CUPP

Critical Understanding
of Predictive Policing

- An ideas catalogue

What does it mean to have a more digitalised police?

Can technology predict and prevent crime?

How are my rights protected when the state knows more and more about me?

Which technologies and what issues are at stake?

Who is watching the watchers?

Understand what is at stake for you as a citizen when the police becomes increasingly digital.

PROSA
The Association of IT-professionals

Supported by:
NordForsk

A Critical Look at the Digital Transformation of Law Enforcement

Content

This catalogue provides an overview of key issues and concerns associated with the ongoing digitalisation of police work, encompassing a wide range of processes across various areas, including traffic and border control, crime prevention, and the prediction of future crimes.

The primary focus remains on privacy, transparency, and fundamental human rights, while critically exploring a broad array of new and emergent digital technologies that promise faster investigations and more effective crime fighting.

In this way, the goal is to offer a range of tools and explanations designed to make a sometimes technical discussion more accessible to a broader audience, rather than to deliver a complete and exhaustive analysis.

The catalogue includes:

The specific content has been selected and compiled by the team behind the larger research project CUPP: Critical Understanding of Predictive Policing. This project, along with its activities, methods, and subprojects, is described in the catalogue (pages 14-16). The scientific frameworks used are outlined on page 3.

On behalf of the CUPP team, September 2024

Critical Understanding of Predictive Policing (CUPP)

Website: www.cuppresearch.info
Time period: January 2021 – January 2025
Participants:
Academic institutions
IT University of Copenhagen (DK)
Tallinn University of Technology (EE)
Baltic Studies Centre (LV)
University of Latvia (LV)
University of Oslo (NO)
Oslo Metropolitan University (NO)
University of St. Andrews (UK)
Communication Partner
PROSA – Danish Association of IT Professionals (DK)

Research grant
NordForsk, Project number 100786

WHAT: The first major interdisciplinary and inter-European research project aiming to identify and critically assess how data-driven police technologies affect crime detection, crime prevention, society, and the people who use these technologies.

HOW: Our methods include classical academic research, production of scientific articles, hosting public citizen seminars as well as international conferences jointly for researchers and practitioners.

WHERE: Geographically we focus on cases in the UK and the Nordic-Baltic region while retaining a cross-border and global orientation.

WHO: Seven academic institutions and one communication partner, with projects in six European countries – Denmark, Norway, Sweden, Latvia, Estonia and the United Kingdom. Funded under the NordForsk Research and Innovation Programme on the Digitalisation of the Public Sector.

Our approach

Drawing on an interdisciplinary framework, the CUPP research team explored the impact of increasing digitalisation in policing based on the following ideas:

- We take a broad view, looking at everyday practices, institutional values, and high-level strategic decisions.
- We examine how data analytics is changing ethical, legal, social, and behavioural aspects.
- We focus on social and ethical concerns, including human rights, fundamental freedoms, data justice, security, and privacy.

Applied Scientific Frameworks

Science and Technology Studies (STS)
A field of study that critically examines how science and technology are created, developed, and impact society, considering the historical, cultural, and social context.

Critical Criminology
A diverse body of theories that explore crime from a broader perspective than traditional notions of 'deviance', anti-social behaviour, and more effective law enforcement. Instead, it examines issues such as power dynamics, social inequality, and the ways biases are maintained as well as topics such as racism and marginalisation.

Critical Data Studies (CDS)
Studies that look at the cultural, ethical, and critical issues that come with Big Data. Instead of viewing Big Data as neutral and objective, CDS insist on a broader perspective, considering how data is created, managed, and the power it holds.

Data science
A field that combines different disciplines and use statistics, computing, and scientific methods to draw knowledge and insights from potentially noisy, structured, or unstructured data.

Urban Studies
A field that studies the complex social, economic, environmental, and political aspects of cities. It brings together ideas from sociology, geography, economics, political science, and urban planning to understand how cities grow, function, and are governed.

Issues that should concern more people – and why

Based on the CUPP project, we have compiled a list of key concepts and issues essential for an informed discussion on the ongoing digital transformation in policing.

Predictive Policing: A method that uses large amounts of data, aiming to predict and prevent possible future crimes. Once seen as a potential police 'super-weapon', it has increasingly been criticised for unrealistic expectations, inaccurate predictions, and violations of rights like privacy, non-discrimination and the presumption of innocence. Banned under the EU AI Act in relation to profiling individuals – unless it is used to support human assessment of a specific person and is based on solid evidence directly linking this person to a crime. The term has now mostly been replaced by concepts such as **intelligence-led policing (ILP), precision policing,** or smart policing, which all focus on data-driven approaches.

'Black Box': A system where you can see what goes in and what comes out, but not how it works inside. Its inner workings are hidden, making it non-transparent and unaccountable to the public and even experts.

Feedback Loops: A process where the output of a system is fed back into it as input, potentially reinforcing biases. In policing, this might mean officers are repeatedly sent to certain areas based on past data, regardless of the actual crime rate.

Confirmation Bias: The tendency to seek out and focus on information that supports one's existing beliefs, while ignoring information that contradicts them. This bias can affect how data is coded, collected, and used in police systems.

Function Creep: The gradual expansion of a technology's use beyond its original purpose, often leading to (unintended) privacy violations. May be contradictory to the principle of purpose limitation required by GDPR.

Technological Fix: Trying to solve a problem solely with technology, rather than considering other solutions in the political, legal, organisational, or social areas.

Mass Surveillance: The collection, processing, and storage of data on large groups of people, without necessarily starting with specific suspicions about individuals.

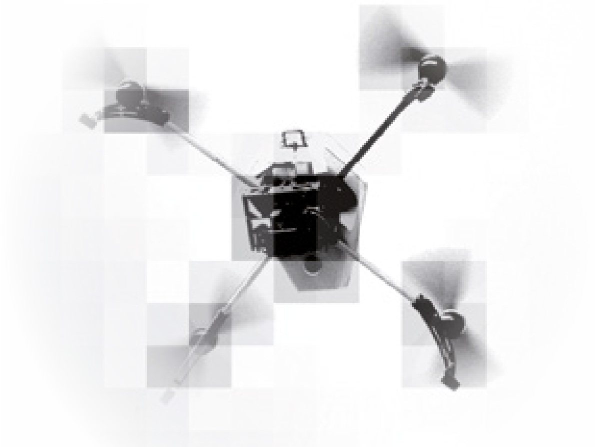
AI Surveillance: A type of surveillance that not only collects data but also uses AI or Machine Learning to better identify and distinguish people and objects.

Sousveillance or Counter-Surveillance: When citizens monitor those who are watching them, like using cameras to document police actions or mapping CCTV cameras. This is done to expose possible abuses or to gain and distribute insights.

Automated Policing/Law Enforcement Technologies: Technologies where computers handle surveillance and data processing, and may even carry out law enforcement actions, such as issuing speeding tickets.

Automated Decision Making (ADM): Decisions made by algorithms, with varying degrees of human intervention. Restricted by the EU's General Data Protection Regulation (GDPR), stating that citizens should not be subject to decisions or profiling with legal or other significant effects based solely on automated processes.

Centralisation: Increased exercise of control and knowledge production, obtained by accumulating and integrating diverse databases on crime, finance, education, and transportation.



Banned by the EU AI Act – fully or partly

New technologies bring new concerns and risks of misuse. The EU AI Act, which became law on August 1, 2024, is one of the most detailed regulations for surveillance technologies. It is generally strict and bans certain technologies but also makes exceptions.

Banned technologies:

- AI-based predictive policing systems
- Live facial recognition in public spaces
- Biometric categorisation systems based on sensitive characteristics
- Emotion recognition in workplaces and schools
- Untargeted scraping of facial images, adding material to facial recognition databases
- AI-based social scoring
- Applications that manipulate human behaviour and deploy subliminal techniques
- AI systems that exploit individual vulnerabilities or specific vulnerable groups

Exceptions:

The AI act makes exceptions from the prohibitions, such as:

- Law enforcement activities related to 16 specified very serious crimes such as terrorism or kidnappings
- Targeted search for specific missing persons or victims of abduction, trafficking or sexual exploitation
- The prevention of foreseeable terror attacks or imminent threats to the life or physical safety of persons.

As with all legislation, the full implications of the exceptions will become clearer with more legal practice.

Disputed police technologies and their legal status

New hardware and software constantly challenge current legal and ethical boundaries, especially in automated policing and law enforcement. We have assembled a list of the most prevalent technologies, focusing on their possible use and their present legal status.

Forecasting Hotspots: Locations or time slots with unusually high rates of certain events. These can create feedback loops, leading to repeated focus on the same areas.

Remote Biometric Identification (RBI): Systems that identify people from a distance by comparing their unique biometric features with a database. Classified as 'high-risk' under the EU AI Act due to concerns over technical inaccuracy as well as fundamental rights such as privacy, data protection and non-discrimination.

'Real-time' Remote Biometric Identification (RBI): Considered especially intrusive because it allows limited time for checks and corrections and could affect fundamental rights like the freedom of assembly. Banned in public spaces for law enforcement under the EU AI Act, except in specific cases such as targeted search for individuals either missing, having committed a crime without being prosecuted yet or being victims of abduction, trafficking or sexual exploitation. Also allowed for the prevention of imminent terror attacks or other physical threats against one or more individuals.

Emotion Recognition: A type of RBI used to identify people's emotions or intentions based on biometric data. Banned in workplaces and schools under the AI Act due to its intrusive nature and disputed scientific validity but allowed in strictly medical or safety contexts.

Facial Recognition Technologies (FRT): The most common but also one of the most controversial types of RBI, with high error rates, especially for black people and women. Classified as high-risk, but not forbidden.

AI Systems Creating or Expanding FRT Databases: Prohibited when built via untargeted scraping of facial images from the internet or CCTV footage, as this practice converges mass surveillance and according to the EU AI act can lead to "gross violations of fundamental rights, including the right to privacy".

AI-based social scoring: Automated creation of risk profiles of individuals based on multiple data points related to their behaviour, such as criminal or financial activities. Classified as prohibited under the AI Act in relation to essential private and public services and benefits, due to the risk of discrimination and violation of dignity.

Automatic Number Plate Recognition (ANPR): High-speed cameras that capture vehicle details like license plates, time, and location. A form of mass surveillance used to identify vehicles, but potentially also where their drivers live, attend political meetings, visit bars or practice their religion. Acknowledged by the Hague district court in 2024 as interfering with privacy rights but deemed lawful and proportional due to its legitimate purpose, proven effectiveness, and adequate safeguards to prevent abuse.

Police Drones: Unmanned flying devices used increasingly for surveillance and crowd control, either remotely controlled or autonomous.

Body-Worn Cameras (BWCs): Cameras worn by police officers to capture audio and video of incidents. They aim to provide an unbiased record but have been criticised for privacy violations, especially when combined with facial recognition software.

Enhanced Video Analysis: AI-powered tools that quickly analyse large amounts of video data, aiding in surveillance, crime detection, and evidence gathering.

Audio and Visual Forensics: Multi-pronged analysis of audio-visual evidence, often combining camera footage with crowd density analysis, 3D modeling, and signal processing.

Gunshot Detection Systems: Sensors that detect and locate gunfire in real-time, immediately alerting law enforcement with precise location data for a quick response.

Real-Time Crime Analysis: AI-assisted monitoring of sources such as cameras and sensors to detect suspicious activities, enabling quick responses and crime prevention.

Social Media Monitoring Software (SMM): Tools for tracking and analysing people's communications, networks, and associations on social media. Can monitor protests, identify social and political leaders, and measure their influence – including information on ethnicity, religion, gender identity, personality traits and health. A potentially powerful tool for the police, but also a serious invasion of privacy that could wrongly implicate an individual or group in criminal behaviour, target innocent speech and harm public debate.

Spyware: Software that secretly collects personal information from a device and sends it to third parties, whether advertisers, criminals or police. Notable examples include *Pegasus*, used for years by various EU (Greece, Poland, Hungary, Spain and Cyprus) and non-EU governments against political opponents, journalists, lawyers and others under the pretext of national security. Prohibited towards journalists under the European Media Freedom Act (EMFA) from March 2024, allowing it however on a "case-by-case basis and subject to authorisation by a juridical authority investigating serious crimes punishable by a custodial sentence".

Open-Source Intelligence (OSINT): Information gathered from publicly available sources, increasingly aided by data mining, machine learning, and other technologies. Prone to misinformation and bias.

NGOs, tools and resources for you to engage with

Watching the watchers is an important discipline for NGOs, journalists, and researchers who focus on citizens' rights. As police work becomes more digital, some groups have specialised in this area – free for you to follow, join, or consult with. The list below is not exhaustive, but it gives you an idea of the range of organisations involved:

NGOs and institutions

Baltic Human Rights Society: *https://www.baltichumanrights.org/en/*
An NGO aiming to promote a culture of human rights in the Baltic region. Conducts research and educational activities and publishes guides, tests and reports. Based in Latvia.

Big Brother Watch: *https://bigbrotherwatch.org.uk/*
A non-profit organisation focusing on civil liberties and privacy. Runs campaigns and research activities on topics such as facial recognition, election watch and more. Based in the UK.

Civil Liberties Union for Europe: *https://www.liberties.eu/en*
An NGO focusing on human rights in the EU. Runs advocacy campaigns and educational activities. Present in 18 countries across Europe.

Civil Rights Defenders (CRD): *https://crd.org/*
An NGO focusing on support to local human rights defenders in the world's most repressive regions, and to be Sweden's local civil rights watchdog group. Based in Sweden.

Danish Institute for Human Rights: *https://www.humanrights.dk/technology*
An independent national human rights institution, funded by the Danish government.

Data Justice Lab: *https://datajusticelab.org/*
A research lab focusing on the intersection of datafication and social justice issues. Part of Cardiff University's School of Journalism, Media and Culture (JOMEC).

EDRi: *European Digital Rights: https://edri.org/*
An international advocacy group consisting of more than 50 non-profit organisations, experts, advocates and academics working to defend and advance digital rights across the continent.

Estonian Human Rights Center: *https://humanrights.ee/en/*
An NGO focusing on diversity, inclusion, and human rights. Has a high focus on digital rights and data protection. Located in Estonia.

Homo Digitalis: *https://homodigitalis.gr/en/about-us/*
An NGO focusing on the protection of digital rights in Greece.

Privacy International *https://www.privacyinternational.org/*
An NGO with an international focus, working to promote privacy, democracy and accountability and provide ways to take concrete action. Based in the UK.

Reclaim Your Face: *https://reclaimyourface.eu/*
A campaign organisation aiming for a complete ban on biometric surveillance practices in the EU. Highly critical of the EU AI act which they see as filled with loopholes. Also they see it as legalising biometric surveillance insofar as it introduces conditions on how to use these systems.

SIPR – Scottish Institute for Policing Research: *https://www.sipr.ac.uk/*
Independent research and evidence-based contributions to policing policy and practice, founded in collaboration between Scottish universities, Police Scotland and The Scottish Police Authority.

Statewatch: *https://www.statewatch.org/*
An NGO that monitors and reports on civil liberties and the state in the EU and beyond in order to inform and enable a culture of diversity, debate and dissent. Based in the UK.

Technopolice: *https://technopolice.fr/*
A campaign and documentation project focusing on "Safe City" projects, automated video-surveillance and predictive policing technologies. Based in France.

Tools

Atlas of Surveillance: *https://atlasofsurveillance.org/*
A database of surveillance technologies used by US police agencies, facilitated by the Electronic Frontier Foundation and the Reynolds School of Journalism, University of Nevada.

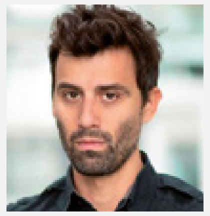
CCTV Open Street Map: *https://cctv.masspirates.org/*
Locations of all CCTV cameras worldwide that have been registered in Open Street Map. Made in collaboration with the Boston Institute for Nonprofit Journalism.

Mapping Police Violence: *https://mappingpoliceviolence.org/*
A US-based collaborative research project. Their website is a police accountability tool featuring interactive tools, maps, and figures that illustrate the impact of police violence in the United States.

Surveillance Cities: *https://surfshark.com/surveillance-cities*
An interactive and global CCTV camera density map, created by the private cybersecurity company Surfshark, based in the Netherlands.

Researchers & experts that eagerly await your call

Do you want to learn more about the digitalisation of the police and related issues? Are you in need of an expert in a particular topic? Feel free to contact the researchers and experts behind the CUPP project, listed below with their areas of expertise.

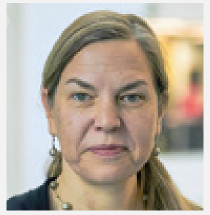


Vasilis Galis, *vgal@itu.dk*
IT University of Copenhagen, Denmark
Keywords: Big data, digital policing, data privacy, Silicon Valley, GDPR
Bio: Associate Professor in the Technologies in Practice (TIP) group at the IT University of Copenhagen. Principal Investigator of Welfare after Digitalisation (funded by the Velux foundation in Denmark) and Critical Understanding of Predictive Policing (funded by Nordforsk).
Research: Law enforcement and digitalisation of the welfare, informed by STS and qualitative methods. Galis' research is interdisciplinary and deeply oriented towards the beliefs and goals of social movements.

Anu Masso, *anu.masso@taltech.ee*
Tallinn University of Technology, Estonia
Keywords: Predictive policing, social transformations, eye-tracking, story completion, critical data studies.
Bio: Associate professor of big data in social sciences at Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology.
Research: Social consequences of the implementation of data technologies, social transformations and spatial mobilities.

Björn Karlsson, *bjrk@itu.dk*
IT University of Copenhagen, Denmark
Keywords: Big data, digital policing, data privacy, Silicon Valley, GDPR
Bio: PhD student at the IT University of Copenhagen in CUPP project where the object of his dissertation is the POL-INTEL programme of the Danish police.
Research: Björn's work draws on Science and Technology Studies, critical theory, political philosophy, epistemology, ontology, critical criminology and data studies.

Tayfun Kasapoğlu, *tayfun.kasapoglu@taltech.ee*
Tallinn University of Technology, Estonia
Keywords: Predictive policing, social morphogenesis, eye-tracking, story completion, critical data studies.
Bio: Postdoctoral researcher at Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology.
Research: Critical data studies with a focus on perspectives of data subjects that are more likely to be the targets of datafied governance procedures.



Anda Adamsone-Fiskovica, *anda.adamsone-fiskovica@bscresearch.lv*
Baltic Studies Centre, Latvia
Keywords: Surveillance, predictive policing, traffic, agency
Bio: Senior researcher at the Baltic Studies Centre in Riga, Latvia. She has an academic background in sociology and in science and technology studies.
Research: While currently specialising in social studies of agriculture and food, she also holds professional interest in innovation studies and topics related to digitalisation across various domains of modern life, including policing.

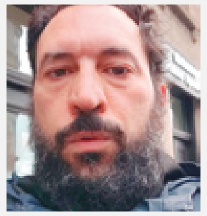
Lolita Buka, *lolita.buka@lu.lv*
University of Latvia, Latvia
Keywords: EU Artificial Intelligence Act, Fundamental Rights, remote biometric identification, predictive policing, prohibited AI practices, preventing mass surveillance
Bio: Researcher and lecturer at the University of Latvia and also a senior researcher and lawyer at the Baltic Human Rights Society. Contributor to the Human Rights Guide and Cilvektiesibas.info.
Research: Human rights and media law, with a particular focus on the implementation of these rights in the digital environment.

Emils Kilis, *emils.kilis@bscresearch.lv*
Baltic Studies Centre, Latvia
Keywords: Surveillance, predictive policing, traffic, distributed agency
Bio: Senior researcher at the Baltic Studies Centre in Riga.
Research: Social studies of science, technology and expertise.

Helene O. I. Gundhus, *h.o.i.gundhus@jus.uio.no*
University of Oslo, Norway
Keywords: Early intervention, prevention, resistance, risk assessment, accountability, youth crime
Bio: Professor and head of Department of Criminology and Sociology of Law at the University of Oslo, and Professor II at the Norwegian Police University College.
Research: Police methods and technology, police professionalism, crime prevention and security. She has also published on issues to do with risk assessments and precautionary logics, migration control and transnational policing.

Irena Barkane, *irena.barkane@lu.lv*
University of Latvia, Latvia
Keywords: EU AI Act, Fundamental Rights, remote biometric identification, predictive policing, prohibited AI practices, preventing mass surveillance
Bio: Researcher and lecturer at the Faculty of Law, University of Latvia. Former member of the UNESCO Ad Hoc Expert Group for the elaboration of the Recommendation on the Ethics of Artificial Intelligence.
Research: Artificial intelligence regulation, law and technology, EU law, human rights, data protection and privacy.

Pernille Erichsen Skjevrak, *perni@oslomet.no*
Oslo Metropolitan University, Norway
Keywords: Early intervention, prevention, resistance, risk assessment, accountability, youth crime
Bio: PhD student at the Centre for the study of Professions, Oslo Metropolitan University.
Research: Social deviations and professional actors' assessments and justifications for preventive measures. In her PhD project, Pernille aims to examine the interplay between structured assessment tools and methodologies and professional discretion in preventive policing.



Antonis Vradis,
antonis.vradis@st-andrews.ac.uk
St Andrews University, United Kingdom

Keywords: Surveillance; Facial recognition; Urban space

Bio: Faculty and Director of the Radical Urban Lab (RUL) in the School of Geography and Sustainable Development, University of St Andrews, Scotland, UK.

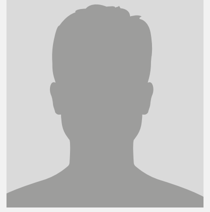
Research: The intersection of urban, policing and migration studies, with a particular focus on field-oriented work with grassroots and under-represented communities.

Evie Papada,

Keywords: Surveillance; Facial recognition; Urban space

Bio: Research and Policy Analyst at the V-Dem Institute. She holds a PhD in Human Geography (University of Loughborough, UK) and has published widely on EU asylum and immigration policies.

Research: Evie has worked in research and policy related roles, within and outside higher education, including international organisations within the broader field of human rights (UNHCR, Amnesty International, MSF).

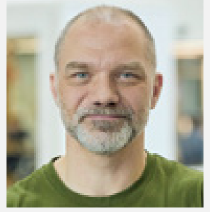


Georgios Mattes,
gm315@st-andrews.ac.uk
St Andrews University, United Kingdom

Keywords: Crime analytics; data analysis; data-driven policing; police science; genealogy; history

Bio: Research Fellow and member of the Radical Urban Lab at the University of St Andrews, in the School of Geography and Sustainable Development.

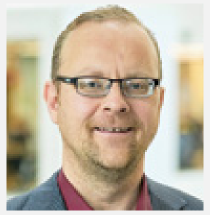
Research: Interested in the intersection of policing studies, urban studies, and the history of modern states. His research is motivated by social inequalities to offer critical explanations & understanding.



Bjarke Friborg, *bfr@prosa.dk*
PROSA - Danish Association of IT Professionals, Denmark

Keywords: Action Research, Citizen Involvement, Science Communication

Bio: Analyst/trade union organiser.



Ole Tange, *ota@prosa.dk*
PROSA - Danish Association of IT Professionals, Denmark

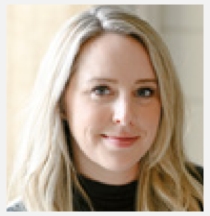
Keywords: Technopolitics, Privacy, Digitalisation in Practice

Bio: IT political advisor, IT developer.

Nicolai Scharling, *nis@prosa.dk*
PROSA - Danish Association of IT Professionals, Denmark

Keywords: Journalism, communications, criminology, IT, tech, society

Bio: Editor in Chief of the PROSA magazine, former editor in chief and head of communications in the Danish Police Union. Journalist and criminologist.



Sarah Brayne, *sbrayne@stanford.edu*
Associate Professor of Sociology at Stanford University, US.

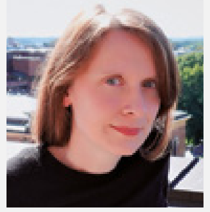
Keywords: Criminal justice surveillance, police, prisons, big data, bias, inequality, privacy, algorithms, predictive policing

Bio: Author of Predict and Surveil: Data, Discretion, and the Future of Policing. Keynote speaker at the January 2024 CUPP conference at the IT University of Copenhagen.

Simon Egbert,
simon.egbert@uni-bielefeld.de
Postdoc researcher at Faculty of Postdoc researcher at Faculty of Sociology of Bielefeld University, Germany.

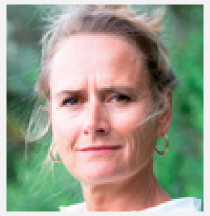
Keywords: Crime forecasts, predictive policing, crime prediction software, public order, algorithmic analysis

Bio: Co-author of Criminal Futures: Predictive Policing and Everyday Police Work. Keynote speaker at the January 2024 CUPP conference at the IT University of Copenhagen.



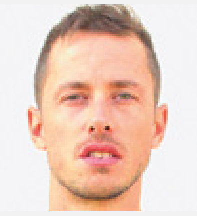
Mareile Kaufmann,
mareile.kaufmann@jus.uio.no
Professor at the Department of Criminology and Sociology of Law, University of Oslo.

Keywords: Digital Criminology, dataveillance, Science and Technology Studies, genetics & DNA, Forensics & police work
CUPP advisory board member.



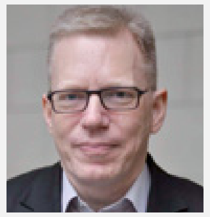
Anna Lundberg
anna.lundberg@soclaw.lu.se
Professor, Head of department, Department of Sociology of Law, University of Lund, member of CUPP advisory board.

Keywords: Discrimination, migration, sociology of law, legal cultures, human rights, rule of law.



Félix Tréguer,
felix.treguer@sciencespo.fr
Associate researcher at the CNRS Center for Internet & Society

Keywords: France, police, action-research, intelligence, oversight, predictive policing, algorithmic videosurveillance, advocacy, human rights. Speaker at the CUPP conference at the January 2024 IT University of Copenhagen.



Jesper Lund, *jesper@itpol.dk*
Chairman of the Danish EDRi member IT-Pol.

Keywords: EU policy areas focusing on data retention, ePrivacy, predictive policing, biometrics and encryption. Speaker at the CUPP conference at the January 2024 IT University of Copenhagen.

Digital police tech companies to look out for

Several private companies have become key suppliers of software and hardware for police use. Some are more controversial than others, however, operating without much public transparency while dealing with matters of public interest and security.

Palantir Technologies: Founded in 2003 in the US by Peter Thiel, co-founder of PayPal. The company develops and supplies the flagship Palantir **Gotham** software platform, an intelligence tool used by police, military, and counter-terrorism analysts in various countries.

Controversies: Criticised for enabling mass surveillance, potentially infringing on civil liberties and leading to over-policing, especially in minority communities. In 2017, Palantir faced backlash in the US for aiding the Trump administration in tracking and deporting immigrants. In 2020 and 2023, the company sparked controversy over transparency concerns when it secured contracts with the British National Health Service, granting a commercial provider of police technologies unprecedented access to citizen's health data. Its owner Peter Thiel remains a polarising figure due to his prominent political involvement.

NSO Group: Founded in 2010 in Israel. A cyber-intelligence company best known for its Pegasus spyware that can be secretly installed on a smartphone without the owner's knowledge or action. Once installed, the software allows full external control of the device, including access to messages from encrypted apps like WhatsApp and Signal.

Controversies: In 2021 an international investigation group revealed that NSO's **Pegasus** software had been used in several countries – including Spain, Poland and Hungary in the EU – to spy on journalists as well as lawyers, political dissidents, and human rights activists. The software was also linked to the murder of the journalist Jamal Khashoggi. Blacklisted in the US since 2021 for selling spyware to repressive regimes.

ClearView AI: Founded in 2017, US. Provides facial recognition software that matches photos with a database of 30+ billion images scraped from the Internet, including social media platforms.

Controversies: The company has been fined by data protection agencies in several EU countries for violating privacy laws by using images without consent. Critics have also raised concerns about potential wrongful arrests and biased targeting due to accuracy issues in its facial recognition technology. A 2020 data breach heightened concerns about data security. Since a lawsuit the same year, the company only accepts clients engaged in criminal law enforcement or national security. The company is currently banned in six US states and has officially halted operations in the EU, UK, Australia, and Canada.

Cytrox: Founded in 2017 in North Macedonia. Specialises in cyberattacks and covert surveillance. Known for its **Predator** spyware, which functions almost similarly to NSO's Pegasus but is more persistent, capable of surviving actions such as a reboot.

Controversies: In 2022 it was revealed that Predator had been deployed against politicians such as the president of the European Parliament and a Greek MEP, as well as a Greek journalist. In 2023 an international investigation group claimed that Predator was in use in several countries and had been used to target journalists, activists, and political opponents, raising serious concerns about freedom of expression and human rights abuses. Known Predator buyers include EU countries Austria and Germany.

Intellexa Consortium: A complex international web of companies either fully or partly controlled by Israeli businessman Tal Dilian. Formed in 2019. Develops and sells surveillance products.

Controversies: As a constantly evolving alliance, it incorporates core technologies such as Cytrox' Predator spyware service, WS WiSpear Systems Limited's Wifi-intercept and password-extraction technology, and Senpai Technologies Ltd's data exploitation and open-source research tools. Promotes itself as "EU based and regulated" but faces criticism for exploiting loopholes and inconsistent regulations.

The CUPP project: Activities and focus areas

- Studies of six specific digitalisation projects
- Citizen seminars with in-depth discussions
- Production of numerous articles, available on cuppresearch.info
- An international conference jointly for researchers and practitioners
- External participation in conferences, science festivals and public discussions
- Discussions and panels on academic outreach and citizen involvement

Denmark: The case of POL-INTEL

INSTITUTION: IT University of Copenhagen
RESEARCHERS: Vasilis Galis, Björn Karlsson
FOCUS: The reasoning behind the implementation of a centralised search engine across police databases, procured from the controversial tech company Palantir.
FINDINGS: Initially hailed as a 'super weapon,' POL-INTEL is now referred to as a routine tool and basic search engine for the police. Although it has accelerated police analyses, its structure relies on embedded decisions made by private actors and the police itself, rather than an objective or scientific framework. The case study reveals a lack of political debate, transparency, and understanding of the software's technical aspects among politicians, highlighting a significant democratic deficit in the procurement and implementation of such complex systems.

Sweden: The case of STATUS

INSTITUTION: St. Andrews University
RESEARCHERS: Georgios Mattes, Antonis Vradis
FOCUS: The reasoning behind the implementation of a centralised search engine across police databases, developed jointly by the Swedish company Qlik and the national police authorities.
FINDINGS: As police increasingly accumulate and centralise data, STATUS is becoming a pivotal hub of citizens' information. This raises concerns about biased policing practices and over fundamental rights like privacy, non-discrimination, and due process. The study also highlight the lack of public debate about STATUS as well as continued technical and legal issues over its use. Effectively, it is still not used for prediction, but rather as a vast data base.

Latvia: Controlling road traffic with digital tools

INSTITUTION: Baltic Studies Centre and University of Latvia
RESEARCHERS: Anda Adamsone-Fiskovica, Emils Kilis, Irena Barkane, Lolita Buka
FOCUS: Social and legal ramifications of digital technologies within road traffic control and surveillance
FINDINGS: New digital police tools such as speed cameras, drones, and mobile apps are changing how traffic is managed and enforced. While meant to improve prevention of accidents, the punishment aspect may not actually help change drivers' behaviour. Additionally, the increasing use of these tools could lead to them being used for purposes beyond their original intent (function creep), raising concerns about basic rights and data protection.

Estonia: Digitalised border control, e-residency and genetic profiling

INSTITUTION: Tallinn University of Technology
RESEARCHERS: Anu Masso, Tayfun Kasapoglu
FOCUS: Three cases are explored as technologies that are not neutral but have embedded ideals, norms and expectations.
FINDINGS: The three systems primarily target vulnerable groups, heightening control and suspicion toward them. This has deepened existing inequalities, yet the increased surveillance has quickly become normalised and is seen by many as fair. The study also shows that how technologies are presented strongly impacts public opinion, often overriding existing reservations. In conclusion, transparency and critical discussion are crucial to highlight how new digital tools can contribute to criminalising certain parts of the population.

→

The CUPP project: Activities and focus areas

Norway: Forecasting future crimes

INSTITUTIONS: University of Oslo, Norway – Oslo Metropolitan University
RESEARCHERS: Helene O. I. Gundhus, Pernille E. Skjevrak
FOCUS: Professional implications of an increased digital framing of police work, specifically in relation to juvenile crime prevention.
FINDINGS: Digital tools are built on certain assumptions and can shape police work. The officers in question, however, still prioritised their professional judgment over software-generated probabilities. Traditional theories, such as the social causes of juvenile delinquency and how police intervention can reinforce stigma, remain significant. Additionally, the country's police faced internal conflicts regarding the Palantir platform Omnia, which struggled to integrate with existing systems. Overall, the adoption of digital policing technologies in Norway has been slower due to a preference for gradual change and preserving public trust.

United Kingdom: Digitalisation of Policing and Urban Public Space

INSTITUTION: St. Andrews University
RESEARCHERS: Evie Papada, Antonis Vradis
FOCUS: The impact of the use of Facial Recognition Technologies (FRT) by the UK Metropolitan Police on Urban Public Space.
FINDINGS: The UK has a long history of surveillance programmes, with facial recognition technology (FRT) for law enforcement being one of the most controversial. Often it perpetuates and even worsens long-standing historical discriminations. The study found that police officers themselves are split as to the benefits and efficiency, given the significant high rates of mismatches. Meanwhile, the researchers also found a high level of sophistication and knowledge in parts of the public regarding the uses and pitfalls of the technology.

A POLICE TRANSFORMATION IN THE MAKING

The rapid evolution of artificial intelligence (AI) and tools such as machine learning, data mining and data analytics also means an expanded toolbox for law enforcement.

The new tools are not simply additional, however, but also create new relations between citizens and the state, new forms of law enforcement, and raise several new issues and concerns, notably in times of persisting social inequality and societal change.

In this catalogue, we will explore the implications of these tools as identified by the CUPP research team – Critical Understanding of Predictive Policing. The aim here is not to provide an exhaustive analysis. Rather we want to assist more people – including journalists, politicians, victims, human rights activists, institutions, organisations, and citizens – in understanding, discussing, and engaging with these important issues.

OPENING THE 'BLACK BOX'

Data scientists and social scientists are only just beginning to explore how data-driven technologies affect crime prediction, prevention, solving, and the relationship between the police and the public. It is a new and developing field, and there is still much to learn.

During the CUPP project (2021-2025), one key idea, ”predictive policing", has already shifted from being popular to being banned by the EU AI Act from 2024 when it comes to individuals – although with some exceptions. This shows that technology is not neutral; different groups, like big tech companies, governments, and citizens, often have conflicting views and interests.

The CUPP project aims to increase transparency and encourage public discussion about new data-driven police practices. Our focus is to open the 'black box' that reveal what happens behind the scenes when law enforcement becomes digital. This includes questions ranging from how technology is bought and developed to how it is used, covering areas like digital traffic control, crime prediction, urban surveillance, and database integration. The goal is to make police authorities more accountable for their actions.