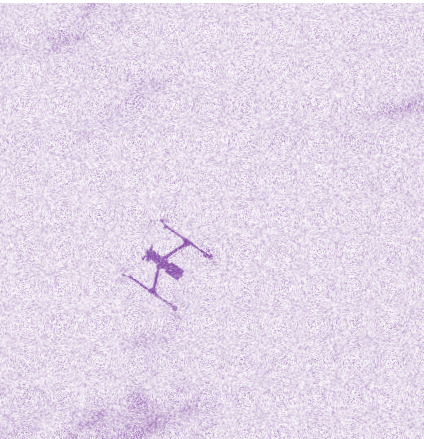
Europol is also working to develop technical infrastructure for developing and testing security AI ([section 4.2.2](#)). **Specific topics of interest include voice print analysis, age and gender detection from audio recordings of voices, and the use of augmented and virtual reality for data analytics.**

As part of this work, it is developing a “sandbox” – an isolated technical environment in which software can be developed and tested with no external effects. Under the AI Act, member state governments are obliged to set up at least one sandbox for use by AI companies, externalising the costs of private sector “innovation” onto the public.

Documents obtained for this report describe a plan to divide Europol’s sandbox into two separate areas: one in which personal data cannot be

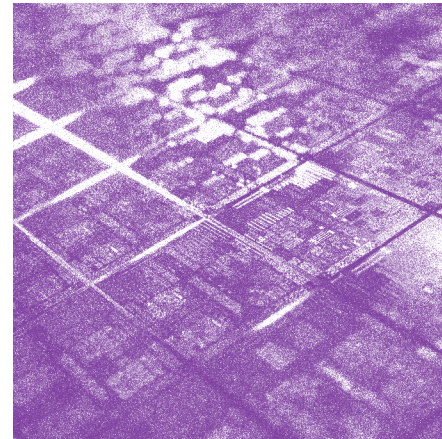
processed, and one in which it can. The latter would make it possible to test new algorithms or techniques “against a live, operational dataset containing personal data.”³² Of course, technologies that are not tested on personal data, or that do not make use of personal data, may still have very personal effects: arrest, questioning, or search and seizure of possessions.

The aim is to have the sandbox up and running as soon as possible. One Europol document describes it as having “paramount strategic significance as it will enable Europol to fulfil its role in leading Law Enforcement Innovation.” It is “a precondition and enabler” and an “infrastructural foundation” for “numerous depending initiatives.”³³



“
***What power
have you got?***

Tony Benn



Questioning the security AI complex

There is a vast ongoing effort from technology companies, governments and other “stakeholders” to insert increasingly powerful technical systems into every aspect of life and society. **This is a political issue and dealing with it requires more democracy, not less. Yet, in relation to security policies and security agencies, less democracy is exactly what the public is being given.**

The AI Act provides an extremely limited framework for the oversight and accountability of security AI. That being said, the law is also confusing and unclear, and it is likely many aspects will be clarified through jurisprudence. Effective legal challenges would see that jurisprudence lead to increased oversight.

The new infrastructure being established to embed security AI in EU policy and practice is secretive, complex and confusing. Even basic transparency measures are lacking: the publication of agendas, minutes and other documentation. This may sound mundane, but it is crucial for democracy. It allows the public to see what is being done in their name, with their money, by whom. Transparency is a fundamental prerequisite for accountability – whatever form that accountability takes.

Other angles are also important: the rapid development of AI technologies and their underlying infrastructure are creating huge demands on the world's natural resources, in particular water and energy. Security AI is by no means the largest part of this problem, but these questions must be taken into account. There is no sign so far of this happening.

The late British politician, Tony Benn, had five questions that he would ask “everywhere he went... on the chalkboards of classrooms and lecture halls... at rallies, protests and marches.” The questions are more relevant than ever - particularly in a context where supranational institutions and agencies continue to accrue new powers and competences:

“What power have you got?”

“Where did you get it from?”

“In whose interests do you use it?”

“To whom are you accountable?”

“How do we get rid of you?”³⁴

With regard to the last question, Benn would say that anyone who cannot answer it “does not live in a democratic system.” **In the interests of a democratic system, then, the least that could be done is for the public and their elected representatives to start asking more questions about the security AI complex.** What follows from those questions remains to be seen.

Notes

1. ['Prime Minister sets out blueprint to turbocharge AI'](#), 12 January 2025
2. [eu-LISA Working Group on AI, 1st meeting minutes](#), 11 May 2021
3. ['Europe's techno-borders'; 'Frontex and interoperable databases: knowledge as power?'; 'Deportation Union: Rights, accountability and the EU's push to increase forced removals'; 'Automated Suspicion: The EU's new travel surveillance initiatives'](#)
4. In the UK, an official report found that London's Metropolitan Police are "institutionally misogynist." See: ['What is institutional misogyny in policing and why does it matter?'](#), University of Liverpool, 4 September 2023
5. Fundamental Rights Agency, ['Tackling racism in policing'](#), 10 April 2024
6. JUSTICIA, ['Disparities in Criminal Justice Systems for Individuals of Different Ethnic, Racial, and National Background in the European Union'](#), November 2018
7. Gene Ray, ['On the targeting of activists in the "War on Terror"'](#), *Statewatch*, 1 July 2008
8. At the extreme end, this includes those who believe that humans will merge their consciousness into, or with, some sort of hyper-powered AI, and through that process become immortal. See: [Darren Orf, 'A Scientist Says Humans Will Reach the Singularity Within 21 Years'](#), *Popular Mechanics*, 8 August 2024,
9. ['NeoConOpticon: The EU Security-Industrial Complex'](#), *Statewatch/Transnational Institute*, 17 February 2009
10. ['New Accountability Framework to use artificial intelligence in a transparent and accountable manner'](#), 10 March 2022
11. ['Joint Declaration of the European Police Chiefs'](#), 24 May 2022
12. ['France spearheads member state campaign to dilute European AI regulation'](#), *Investigate Europe*, 22 January 2025
13. ['Exceptions, loopholes and carve-outs: Presidency wants "internal security needs" recognized in EU digital policies'](#), *Statewatch*, 23 February 2023,
14. Innovation Hub Team, ['EU Innovation Hub for Internal Security – multi-annual planning of activities 2023-26'](#), Council doc. 5603/23, LIMITE, 16 February 2023, p.21
15. ['Trilogues: the system](#)

- [that undermines EU democracy and transparency](#), *European Digital Rights*, 20 April 2016;
- ['EU: Civil society calls for rights to be prioritised in secret AI Act "trilogue" negotiations'](#), *Statewatch*, 12 July 2023
16. ['EU Innovation Hub for Internal Security'](#), 5757/20, 18 February 2020,
 17. ['EU Innovation Hub on Internal Security'](#), 5757/20, 18 February 2020
 18. ['Europe's techno-borders'](#), pp.36-39
 19. Its full name is the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.
 20. ['EU agencies and interoperable databases'](#)
 21. Deloitte study for European Commission, ['Deliverable 3.01: AI Centre of Excellence definition'](#), HOME/2020/ISFB/FW/VISA/0021, undated, p.6
 22. Email, 8 February 2025.
 23. European Court of Auditors, ['External consultants at the European Commission: Scope for reform'](#), 2022
 24. ['Study proposes giving EU complete control over Schengen borders'](#), *Statewatch*, 10 December 2014
 25. ['EU agencies and interoperable databases'](#)
 26. The programme currently has
- the formal title ['Civil Security for Society'](#)
27. Forthcoming work by the *Resist Europol* network will analyse the role of the EU security research programme in developing security AI technologies.
 28. ['Did Mark Zuckerberg Say, 'Move Fast And Break Things'?'](#), *Snopes*, 29 July 2022
 29. European Commission, ['Call for proposals on data sets for the European Data Space for Innovation'](#), 21 March 2023
 30. For an explanation of metadata, see: ['What is Metadata? An introduction'](#), GSMA, undated
 31. European Commission, ['Call for proposals on data sets for the European Data Space for Innovation'](#), 21 March 2023
 32. Europol, ['Building the Research and Innovation Pipeline: Update on the implementation of article 33a and the R&I Sandbox environment'](#), 17 April 2023, EDOC #1301551v2, document for meeting of the Information Management Working Group meeting on 16-17 May 2023
 33. Europol Innovation Lab, ['Progress Report and Strategic Priorities 2024-2026'](#), 22 September 2023, EDOC #1321956v13, p.5
 34. John Nichols, ['Tony Benn and the Five Essential Questions of Democracy'](#), *The Nation*, 14 March 2014

Image credits

Cover: “[2012-10-17 17-41-39.jpg](#)” by Matthias Vandegaer

Page 3: [EPCC 2024 Head of Delegations](#), from EUROPOL; “[black and white concrete building](#)” by Possessed Photography; “[Speech of Commissioner Avramopoulos at the Frontex Conference on the European Day for Border Guards, Warsaw Poland](#)” by Dimitris Avramopoulos

Page 4: “[The doctor’s hand in a white medical glove](#)” by Diana Polekhina

Page 5: “[Gatwick Airport passport control, Covid-19](#)” by Mark Hodson ([follow](#))

Page 6: [EUROPOL badge](#), from EUROPOL

Page 7: “[film the police](#)” by Steev Hise

Page 8: “[two men wearing helmets](#)” by Ben Koorengevel

Page 9: [EUROPOL building](#), from EUROPOL; “[smoke](#)” by Corina Rainer

Page 10: “[Riot police](#)” by Ivan Bandura; “[smoke](#)” by Corina Rainer

Page 11: “[a neon sign that reads emergency use only](#)” by Jinsoo Choi

Page 12: “[Top Secret](#)” by Vs Heidelberg Photos

Page 13: “[War on terror? War is terror](#)” by Anna Hanks

Page 14: “[Riot police](#)” by Synne Tonil

Page 15: “[Riot police Budapest](#)” by Ronan Shenhav

Page 16: “[outdoor festival - access denied](#)” by Giuseppe Savo

Page 17: [Artificial Intelligence eu-LISA Industry Roundtable Event Report](#), from eu-LISA

Page 18: “[Deloitte](#)” by fourbyfourblazer

Page 20: “[CERN DAY #2](#)” by Rosa Menkman

Page 21: “[Ask About: Facial Recognition 2.0](#)” by World Economic Forum

Page 23: “[black and white no smoking sign](#)” by Waldemar; “[a traffic light with multiple cameras attached to it](#)” by Andrew Heald; “[insect flying close-up photography](#)” by Kelly Sikkema; “[iridescent microchips](#)” by Ai.Comput’In