1 Preface

Lene Wacher Lentz and Markus Naarttijärvi

1.1 Dilemmas in new technologies for combating crime

Law enforcement agencies, privacy organisations and many others had their eyes set on the EU Council meeting on 20 June 2024, where a controversial proposal was meant to be discussed: the Child Sexual Abuse (CSA) Regulation. The aim of the proposal, presented two years earlier on 11 May 2022 by the European Commission, was to make it mandatory for communication service providers to scan private communications for child sexual abuse material and make the information available to law enforcement authorities.[1]

The proposal, also referred to as the EU 'Chat Control', was presented with the aim of combating crimes related to sexual violence against children.[2] However, the proposal has been heavily criticised, for example by privacy organisations, for subjecting EU citizens to mass surveillance, thus jeopardising the fundamental right to private communication.[3] As the obligation would also extend to providers of end-to-end encryption, an intense technical debate emerged, specifically on how the providers could 'moderate the upload' without breaking the end-to-end encryption.[4]

Shortly before the EU Council meeting on 20 June 2024, the proposal was taken off the agenda, apparently because no agreement on it had been reached.[5] There is so far no date for a new discussion of the proposal.

The initiative illustrates a profound challenge in balancing the new technological possibilities for law enforcement agencies in the investigation of crimes, and the implications for fundamental human rights. It also demonstrates an important challenge regarding how much power must be handed to law enforcement agencies for preventive measures, meaning before anyone has committed a crime, rather than

1 2022/0155(COD).
2 2022/0155(COD), Explanatory Memorandum, Section 1, Context of the Proposal.
3 EDRi and 47 civil society organisations: 'Joint statement on the future of the CSA Regulation', 1 July 2024, calling for the proposal to be withdrawn, https://edri.org/our-work/joint-statement-on-the-future-of-the-csa-regulation/.
4 E.g. statement from Meredith Walker, President of the communication network Signal: 'New Branding, Same Scanning: "Upload Moderation" Undermines End-to-End Encryption', 17 June 2024, https://signal.org/blog/pdfs/upload-moderation.pdf.
5 Clothilde Goujard, Politico: 'EU cancels vote on child sexual abuse law amid encryption concerns', 20 June 2024, https://www.politico.eu/article/eu-council-cancels-vote-on-encryption-breaking-child-sexual-abuse-law/.

reacting to crimes already committed. Naturally, law enforcement agencies have an interest in gaining as much knowledge as possible, thus enabling them to intervene as early as possible, before or when a crime is committed. From a citizen's perspective, the state's surveillance and interference are only justified if one actually does something wrong; only a reasonable suspicion can justify interference.

From a privacy perspective, it has been argued that tools for scanning communication would make all communication liable to interference, and for example catch teenagers consensually sending nudes to each other.[6] It has also been pointed out that the fight against child sexual abuse material is only the beginning for these tools; once the technology for messaging and chat control has been established, it becomes very easy to use them for other purposes.[7]

From a legislative point of view, crucial implications are at stake when EU law is used to combat crimes. Considering the law enforcement perspective, crimes against children involving abusive material are often found online and have cross-border aspects. The EU countries would benefit from cooperation on these matters. The harmonisation would ensure that all communication service providers in the EU are subject to the same obligation, although it has been argued that a mandatory scan would not effectively combat these crimes, as the perpetrators organise in self-run forums and the law enforcement agencies would be flooded with automatically generated information, most of which will be irrelevant.[8] It is also important to note that the CSA initiative is a proposal for an EU regulation, which would be directly applicable in each Member State. The legislative tool is therefore particularly strong, since it cannot vary from member state to member state.

While the proposal was presented by the EU Commission, the EU Court of Justice has elsewhere made a particularly strong stand on privacy in relation to data retention of call data records. The EU Data Retention Directive of 2006[9] aimed to harmonise data retention across the EU countries, for the benefit of law enforcement agencies in combating serious crimes, but it was annulled by the EU Court of Justice with the judgment in the joint cases of *Digital Rights Ireland* and *Kärntner Landesregierung* in

6 Electronic Frontier Foundation: 'Now The EU Council Should Finally Understand: No One Wants "Chat Control"', 1 July 2024, https://www.eff.org/deeplinks/2024/06/now-eu-council-should-finally-understand-no-one-wants-chat-control.

7 Patrick Breyer, German Member of the European Parliament: 'Chat Control: The EU's CSEM scanner proposal', blogpost (last visited 13 July 2024), https://www.patrick-breyer.de/en/posts/chat-control/#how-does-this-affect-you

8 Patrick Breyer, blogpost, https://www.patrick-breyer.de/en/posts/chat-control/#how-does-this-affect-you.

9 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

2014.[10] The CJEU's case law over the years on these matters has always related to the traffic data of the communication, not the content of the communication. The court noted in the *Tele2 Sweden* judgment that the Swedish legislation provided for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.[11] Furthermore, the Court stated:

> That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[12]

If – or when – the proposal for a CSA Regulation emerges for consideration in the EU Council, it will face strong debate again, as fundamental considerations are at stake. Ultimately, such a regulation would also have to deal with the CJEU's strong stance on privacy in communication.

The EU proposal for the service providers to scan communications for CSA illustrates some of the fundamental considerations at stake: the investigation of crime versus privacy; the never-ending drive of new technology; whether the role of the police is to react or prevent; how to design new technology to take into consideration privacy and avoid mass surveillance; and the role of national law, the EU and international organisations, such as the Council of Europe and the European Human Rights Convention. Continuous research on these matters is needed to ensure the right balance; it must also be interdisciplinary, so that the legal framework intended matches the technology and aligns with the ethical boundaries.

These topics are core interests of the dedicated researchers within the Policing in the Digital Society Network.

---

10 CJEU, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof.

11 CJEU, 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, para. 97.

12 *Tele2*, para. 99. The CJEU's approach on these matters has been developed in subsequent judgments, e.g. in 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*.

1.2 A brief history of the Policing in the Digital Society Network

The Policing in the Digital Society Network and its associated conference emerged from the merger of two groups: the Nordic Cybercrime Conference and the PDTor research project. Both groups consisted of researchers in the fields of policing and criminal law, focusing on new technologies and the possibilities and challenges they present. In 2023, on the initiative of Wouter Stol and Inger Marie Sunde, initial meetings were held to discuss setting up a European network and annual conference. We saw the benefit of enhancing collaboration and reaching out to a broader community, thereby adding new perspectives to our research and fostering new relationships.

The Nordic Cybercrime Conference, initiated by the Law Department at Aalborg University, was first held in 2017. This gathering of researchers and practitioners from law enforcement authorities proved very promising, with participants expressing a strong desire to continue the event and the associated cooperation and network. Since then, the conference has also been hosted by the Norwegian Police University College and Umeå University. It has expanded its focus from specific provisions related to cybercrime and criminal procedure to broader topics like policing, big data, surveillance and related legal issues.

The PDTor research project (2017-2022) was formed by researchers from the Netherlands, the United Kingdom, Sweden and Norway, supported by a NordForsk research grant. The project explored the tension between citizens'' privacy (Tor users) and state power (police on the Tor network) in crime prevention and investigation. The project's core idea was to compare daily police work with the demands of forensic correctness and legal fairness. The results aim to assist police in modern crime-fighting and provide accountability and fresh insights to the academic community on technology-based policing, human rights and enforcing laws on anonymous communication networks.

The new network that was formed on the basis of the two above-mentioned networks held its first European conference on 15-17 November 2023, at the Dutch Police Academy in Apeldoorn. The three-day event featured inspiring keynotes and a packed programme of exciting presentations divided into four tracks: (1) Our Digital Society and Its Police; (2) Everyday Policing and Digital Technologies; (3) Predictive Policing and AI; and (4) Digital Evidence. With up to 100 participants, the conference facilitated fruitful discussions and networking, leading to important new contacts and promising future collaborations. We received very enthusiastic feedback, reinforcing our desire to continue this network and cooperation. The network is currently organising the next European Conference on Policing in the Digital Society, scheduled for January 2025 in Newcastle.

Based on abstracts from distinguished researchers in the field of digital policing, this volume was created through a writing and review process conducted in 2024. With this

edited volume, our network's website (www.policinginthedigital.org), the additional newsletter and the conference, we are very pleased with the network's achievements and progress thus far.

1.3 The wide scope of digital policing

The development of the network we have described so far illustrates an important point about digital policing. It is an area that has long existed at the intersection of different academic disciplines. Even within a single discipline, such as legal science, digital policing can intersect intradisciplinary boundaries between constitutional law, criminal law, procedural law, administrative law, data protection law, etc. Research questions relating to digital policing routinely flow between and through these different areas. In a similar vein, our conferences have illustrated how a commonly discussed topic, such the use of algorithms for predictions or recommendations in policing, can bring together researchers from sociology, policing studies, management, law, political science and more – each with their own unique insights and perspectives, and each contributing to a fruitful exchange where everyone leaves the conference a little wiser and a little more mindful of the complexities we face.

These disciplinary exchanges and accompanying insights are valuable in their own right. As legal researchers – traditionally less empirically driven – we can, through these exchanges, identify fresh issues ripe for legal analysis that might have remained invisible to us otherwise. As researchers of policing practices, we can recognise the impact of those practices on victims, or on legal procedures, fundamental rights, the efficiency or effectiveness of policing, or wider societal values. Listening to practitioners, we can learn where the frontlines of digital policing are, what problems they face and the solutions they have found. Meanwhile the practitioners can draw from a wellspring of research-based insights into what works, what does not, and where the possible red lines are.

While these exchanges are important in their own right, they also speak to the vast potential for interdisciplinary and transdisciplinary approaches to digital policing. We have over the years been able to see the important insights such approaches can bring, through presentations of interdisciplinary projects at our yearly conference. But we can also see the seeds of new collaborations grow in the intense discussions and conversations taking place during the coffee breaks and conference dinners, discussions where interdisciplinary exchanges happen organically and spontaneously, and have led to articles, research applications, seminars and more, that might never have happened otherwise.

As a network organised not around a discipline, or a method, but around a societal issue and a practice, the PDS Network is not only a place where such collaborations can begin. The network is in itself a pool of diverse competences and experiences, insights