

1 PREFACE

Lene Wacher Lentz, Litska Strikwerda, and Jurjen Jansen

1.1 TECHNOLOGY ON THE GLOBAL STAGE

As new digital technologies emerge, their vast potential unfolds – both for commercial purposes and for use in law enforcement. At the same time, it is becoming increasingly clear that their application also entails significant risks. How do these technologies operate? What kinds of data do they rely on? Are they trustworthy or biased? Do they threaten privacy and fundamental rights?

Innovation, law, and ethics must work hand in hand, as democratic societies define both the uses and the limits of these technologies. In this regard, the European Union has taken a proactive role by enacting the AI Act, addressing concerns about artificial intelligence and adopting a strict regulatory approach.¹ Yet it is equally important to remember that the EU is also influenced by political trends and pressures: rights that were once hard-won may again be called into question.

In the fight against the sexual abuse and exploitation of minors, the European Commission has previously advanced a controversial proposal: the Child Sexual Abuse (CSA) Regulation, often referred to as ‘Chat Control’.² The initiative would oblige communication service providers to scan private messages for child sexual abuse material and share relevant information with law enforcement authorities.

As noted in the Policing in the Digital Society Network Yearbook 2025, the proposal was removed from the EU Council’s agenda in 2024.³ However, with the Danish government assuming the EU Presidency from 1 July to 31 December 2025, and with a clear focus on preventing and combating the sexual abuse and exploitation of children, the CSA Regulation re-emerged on the political agenda.⁴ Once again, critics mobilised, emphasising the need to defend fundamental rights such as privacy and freedom of

1 Artificial Intelligence Act (Regulation (EU) 2024/1689).

2 2022/0155 (COD).

3 Lentz and Naarttijärvi (2025), p. 13.

4 Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Presidency compromise texts, 1 July 2025, <https://data.consilium.europa.eu/doc/document/ST-10131-2025-INIT/en/pdf>; Danish EU Presidency, ‘A strong Europe in a changing world: July 1 – December 31, 2025, p. 24, <https://danish-presidency.consilium.europa.eu/media/xv5jn5nx/programme-of-the-danish-eu-presidency-2025.pdf>.

expression.⁵ With Germany allegedly seen as the decisive opponent of the proposal, it was once again taken off the table – but for how long?

When crime occurs in new forms, such as on digital platforms, and law enforcement agencies lack the investigative tools to address these emerging challenges, there is a risk that the police will be perceived as ineffective or powerless. A simplistic response – relying on increased control and surveillance – risks undermining the democratic values and fundamental rights upon which our societies are built. A more nuanced and balanced approach is therefore needed.

The CSA initiative poses a challenge not only to the fundamental rights of EU citizens, but also to the commercial digital infrastructure. Companies have a vested interest in developing and distributing robust technical solutions for communication – a principle recognised by EU legislation, particularly the General Data Protection Regulation (GDPR), which mandates privacy by design and privacy by default.⁶ These requirements oblige companies to integrate privacy considerations at every stage of technological development.

Assisting law enforcement agencies by providing backdoors into encrypted communications runs counter to these interests. There is a significant risk of misuse: for now, we may trust European law enforcement to exercise such powers responsibly and only to the extent that is strictly necessary. At the same time, it is easy to envisage contexts in other states where the risk of abuse is real. Commercial digital infrastructures are playing an increasingly prominent role in international affairs and politics, with Elon Musk's Starlink in Ukraine serving as a notable example. At the same time, these companies risk being caught in the midst of international conflicts. For instance, following Trump's sanctions on the International Criminal Court, Microsoft reportedly deactivated the email account of the Court's chief prosecutor.⁷

Addressing these complex challenges requires more than technological solutions or regulatory measures alone. It demands a societal debate in which the difficult dilemmas are openly discussed, and where the perspectives of researchers, practitioners, and policymakers are actively integrated. By bringing together rigorous research, practical experience, and policy expertise, we can better understand the implications of new

5 Cointelegraph, 'EU's Chat Control law would push users toward "Web3 alternatives" – Experts', 21 September 2025, <https://cointelegraph.com/news/eu-chat-control-privacy-warning-web3-shift>.

6 Regulation (EU) 2016/679 of 27 April 2016.

7 EU Parliamentary question, 'The effect of the sanctions imposed by the United States on the functioning of the ICC', 5 June 2025 (P-002270/2025) https://www.europarl.europa.eu/doceo/document/P-10-2025-002270_EN.html; see also media coverage: AP, 'Trump's sanctions on ICC prosecutor have halted Tribunal's work', 15 May 2025, <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>; LBC News, 'British ICC chief prosecutor lost access to email and has bank accounts frozen after Trump's sanctions on top court', 15 May 2025, https://www.lbc.co.uk/article/british-icc-chief-prosecutor-lost-email-bank-accounts-frozen-trump-sanctions-rpTkm_2/.

technologies, safeguard fundamental rights, and navigate the trade-offs between security, privacy, and innovation.

Equally important is the creation of networks and collaborative platforms where practitioners and scholars can meet, exchange knowledge, and jointly develop solutions to these pressing issues. Such collaboration not only enriches our understanding but also ensures that responses are grounded in both theory and practice, fostering approaches that are effective, ethical, and socially legitimate.

1.2 POLICING IN THE DIGITAL SOCIETY NETWORK

In an era where digital technologies permeate every aspect of social life, the Policing in the Digital Society Network stands as a vital interdisciplinary initiative that explores the evolving relationship between policing and digital transformation. Based in Scandinavia, the United Kingdom, and the Netherlands but internationally oriented, the network brings together scholars, practitioners, and students from diverse fields – police studies, criminology, law, sociology, computer science, communication studies, and public administration – to critically examine how digitalisation reshapes the practices, ethics, and governance of policing.

The network's mission is not only to understand the implications of digital tools – such as predictive analytics, body-worn cameras, and social media surveillance – but also to foster dialogue about their societal impact. What does it mean for police to be 'present' online? How do digital platforms influence trust, legitimacy, and proximity between law enforcement and communities? These are the kinds of questions that animate the network's research agenda.

Through conferences, collaborative research projects, and public engagement, the network cultivates a space where theoretical inquiry meets practical relevance. It encourages reflexivity among police professionals and offers students a unique opportunity to engage with cutting-edge debates on digital policing. The network also contributes to policy development by offering evidence-based insights into the opportunities and challenges posed by digital technologies in law enforcement.

In a time when digitalisation is both a promise and a peril, the Policing in the Digital Society Network provides a crucial platform for critical reflection, innovation, and responsible governance. It invites all who are interested in the future of policing to join the conversation. This volume features a selection of contributions from the 2025 conference, held at Northumbria University in Newcastle upon Tyne (20–22 January), showcasing the breadth and depth of ongoing research within the network – covering a wide array of themes related to policing in an increasingly digitised society.

Over the course of three dynamic days, the conference brought together up to 100 participants for an engaging programme filled with thought-provoking keynotes and a diverse range of presentations organised across four thematic tracks: (1) developing

new technological capabilities in a police setting; (2) new technological capabilities and data use in policing and criminal justice; (3) criminal procedure and digital policing; and (4) technological capabilities, the police, and the public. The event fostered lively discussions and meaningful exchanges, creating a fertile ground for networking and sparking new collaborations that promise to shape future research and practice in the field of digital policing.

This was the second annual conference in its current form (see also Lentz & Naarttijärvi, 2025 for a brief history of the network). During the conference, the heads of departments from the collaborating knowledge institutions – who together installed the PDS steering group – signed a letter of understanding to formalise and secure the partnership. The network subsequently began preparations for the next European Conference on Policing in a Digital Society, held on 13-15 January 2026 in Oslo, Norway.

1.3 OPPORTUNITIES AND CHALLENGES LAW ENFORCEMENT FACES IN THE DIGITAL AGE

The field of policing is undergoing drastic changes due to the rapid development of digital technologies. This book brings together five chapters that explore various opportunities and challenges law enforcement is facing in the digital age. From the use of artificial intelligence transcription tools in investigative interviews to the ethical dilemmas posed by new surveillance mandates, the authors offer a critical and timely examination of how digital tools are reshaping the practice, culture, and governance of policing.

All chapters went through a double-blind peer review procedure. Every submission was first reviewed by two members of the editorial board and – in most cases – subsequently reviewed by two academic experts on the field in question, from two different countries other than the author's home country. About half of the submissions led to a chapter in this yearbook. The editors would like to express their gratitude to all the (anonymous) external reviewers and want to thank the authors for their patience during the reviewing process and their enthusiasm during the phase of finalising their chapters.

At the heart of this volume lies a shared concern: how can law enforcement utilise technological innovation while safeguarding important rights and values, such as fair trial, transparency, accountability, privacy, and human dignity? Each chapter addresses this question from a distinct perspective, drawing on empirical research, legal analysis, sociological analysis, and practitioner insights to illuminate the tensions and possibilities inherent in digital policing.

Chapters 2 and 3 are about the specific opportunities and challenges presented by two particular AI tools in digital policing. Chapter 2, written by Thomas Beka, Kyle Porter, and Bente Skattør, investigates the use of local and open-source speech-to-text technologies in transcribing investigative interviews in the Norwegian jurisdiction.

While AI transcription tools promise efficiency and accessibility, this study reveals that the application of these systems in sensitive contexts, such as interviews with children or vulnerable individuals, poses challenges. These findings underscore the importance of human oversight and contextual judgement, which are also emphasised by the EU's AI Act, and remind us that technological solutions must be critically evaluated within the realities of police work.

In the third chapter, Harm van Beek and Hans Henseler explore how large language models (LLMs) can serve as investigative copilots within forensic environments. With exploratory experiments conducted on the Hansken platform, they demonstrate that LLMs can assist investigators through semantic multilingual search, correlating disparate pieces of evidence, and producing logically structured analyses. Although the authors think LLMs can help to manage the exponential growth and complexity of digital evidence, they also caution against the risks of AI hallucinations and opaque decision-making. They therefore call for robust safeguards to ensure transparency and accountability in forensic processes.

The fourth chapter focuses on human-centred digital transformation in policing with a study of the concept of digital literacy in the context of the investigation of online CSA. In this chapter, Alva Lindholm studies how digital literacy is understood within online CSA investigations and how it is applied in practical, day-to-day work in this specific investigative context. Through interviews and observations with Swedish online CSA investigators, the study reveals that digital literacy is not merely a technical skill but a dynamic, context-dependent set of competencies. Emotional resilience, a common professional language, and trust in technology are important, in addition to technical proficiency. This chapter challenges the notion that training alone can increase digital literacy, advocating instead for a more holistic and practice-oriented approach.

The last two chapters are about ethical and legal tensions in digital police work. In the fifth chapter, Marie Eneman examines the legitimacy of three new surveillance mandates in Swedish policing: Secret Data Reading, Forensic DNA Genealogy, and Facial Recognition in Real-Time. Drawing on interviews with institutional actors, the study uncovers the narratives of necessity and protection that underpin these powers, as well as the democratic tensions they provoke. The chapter argues that policing is undergoing an epistemological shift – from evidence-based investigation to probabilistic approximation – that poses profound challenges for the rule of law and civil liberties. Ultimately, this reveals a democratic paradox where the very technologies introduced to safeguard society risk eroding the rights and freedoms they are meant to protect.

Finally, in the sixth chapter Lene Wachter Lentz delves into the legal standards governing encrypted communication evidence in criminal trials, as established by the European Court of Human Rights to ensure a fair trial under Article 6 of the European Convention on Human Rights. The chapter focuses on the use of messaging data from the communication platform EncroChat in Danish criminal proceedings.