EU Proposal for Artificial Intelligence Regulation and the need for stricter approach to biometric surveillance

Irena Nesterova, University of Latvia, Latvia
Helene Oppen Ingebrigtsen Gundhus,
University of Oslo, Norway

CUPP
Critical Understanding
of Predictive Policing

NordForsk

The 8th International Scientific Conference of the Faculty of Law, the University of Latvia
21-22 October, 2021, Online

The AI Act and fundamental rights

AI Act aims to:

- foster the development, use and uptake of AI in the internal market
- create the ecosystem of trust by seeking to ensure protection of safety, fundamental rights and EU's values

Ensuring a high level of protection for fundamental rights requires also to introduce the prohibitions of certain AI-practices that violate fundamental rights

Fundamental rights risks

- Human dignity
- Privacy and data protection
- Non-discrimination
- Freedom of expression
- Freedom of peaceful assembly
- etc.

“The clearest distinction between AI systems in authoritarian countries and AI systems in democratic countries is the use of facial recognition for mass surveillance. Such indiscriminate ongoing surveillance is intended precisely to coerce social behaviour and to control populations”

CAIDP. (2021). Statement on Proposed EU AI Regulation.

Calls for the red lines

“AI systems should not be used for social scoring and mass surveillance purposes”

UNESCO Draft Recommendation on the Ethics of Artificial Intelligence, para 26.

Calls for the red lines

The United Nations High Commissioner for Human Rights recommends the States:

- Expressly ban AI applications that cannot be operated in compliance with international human rights law and impose moratoriums on the sale and use of AI systems that carry a high risk for the enjoyment of human rights, unless and until adequate safeguards to protect human rights are in place
- Impose a moratorium on the use of remote biometric recognition technologies in public spaces, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards and the absence of significant accuracy issues and discriminatory impacts […]

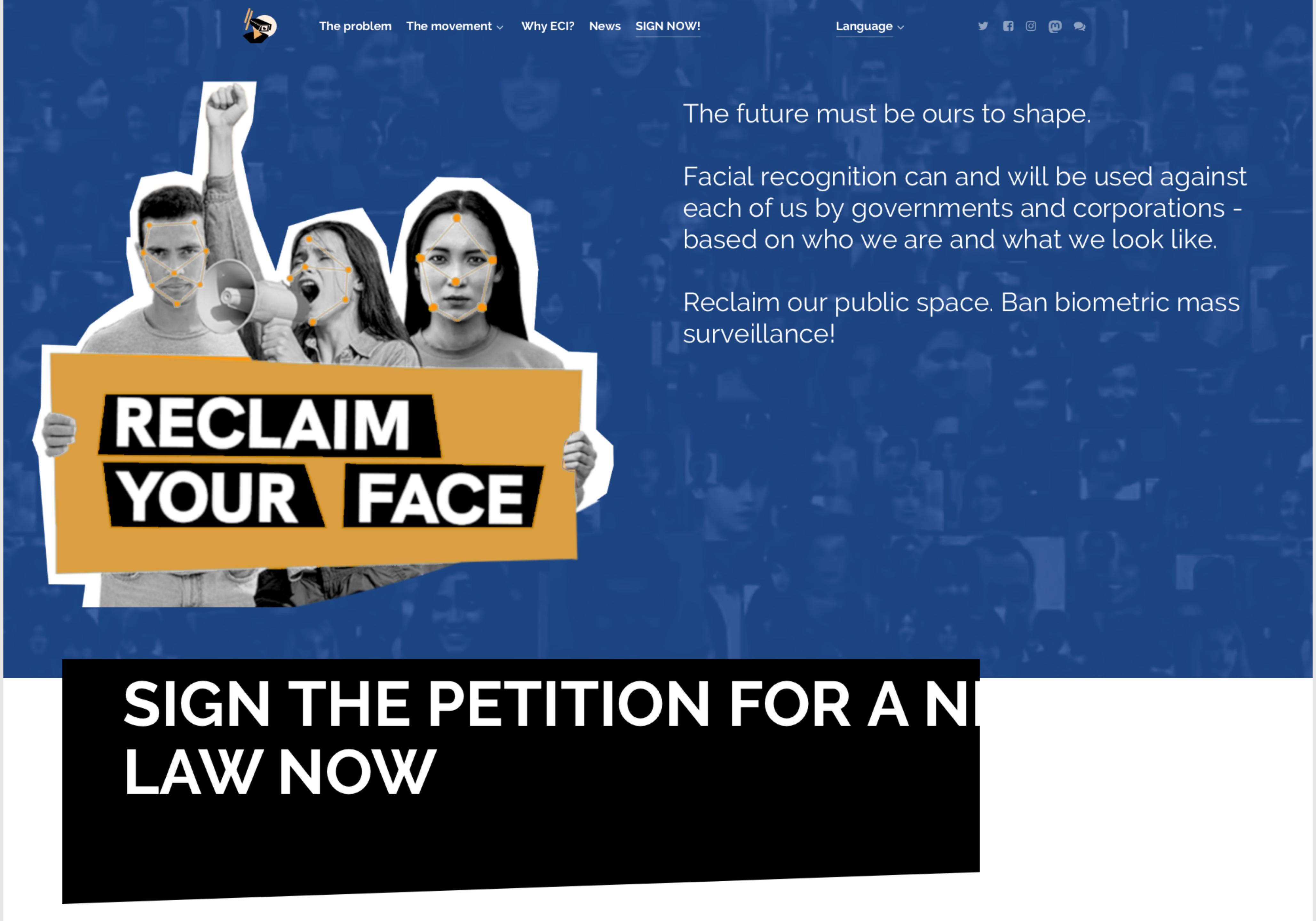
Report of the United Nations High Commissioner for Human Rights “The right to privacy in the digital age”, 2021.

Calls for the red lines

European Parliament calls for:

- a moratorium on the deployment of facial recognition systems for law enforcement purposes that have the function of identification unless strictly used for the purpose of identification of victims of crime,
- the prohibition of the use of automated analysis and/or recognition in publicly accessible spaces of other human features, such as gait, fingerprints, DNA, voice, and other biometric and behavioural signals
- a ban on the use of private facial recognition databases in law enforcement

European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))



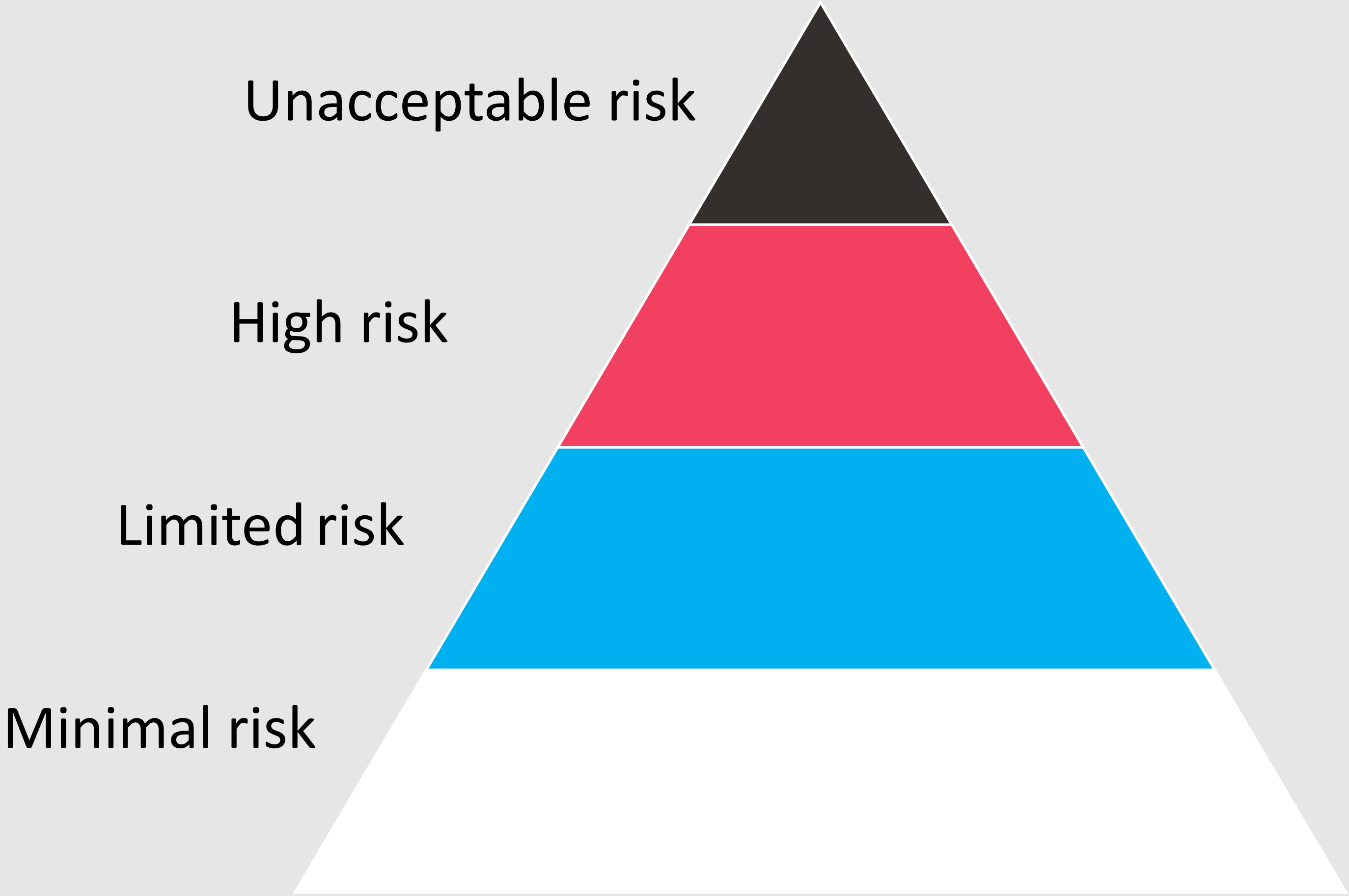
The future must be ours to shape.

Facial recognition can and will be used against each of us by governments and corporations - based on who we are and what we look like.

Reclaim our public space. Ban biometric mass surveillance!

SIGN THE PETITION FOR A NI
LAW NOW

Risk-based approach in the AI Act



Unacceptable risk

High risk

Limited risk

Minimal risk

Prohibited AI practices

1) the deployment of subliminal techniques beyond a person's consciousness
2) the exploitation of vulnerabilities of specific vulnerable groups
3) social scoring for general purposes done by public authorities
4) the use of
   i. real-time
   ii. remote
   iii. biometric identification systems
   iv. in publicly accessible spaces
   v. for the purpose of law enforcement,

   An exhaustive list of exceptional cases in which the prohibition does not apply

The need to remove exceptions and loopholes

Legal requirements for high-risk AI systems

- Risk assessment and mitigation
- High quality of data sets used
- Technical documentation and record-keeping
- Transparency and the provision of information to users
- Human oversight
- Robustness, accuracy and cybersecurity

- *Ex-ante* conformity assessment
  - through internal control checks
  - with the exception of remote biometric identification systems that would be subject to third party conformity assessment

Third party conformity assessment should be required in all cases

No reference to the rights of individuals as well as complaints and redress mechanisms

Compliance with data protection law

- The fact that an AI system is classified as high risk should not be interpreted as indicating that the use of the system is necessarily lawful under other acts of EU law or under national law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons.
- The AI Act should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant.

(Recital 41)

EDPB and EDPS recommends to introduce a clear obligation to comply with data protection law.

High-risk AI systems

Areas listed in Annex III, including:

- Biometric identification and categorisation of natural persons
- AI systems used in law enforcement, including:
  - for making individual risk assessments of natural persons in order to assess the risk for offending or reoffending or the risk of potential victims of criminal offences
  - predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons or assessing the personality traits and characteristics or past criminal behaviour of natural persons and groups
  - AI systems used as polygraphs and similar tools or to detect the emotional state of a natural person

Biometric categorisation and emotional recognition

AI Act proposal classifies as:

- limited risk systems with limited transparency rules
- high risks AI system, e.g. in the areas of education, employment, law enforcement, migration

However, these AI systems:

- raise significant risks to human dignity, autonomy, the right to privacy, non-discrimination and other fundamental rights
- no scientific evidence proving their abilities

Reconsidering the classification of high-risk and limited risk AI systems

Calls for ban on:

- any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals - in any context,
- biometric categorisation, for both public authorities and private entities
- the use of predictive systems by law enforcement authorities that determines and classifies person's future behaviour
- the use of AI to infer emotions of a natural person, except for certain well-specified use-cases, namely for health and research purposes.

EDPS, EDPB, Joint Opinion 5/2021, endorsed by EDRI, CAIDP, ALLAI etc.

Lessons and warnings for European countries

CUPP

- Brings together seven partner organisations from Denmark, Norway, Latvia, Estonia and the United Kingdom to explore the digital transformation of law enforcement and its impact on crime detection and prevention
- aims to identify and critically assess the effects and impact of data-driven police technologies on society and end-users.

IT University of Copenhagen

PROSA
Forbundet af It-professionelle

UNIVERSITY OF LATVIA

TALLINN UNIVERSITY OF TECHNOLOGY

CUPP Critical Understanding of Predictive Policing

UNIVERSITAS OSLOENSIS MDCCCXI

University of St Andrews

BSC BALTIC STUDIES CENTRE

National case studies

DENMARK	General crime	• POL-INTEL - Intelligence-led policing platform
NORWAY	Youth crime/gangs	• Risk assessment tools
LATVIA	Road traffic safety	• Future Intelligent Transport Systems • Unmarked police bus with a 360-degree camera, drones • Drones • Smartphone apps allowing citizens to report crimes and incidents
ESTONIA	Data instead of humans on the move	• Genetic engineering (CRISPR-Cas9) • E-residency and digital migration • Border control & smart city
SWEDEN	Enhancing policing power for security guards	• Gothenburg’s Brunnsparken, private security
UNITED KINGDOM	Urban public space policing	• London’s St Pancras, facial recognition system

Norway: Forecasting future crimes & criminals

Focus: Predictive policing as a tool for reducing uncertainty and risks in the Norwegian police.

Case studies: exploring differences in the use of predictive policing efforts, depending on whether data-driven algorithms are integrated in the software program or not. Comparing Denmarks Pol-Intel

Norway: Data collection (2019-2024)

- 2019: Intelligence to prevent youth crime, gangs and violence in South Oslo, 10 interviews, 8 observations

- 2021-23: Risk assessment tool – risk-need (with Pernille S. Eriksen)
  - Analysis policy documents and 10 interviews with decision-makers and software engineers, 15 interviews with OP Super and other relevant cases/direct observation (CUPP)

- 2021-24: Interviews and observations Algorithm goverance and policing cultures (ALGOPOL, NRC) – with Christin Wathne & Tereza K. Østli
  - in police districts, special units and collaborators, software engineers, decision makers and developers
  - document and analysing data registrers

Analysing shift towards big data surveillance

- To what degree are discretionary assessments of risk supplemented and quantified using risk scores?
- To what degree are data used for predictive, rather than reactive or explanatory, purposes?
- To what degree makes the proliferation of automatic alert systems it possible to systematically surveil an unprecedentedly large number of people?
- To what degree is the threshold for inclusion in law enforcement databases lower, now including individuals who have not had direct police contact?
- To what degree are previously separate data systems merged, facilitating the spread of surveillance into a wide range of institutions?

Thank you!