“Should everyone have access to AI? " Perspectives on Ownership of AI tools for Security.

EZZEDDINE, Yasmine <http://orcid.org/0000-0002-2810-2231> and BAYERL, Petra <http://orcid.org/0000-0001-6113-9688>

“Should Everyone Have Access to AI? " Perspectives on Ownership of AI Tools for Security

Yasmine Ezzeddine and Petra Saskia Bayerl
Sheffield Hallam University, Sheffield, UK

y.ezzeddine@shu.ac.uk
p.s.bayerl@shu.ac.uk

Abstract: Given the widespread concerns about the integration of Artificial Intelligence (AI) tools into security and law enforcement, it is natural for digital governance to strive for greater inclusivity in both practice and design (Chohan and Hu, 2020). This inclusivity can manifest in several ways, such as advocating for legal frameworks and algorithmic governance (Schuilenburg and Peeters, 2020), allowing individuals choice, and addressing unintended consequences in extensive data management (Peeters and Widlak, 2018). An under-reflected aspect is the question of ownership, i.e., who should be able to possess and deploy AI tools for law enforcement purposes. Our interview findings from 111 participants across seven countries identified five citizens viewpoints with respect to AI ownership of security-related AI: (1) Police and police-governed agencies; (2) Citizens who disassociate themselves; (3) Entities other than the police; (4) All citizens including themselves; and (5) No one or Unsure. The five clusters represent disparate perspectives on who should be responsible for AI technologies, as well as related concerns about data ownership and expertise, and thus link into broader discussions on responsibility for security, i.e., what deserves protection, how and by whom. The findings contribute theoretically to digitalization, smart technology, social inclusion, and security studies. Additionally, it seeks to influence policy by advocating for AI development that addresses citizen concerns, thereby mitigating risks, social, and ethical implications associated with AI. Crucially, it aims to highlight citizens’ concerns around the potential for malicious actors to exploit ownership of such powerful technology for harmful purposes.

Keywords: Artificial intelligence, Ownership, Citizens, Law enforcement agencies, Police

1. Introduction

In the domain of security and policing, the integration of Artificial Intelligence (AI) tools presents both unprecedented opportunities and ethical considerations. At the crux of these advancements lies a pivotal question: who should hold ownership of these AI tools, and thus who owns the responsibility for security?

Expanding the definition of AI is crucial, considering recent entries defining AI as "systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals" (European Commission, 2020). With AI tools rapidly expanding across society, including in the security and policing domain, digital governments are seeking more inclusive dynamics in practice and design to ally valid citizen concerns (Chohan and Hu, 2020). This inclusivity can manifest in various ways, from calls for dedicated legal frameworks to algorithmic governance and better accounting for unintended consequences in large data management (Schuilenburg and Peeters, 2020; Peeters and Widlak, 2018).

An underexplored aspect in this regard is AI ownership. Generally, AI in the security and policing domain is conceptualised as police-owned capability. However, the ongoing privatisation and personalisation of security (for instance privately owned door cameras with AI capabilities) opens the field to a much more fluid landscape of ownership. This study explores the perceptions and preferences of citizens regarding the ownership of AI tools, particularly in policing and law enforcement contexts. Understanding public stances on this matter is crucial, as they reflect societal values on societal understandings about responsibilities for security (Bayerl et al., 2022) and can therefore contribute to shaping policies governing AI deployment and ownership.

In the realm of AI and societal implications, the discourse on ownership of security-related AI capabilities has been a focal point in academic and policy discussions. Numerous studies have explored AI deployment landscapes. However, these discussions often overlook citizen perspectives regarding ownership of security-related AI. While scholars and policymakers deliberate on governance models and ethical frameworks, citizen voices remain underrepresented in these discussions (Floridi and Taddeo, 2016).

Understanding citizen perspectives is pivotal for shaping inclusive, ethically sound, and socially acceptable AI deployment strategies for AI in security and policing. Citizens' concerns, and preferences play a fundamental role in determining legitimacy, trustworthiness, and societal acceptance of AI systems used by law enforcement and security agencies (Crawford and Calo, 2016). Thus, this article aims to fill the gap in existing discourse by elucidating the significance of citizen perspectives in defining the preferred ownership of AI tools

within security domains. By amplifying these insights, this study underscores the importance of inclusive governance frameworks that prioritize the amalgamation of citizen opinions, ensuring responsible and beneficial AI integration into society.

1.1 AI Ownership in Security and Policing Contexts

The deployment of AI tools within the security domain such as predictive policing algorithms (e.g., PredPol) and facial recognition systems (e.g., Clearview AI) highlight the complexities of AI ownership and showcase the intersection of technological innovation, legal frameworks, and societal implications. The discourse on AI ownership revolves around control, accountability, and responsibility for actions and decisions executed by these intelligent systems. Floridi (2019) argues that ownership extends beyond possession to include responsibility for AI actions, such as biases, errors, and ethical implications. This aligns with broader discussions on accountability and the necessity for transparency and oversight in AI deployment (Kroll et al., 2017).

The adoption of AI technologies such as automated license plate readers (ALPRs) and crime mapping tools, raises both concerns and opportunities. The potential of AI to augment law enforcement capabilities and optimize resource allocation is juxtaposed with apprehensions regarding privacy infringement, fears of biases, and the erosion of discretion in decision-making (Aloisi and Gramano, 2020; Mittelstadt et al, 2016). The ownership and deployment of these tools by police raises debates around balancing security with societal values and whether ownership should be exclusive to law enforcement or more distributed (Orwell, 2000).

1.2 Aim of This Study

This research aims to explore the perspectives of citizens regarding the preferred owner(s) of AI tools for policing and law enforcement applications. Through semi-structured interviews, this study seeks to elucidate public perceptions, concerns, and preferences concerning AI ownership, contributing to informing policy frameworks and ethical guidelines governing the deployment and ownership of AI tools in security domains. Understanding citizens' perspectives towards ownership of AI tools is crucial, especially given the legal and moral implications involved (Robaey, 2015; Hayes et al, 2020). By understanding the rationale behind citizens' viewpoints on access and ownership of AI policing capabilities, this study aims to contribute to the theoretical and social context in which security opportunities align with community needs and perspectives, leading to potential endorsement of a virtuous implementation of AI within policing.

2. Methodology

Semi-structured interviews were conducted in eight different countries (UK, Netherlands, Italy, Spain, Portugal, Czech Republic, Germany, and Greece), involving 111 participants. Participants were recruited based on specific group specifications relevant to each of the partner countries as part of the AIDA2020[1] joint project. The interviews focused on citizens' attitudes towards AI use by law enforcement agencies (LEAs), and namely ownership. Interviews were chosen as a qualitative approach to better understand and integrate citizens' perceptions towards AI ownership, following a structured theme of scenario-based interview questions. The data collected from these interviews underwent thematic and content analysis to identify main themes and patterns. Participant responses were coded and clustered into high-order categories, allowing for the emergence of common perspectives reflecting preferences for AI ownership in different contexts. This analysis, performed using NVivo's qualitative data analysis software, enabled the exploration of citizen perspectives on AI ownership, contributing to the broader discourse on AI ownership within security contexts.

2.1 Participants

Participants were recruited by researchers in the eight participating countries. The selection allowed free choice of the citizen group to allow partner countries to choose groups that they considered relevant and of interest in their national context. A total of 111 individuals participated. Germany focused on young women (18-25 years, n=16), Czech Republic (n=10) focused on young people in general between 18-25 years old, while Italy addressed older citizens (65+ years). The Netherlands focused on expatriates (n=16) with experience in the Cybersecurity field. In the UK, 11 individuals with a migration background were recruited. Spain (n=20) and Portugal (n=6) chose participants who are familiar with AI, while Greece (n=16) decided to adopt an open

[1]AIDA2020: Artificial Intelligence and Advanced Data Analytics for Law Enforcement Agencies. https://www.project-aida.eu/

selection of participants of diverse occupations and disciplines. Table 1 shows the demographic and gender distributions of the selected groups.

Table 1: Demographic characteristics of participants per country

Country	Number of Participants	Group specifications	Gender distribution Women / Men	Average age
Czech Republic (CZ)	10	Young people between 18-25 years old	60% / 40%	23.4
Germany (DE)	16	Young women between 18-25 years old	100% / 0%	26.3
Greece (GR)	16	Experts in IT Law and IP law	78.57% / 24.4%	33.25
Italy* (IT)	16	Older citizens (65+)	50% / 50%	72.8
Netherlands (NL)	16	Expatriates	43.7% / 56.2%	26.3
Portugal (PT)	6	People with limited knowledge of AI	50% / 50%	44.7
Spain (SP)	20	AI experts	40% / 60%	37.5
UK	11	Citizens with migration background	72.7% / 27.2%	33.4
Total	*111*		*62.2% / 37.8%*	*38.3*

2.2 Data Collection

A total of 111 semi-structured interviews were conducted addressing citizens' attitudes towards AI use by LEAs. While the first part of the interview focused on overall questions of acceptance and acceptance conditions, the second part offered participants the opportunity to reflect more specifically on potential ethical dilemmas of AI use and possible resistance. This paper focuses on one part of the interview, particularly the part where participants were asked about whether AI capabilities should be limited to police only, or would they want to have access to such tools themselves.

The interviews were conducted either face-to-face or online by researchers in each participating country to allow participants to react to questions in their own language. Therefore, all participating countries provided participants with the information sheet, the informed consent, and the interview guidelines in the language of the respective country, except for the Netherlands where the researchers chose to share the documents with the participants in English instead of Dutch since they interviewed expatriates. Follow-up questions, prompts and comments were made by interviewers in each country to encourage participants to elaborate on the rationales for their choices. All interviews were audio-recorded. Some were transcribed as summaries, others were transcribed verbatim, and all the data was anonymized before analysis.

2.3 Data Analysis

The transcripts and the summaries obtained in the native countries' languages were translated to English using a designated translation software which was followed by close proof-reading. The English transcripts/ summaries were used for the data analysis. Our analytic approach followed thematic (Auerbach and Silverstein, 2003) and content analysis principles (Krippendorff, 2004) for the purpose of identifying main themes and patterns in the data. First, the answers were coded in cycles, starting with open or initial coding (Charmaz, 2006), followed by clustering into high-order categories for each main topic. Thematic analysis was used to allow for the thorough evaluation of the statements made by each participant which revealed common perspectives whereby specific ownership was preferred by participants, depending on the situation, and was justified by different rationales. This coding was performed using NVivo's qualitative data analysis computer software package. As a second step, participant's responses were thoroughly reviewed, coded, and assessed for similarities, then clustered under common sub-themes. This process is largely exploratory,

whereby the analysis does not rely on any predefined categories or features in creating the clustered perspectives.

2.4 Ethics

This study has been approved by the ethics committee of the authors' affiliated university. Additionally, participants were informed of the context and legal basis of the study, the details of data handling and their rights through the information sheet and informed consent form which the participants had to sign prior to the interview. The right to withdraw and to opt out from providing demographic information was also explicitly stated in the above-mentioned forms. All data was analysed in pseudonymized form.

3. Results

3.1 Analysis of Perspectives

The approach revealed five disparate perspectives towards the preferred ownership of AI capabilities for security. Figure 1 shows the percentages of respondents who favoured each form of AI owner. Below, we provide an in-depth analysis of these responses, citing participant comments in italics to clarify their decision-making process. Each perspective is summarized with a descriptive title highlighting key aspects.

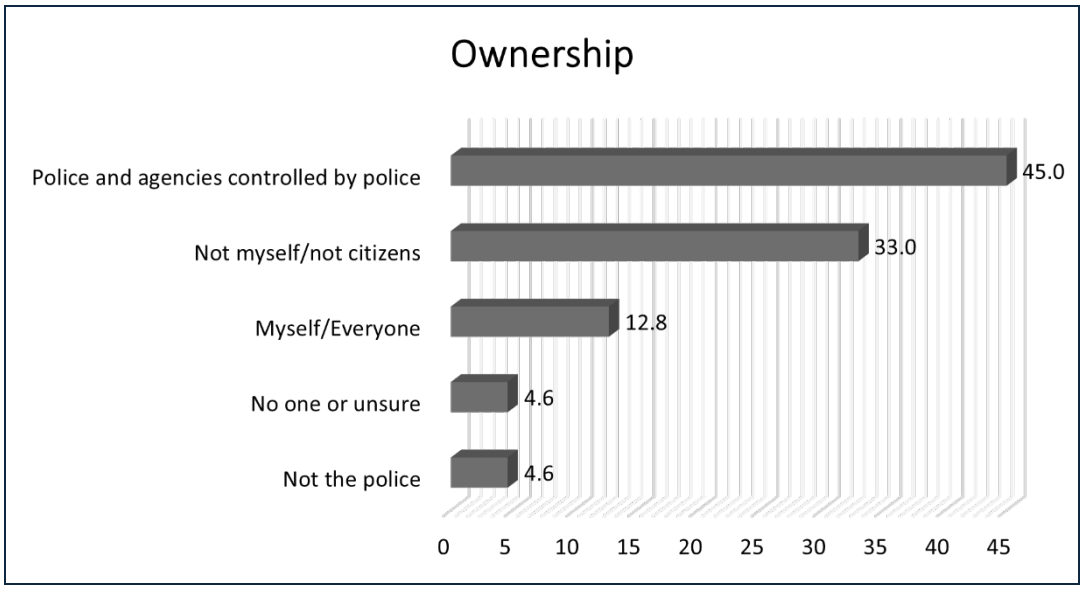

Figure 1: Clustered Perspectives on preferred owner(s) of security-related AI (in percentages of participants in the sample)

Perspective 1: Preference for Police, LEAs, and Government Agencies

This was the most common perspective, with most participants preferring LEAs/Police to own and control AI tools. They cited public safeguarding, reducing costs, and proactively preventing crimes as key reasons. The trust in LEAs stems from their established role for safeguarding society and their existing access to confidential information, coupled with their training to handle extreme cases and the biases of AI.

Participants believe that police and LEAs have the necessary skills, competence, and ethical obligations to use AI responsibly compared to private entities. Participants specifically emphasized the role of police in protecting citizens: "This must be with the police; they must protect us" (PT-05). Concerns about private entities mishandling data surpassed worries about police use of personal data, reflecting a general acceptance of the police's role in safeguarding. They trust police forces to protect private information and use AI for public safety. As NL-13 said, "I trust the police with this kind of information."

Some participants suggested extending AI ownership to other government agencies, intelligence units, independent auditors, academia, and corporations with appropriate vetting and accountability measures. Centralized authorization under LEA supervision was also suggested, reflecting the belief that protecting the population is a core police mission (PT-05).

Perspective 2: Preference against Police Ownership

A smaller number of participants opposed police ownership of AI, citing the need for broader monitoring and evaluation to ensure effective use. They doubted the police's expertise and transparency in handling AI for crime prevention. GR-12 remarked, “For police I don’t know how they will use it, and I am a bit overwhelmed knowing that.” This group thus represents an opposing view to Perspective 1. The two opposing perspectives illustrate the importance of trust in police and perceptions of competence as basis for AI ownership.

Perspective 3: Preference for no ownership by citizens (including themselves)

This perspective indicates a general rejection of AI ownership by citizens, citing their lack of qualifications to handle such tools. This included participants themselves as well as others. As IT-11 stated, “It would be a waste of time if I had some computer tools to protect myself because I wouldn't be able to handle them, honestly.”

Others felt unsafe with such information, preferring police to handle AI for protection (PT-04). Participants compared AI ownership to gun ownership, fearing misuse: “I don't think it should be something that goes out to just anyone because that turns out to be a bit like gun ownership” (PT-01). They were concerned about AI becoming a weapon in the wrong hands (NL-04).

Perspective 4: Preference for Everyone (including themselves)

Contrary to Perspective 3, some participants supported citizen ownership of AI tools for personal safeguarding, especially against cybercrimes. As IT-4 stated, “For cybercrime, I think that all of the people that wanted something to protect themselves from cybercrime should be allowed to have those.” However, some suggested limiting AI ownership to themselves to avoid misuse by others (GR-16). This perspective thus suggests that citizen ownership may be warranted for very specific purposes, while also expressing fear of mistrust in other citizens’ intentions.

Perspective 5: Preference for No one to own AI / unsure about preferred Owner

The final perspective argued against anyone owning AI tools due to concerns about data accuracy, algorithm transparency, and potential misuse (SP-03). Some participants expressed uncertainty about potential AI owners and preferred not to elaborate. This perspective indicates generalised concerns about the viability of AI for security, which translated into a position that no one should own such tools.

3.2 Interpretation of Viewpoints

Participants from various countries shared similar reactions toward police use of AI, though there were notable differences in reasoning. Supporters of perspective 1 believed that only police should own AI tools, citing their role in public safety and trustworthiness with personal data. Some also supported AI use by other LEAs and government bodies for better oversight and objective evaluation. Conversely, participants in perspective 2 opposed police use of AI due to concerns around their capability to manage AI technologies and the transparency of AI-driven decisions. Perspective 3 revealed strong opposition to AI ownership by the public in fear of inadequate knowledge and training, linking it to the risks of public gun ownership in the U.S. In contrast, perspective 4 advocated for public access to AI tools, provided proper training and ethical guidelines are in place. These participants emphasized the need for public involvement in evaluating AI use in policing to ensure transparency. Perspective 5 included a minor group entirely opposed to AI use by anyone, preferring traditional non-AI technologies that have been effective so far.

4. Discussion

In our contemporary world, ownership spans both material items and intellectual properties, with laws protecting these rights to ensure owners can control and benefit from them (Hayes et al., 2020). Ownership of AI includes the rights to possess, use, manage, and benefit from these tools, along with associated responsibilities (Robaey, 2015; Honoré, 1961). The prevalence of AI tools necessitates exploring their ownership to ensure adherence to human rights and privacy laws, which could enhance societal acceptance of AI in policing (Ezzeddine et al., 2022).

This paper examines citizens' views on AI tools’ ownership, discussing these perspectives in relation to debates around AI governance in policing. The findings touch on legal and ethical implications, including roles, responsibilities, expertise, accountability, and public acceptance (Carrasco et al., 2019; Neudert et al., 2020), as well as public willingness to trade privacy for safety (Pavone & Esposti, 2012).

Participants' preferred AI owner correlated with roles, responsibilities, and benefits to the public. Many expressed frustrations over data used for personalized ads without consent, while fewer were concerned about police accessing the same data. Significant concerns included AI's lack of autonomous moral operation and biases in police decision-making (Farina et al., 2020). This correlates to ongoing ethical discussions and recent research highlighting the importance of ownership models that prioritize ethical principles and societal values to foster acceptance (Nemitz, 2018).

Opinions on police ownership were divided. Some trusted police ownership due to their safeguarding roles, while others doubted police expertise and transparency. Some even suggested extending AI ownership to other government and professional entities for oversight (Martin, 2019). This debate aligns with broader discussions around transparency and need for police digitalization strategies (Gundhus et al., 2022). It also reiterates the importance of trust in LEAs and its significant impact for public support of AI in policing. In this context, participants specifically highlighted the importance of police legitimacy and accountability in accessing personal data, reflecting expectations that police actions should prioritize national security (Tyler & Huo, 2002).

Moreover, participants' views often balanced privacy and security. Some accepted police AI use but mistrusted others, suggesting stringent regulations to prevent misuse (Jones & Haggerty, 2021). The debate on privacy versus safety remains critical, with calls for ethical considerations in AI deployment (Lyon, 2002; DiVaio et al., 2022). Some saw AI in surveillance as potentially invasive, linking it to mass data collection and bulk data analysis (Albrecht, 2020). This contrasts with historical arguments defending surveillance for improved security (Bentham, 1791) by highlighting that excessive monitoring could reduce trust in law enforcement (Yesberg et al., 2021).

Participants also recognized the significant influence of corporations on AI development and regulation. They were more critical of AI in targeted advertising by corporations than to its use by police, citing trust in law enforcement's accountability and safeguarding principles (Ezzeddine et al., 2022).

In terms of practical implications, the findings suggest options for differentiated ownership models, as well as the need for robust legal and ethics oversight, and community engagement to address preferences for AI tool ownership in law enforcement. These measures could enhance transparency, trust, and shared responsibility, aligning AI use with societal values and priorities. Below we list some concrete options to increase citizen support of AI use for security purposes:

- Differentiated Ownership Models: Exploring disparate ownership models involving law enforcement and citizen representatives (e.g., acknowledging data origins and dependencies in safety production) to enhance transparency and trust. This could include shared ownership models and public-private partnerships to ensure no single entity dominates (Crawford et al., 2019; Eubanks, 2018). Ownership should reflect data origins and AI's impact on communities, ensuring those most affected have a say in decision-making (O'Neil, 2016).
- Robust legal and Ethical Oversight: Implementing stringent ethics guidelines and independent oversight mechanisms to ensure compliance and prevent misuse. This involves developing comprehensive legal guidance and ethics standards focusing on privacy, bias mitigation, and accountability, with input from diverse stakeholders (Floridi, 2019). Alternatively, independent bodies auditing AI tools can ensure compliance with legal, professional and ethics standards through regular reports (Whittaker et al., 2018).
- Community Engagement: Promoting community-led forums for citizen input in AI tool ownership and control decisions. This includes facilitating citizen assemblies and public consultations to ensure community input is integrated into AI governance, aligning it with public values (Zuboff, 2019). Additionally, creating community-led oversight committees to monitor AI use and advocate for necessary changes can promote education and transparency (Benjamin, 2019).

In summary, the study highlights the need for differentiated considerations on AI ownership and deployment and the importance of citizen engagement to ensure trust and accountability. Future research should explore deeper rationalizations around AI ownership preferences, focusing on roles, responsibilities, expertise, accountability, and the balance between costs and benefits.

As for limitations, our sample was skewed younger and included more women than men, suggesting the need for broader participant demographics in future research. Additionally, some participants felt unqualified to comment on AI ownership, indicating a need for inclusive discussions accounting for all perspectives. Future

studies should address these issues to provide a comprehensive understanding of public perceptions and factors influencing preferences for AI ownership in policing.

5. Conclusion

This study critically examines citizens' perspectives on legitimate ownership of AI technologies, emphasizing the balance between rights and duties of AI implementers, particularly in policing and security. It suggests a need for public involvement in AI tool implementation, accountability, and transparency in data processing and decision-making (Vestby and Vestby, 2019). Moral responsibilities are highlighted, with citizens seen as potential owners, stressing the need for ethical governance and trust in AI applications (Lawrence et al., 2018). The research suggests active public involvement in decision-making to align ownership structures with societal values and ethical considerations (Pavone and Esposti, 2012). This approach enhances understanding of AI acceptance and trust, emphasizing inclusive governance and ethical frameworks (Benjamin, 2020; Ferguson, 2017).

Our findings align with ethical AI principles proposed by entities like the European Commission, addressing public concerns about accountability, legitimacy, and privacy (Ezzeddine et al., 2022). They underscore the importance of training, skills, and ethical principles for AI regulation, regardless of ownership (Albrecht, 2020). Citizens in the study exhibited diverse, instance-based perspectives on AI in policing, guided by roles, responsibilities, and a balance of costs versus benefits, rather than outright rejection (Angwin et al., 2016). This diversity indicates the need for differentiated communication and engagement with citizens about the deployment of AI capabilities for security that acknowledges multiple owners – not only of AI but also of the responsibility to secure society (Bayerl et al., 2022; Terpstra, 2009). By involving the public and ensuring transparency, LEAs can integrate AI technologies while maintaining ethical standards and public trust, reflecting citizens' inquisitive mindset towards ethically guided AI deployments (Yesberg et al., 2021).

Acknowledgement

This work was supported by the European Union's Horizon 2020 research and innovation program under grant agreement No 883569 as part of the AIDA project (AIDA - Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies). For the purpose of open access, the authors applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising from this submission.

References

Albrecht, H.J. (2020). Data, Data Banks and Security. European Journal of Security Research, 5(1), pp. 5-23. doi:10.1007/s41125-019-00062-9.

Aloisi, A. and Gramano, E. (2020). Artificial Intelligence is Watching You at Work. Digital Surveillance, Employee Monitoring and Regulatory Issues in the EU Context. Comparative Labor Law and Policy Journal, pp. 95-121.

Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016). Machine Bias. There is software that is used across the county to predict future criminals. And it is biased against blacks. [online] Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [Accessed 15 February 2022].

Auerbach, C.F. and Silverstein, L.B. (2003). Qualitative Data: An Introduction to Coding and Analysis. NYU Press.

Bayerl, P.S., Butot, V., & Jacobs, G. (2022). Produktion urbaner Sicherheit aus Bürgerperspektive. In: D. Wehe, H. Siller (eds.), Handbuch Polizeimanagement, Springer Nature, pp. 1-18.

Benjamin, G. (2020). Facial recognition is spreading faster than you realize. The Conversation. [online] Available at: https://theconversation.com/facial-recognition-is-spreading-faster-than-you-realise-132047 [Accessed 15 February 2022].

Benjamin, R. (2019) Race After Technology: Abolitionist Tools for the New Jim Code, Polity.

Bentham, J. (1791). Panopticon, or, The Inspection-House. Dublin: T. Payne.

Carrasco, M., Mills, S., Whybrew, A. and Jura, A. (2019). The Citizen's Perspective on the Use of AI in Government. BCG Digital Government Benchmark. [online] Available at: https://www.bcg.com/publications/2019/citizen-perspective-use-artificial-intelligence-government-digital-benchmarking.aspx [Accessed 15 February 2022].

Charmaz, K. (2006). Constructing Grounded Theory: A Practical Guide through Qualitative Analysis. London: Sage Publications.

Chohan, S.R. and Hu, G. (2020). Strengthening digital inclusion in e-government: Cohesive ICT training programs intensify digital competency. Information Technology for Development, 28(1), pp. 1-23. doi:10.1080/02681102.2020.1841713.

Crawford, K. and Calo, R. (2016). There is a blind spot in AI research. Nature, 538(7625), pp. 311-313.

Crawford, K., Dobbe, R., Dryer, T., Fried, G., Green, B., Kaziunas, E. and Whittaker, M. (2019) AI Now 2019 Report, AI Now Institute.

Di Vaio, A., Hassan, R. and Alavoine, C. (2022). Data intelligence analytics: A bibliometric analysis of human–AI interaction in public sector decision-making effectiveness. Technological Forecasting and Social Change, 174, 121201. doi:10.1016/j.techfore.2021.121201.

Eubanks, V. (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, St. Martin's Press.

European Commission. (2020). EU Economic and Social Committee Regulation on AI in Europe, 237 final. Brussels: European Commission. [online] Available at: https://www.njb.nl/umbraco/uploads/2018/7/COM-2018-237-F1-EN-MAIN-PART-1.PDF [Accessed 18 February 2022].

Ezzeddine, Y., Bayerl, P.S. and Gibson, H. (2022). Citizen Perspectives on Necessary Safeguards for the Use of AI by Law Enforcement Agencies. arXiv.org. doi:10.48550/arXiv.2306.01786.

Farina, M., Zhdanov, P., Karimov, A. and Lavazza, A. (2022). AI and society: A virtue ethics approach. AI & Society. doi:10.1007/s00146-022-01545-5.

Ferguson, A.G. (2017). Policing Predictive Policing. Washington University Law Review, 94(5), pp. 1109-1189.

Floridi, L. (2019). The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford University Press.

Floridi, L. and Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A, 374(2083), 20160360.

Gundhus, H.O., Talberg, N. and Wathne, C.T. (2022). From discretion to standardization: Digitalization in police organizations. International Journal of Police Science & Management, 24(1), pp. 27-41. doi:10.1177/14613557211036554.

Hayes, P., van de Poel, I. and Steen, M. (2020). Algorithms, values, and justice in security. AI & Society, 35, pp. 533-555. doi:10.1007/s00146-019-00932-9.

Jones, R. and Haggerty, K.D. (2021). AI policing: A white paper. Surveillance & Society, 19(3), pp. 331-337.

Krippendorff, K. (2004). Content Analysis: An Introduction to its Methodology. Thousand Oaks; London; New Delhi: Sage Publications.

Kroll, J.A., et al. (2017). Accountable Algorithms. University of Pennsylvania Law Review, 165(3), pp. 633-705.

Lawrence, D., Peterson, B. and Thompson, P. (2018). Community views on Milwaukee's police body-worn camera program. Justice Policy Center, Urban Institute.

Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. Information, Communication & Society, 5(2), pp. 242-257. doi:10.1080/13691180210130806.

Martin, G. (2019). Public attitudes towards police use of facial recognition technology. Police Quarterly, 22(3), pp. 349-368.

Mittelstadt, B.D., et al. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679.

Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133), 20180089. doi:10.1098/rsta.2018.0089.

Neudert, L.M., Knuutila, A. and Howard, P. (2020). Global Attitudes Towards AI, Machine Learning & Automated Decision Making: Implications for Public Service and Good Governance. University of Oxford: Oxford Commission on AI and Good Governance.

O'Neil, C. (2016) Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown.

Orwell, G. (2000). 1984 Nineteen Eighty-Four. Introduced by Thomas Pynchon. England: Penguin Classics.

Pavone, V. and Esposti, S. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. Public Understanding of Science, 21(5), pp. 556-572. doi:10.1177/0963662510376886.

Peeters, R. and Widlak, A. (2018). The digital cage: Administrative exclusion through information architecture – The case of the Dutch civil registry's master data management. Government Information Quarterly, 35(2), pp. 175-183.

Robaey, Z. (2015). Looking at moral responsibility for ownership: A way to deal with hazards of GMOs. Journal of Agricultural and Environmental Ethics, 28(1), pp. 43-56. doi:10.1007/s10806-014-9517-8.

Schuilenburg, M. and Peeters, R. (2020). Algorithmic society. Algorithmic Society, pp. 1-15. doi:10.4324/9780429261404-1.

Terpstra, J. (2009a). Citizen involvement in local security networks. Security Journal, 22, 156–169.

Tyler, T.R. and Huo, Y.J. (2002). Trust in the Law: Encouraging Public Cooperation with the Police and Courts. Russell Sage Foundation.

Vestby, A. and Vestby, J. (2019). Machine Learning and the Police: Asking the Right Questions. Policing: A Journal of Policy and Practice. doi:10.1093/police/paz035.

Whittaker, M., Crawford, K., Dobbe, R. and Fried, G. (2018) AI Now 2018 Report, AI Now Institute.

Yesberg, J., Brunton-Smith, I. and Bradford, B. (2021). Police visibility, trust in police fairness, and collective efficacy: A multilevel structural equation model. European Journal of Criminology. doi:10.1177/14773708211035306.

Zuboff, S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, PublicAffairs.