Body Worn Cameras with an embedded FRT

Ethical Audit and evaluation

**

**

•Computing methodologies~Artificial intelligence~Computer vision~Computer vision problems

Additional Keywords and Phrases: Body-Worn Cameras, Facial Recognition Technology, Ethical Auditing, AI Systems, Transparency, Fairness, Privacy, Accountability, Safety, Law Enforcement, Garda Síochána.

Abstract

While AI technology has the potential to transform many parts of our life, it also poses substantial ethical issues. This research briefly presents ethical challenges surrounding AI, with a focus on the utilization of body-worn cameras (BWCs) equipped with embedded facial recognition technology (FRT) by the Garda forces in Ireland. I highlighted the current approaches to ensure an ethical AI, and at the end, I did an audit report for the BWCs with an embedded FRT that the Irish government plans to emblement and adopt to reenforce the Garda with. I selected the Assessment List for Trustworthy AI (**ALTAI)** to do the audit evaluation and developed tailored recommendations that covered the aspects of Human agency and oversight, Technical robustness and safety, Privacy and Data Governance, Transparency, Diversity, non-discrimination and fairness, Societal and environmental well-being, and accountability.

1 OVERVIEW OF ETHICAL ISSUES IN AI

Introduction

AI has evolved as a strong technology with the potential to transform many parts of our life. It has enormous potential, from boosting industrial efficiency to improving medical diagnoses. However, AI presents substantial ethical challenges in addition to its transformational promise. privacy, transparency, fairness, human agency, and the possibility for bias and discrimination are all examples of ethical challenges in AI. It is critical to address these challenges in order to maintain responsible development, high integrity, and efficiency.

1.1 Overview of Ethical Issues in AI

Stahl [1] has spotted 39 Ethical issues for AI, however, the most important ones are the following:

- Bias, Fairness: As per Benjamin [2]: Technological developments are promoted as ethically better because they claim to be beyond human bias, despite the fact that they could not exist without data gathered from histories of discrimination and exclusion. AI algorithms can magnify existing bias in the data they are trained on, resulting in unfair or discriminatory outcomes in domains such as hiring, lending, and criminal justice.

Benjamin [2] says that bias comes through the backdoor of design optimization, where the individuals who construct the algorithms are concealed from view.

- Privacy and Data Protection and Accuracy: AI systems frequently require access to massive volumes of data, generating issues about privacy, data security, and surveillance, and the possibility for illegal use or exploitation of personal information. As per Saheb [3], the decry of AI technologies is for their unintended or deliberate detrimental consequences, notably in the lives of individuals, as well as their ability to assist anti-democratic policies and abuses of privacy and human rights norms.
- Accountability and transparency: AI systems may be complicated and vague, making understanding how choices are made challenging. Transparency raises questions about responsibility and the capacity to rectify problems or errors. Cavoukian [4] explains that the AI systems should guarantee to all stakeholders that the practice or technology involved is performing in accordance with the stated promises and objectives, subject to independent verification, and all of its processes components should be clear and transparent to both consumers and suppliers.
- Job Displacement and Economic effect: Because AI-enabled automation can result in job displacement, economic inequality, and social rampage, the societal effect of AI-driven innovations must be considered. As per Stahl [1] It is more likely for the job loss to become a key problem, and humans are required to be creative to come up with new job opportunities in this era and improve the possibilities for the current employees and give them the chance to upgrade their skills.
- Autonomy and Human Agency: As AI systems become more autonomous, issues regarding the role and responsibility of people in decision-making processes arise, as does the potential for AI to undermine human agency. Stahl [1] elucidates that AI has the potential to create numerous opportunities and possibilities that were previously unimaginable. However, it can also limit individual freedom by diminishing the capacity to make choices and take actions, both in less or more subtle ways.

1.2 AI For policing

AI for policing and predictive policing purposes, including the utilisation of body worn cameras, facial recognition technology (FRT), biometric systems, and video surveillance cameras, has become a critical area that requires careful examination. While AI-enhanced law enforcement can enhance crime prevention and evidence gathering, it also gives rise to a range of ethical concerns and potential risks.

1.3 The Adoption of Body Worn Cameras for Guards in Ireland

As Miranda [5] explains, the body-worn camera (BWC) is a device that records audio and video and is worn by police officers. BWCs accompany officers as they move and physically engage with their surroundings, serving as a tool that influences the dynamics of interactions between police and citizens.

In his statement, Simon Harris the Minister of Justice said "I am absolutely determined to do everything I can to protect members of the force" [6].

The Ministry of Justice is actively working towards enacting legislation that permits police officers to carry wearable cameras. By equipping officers with these cameras, they will have the ability to document all incidents they come across. The Minister of Justice advocates for incorporating facial recognition capabilities into these cameras, emphasising that officers face frequent verbal and physical assaults on a daily basis. According to the Department of Justice [7] This technological advancement will enhance the national security measures, empower officers to pursue attackers, and play a crucial role in establishing evidence against criminals. And as per Harris [8], in this way, the Irish Guards will keep pace with global development as well. According to the Irish Council for Civil Liberty (ICCL) [8], This technology was originally brought to monitor the violence, abusive and immoral behaviour of police officers, in the US towards some groups of people (based on their race).

1.4 The ethical issues associated with the BWCs

1.The breaching of privacy: BWCs record audio and video of both police officers and the people they interact with, which raises concerns about invasions of privacy, particularly in private or delicate circumstances. Finding a balance between police transparency and defending citizens' rights to privacy is a critical ethical consideration. As per Cross & Cavallaro [9] Generating huge amount of data out of using BWCs leads to the need to use tools provided by a third-party to store them using the cloud technology, and that makes all of that data vulnerable to leakage and/or hacking.

2.Surveillance and Constant Monitoring: The extensive deployment of BWCs can lead to a pervasive surveillance culture in which individuals feel constantly scrutinised. This can have serious consequences for freedom of expression, privacy, and the capacity to engage in activities without fear of undue scrutiny. ICCL [8] brought an example that citizens decide not to participate in a demonstration if they know Guards will be wearing the device, or they may limit their speech or who they interact with for fear of being filmed. **3.**Bias and Fairness by being selective: BWCs do not continuously record and must be manually triggered by the officer [10]. Hence, officers can selectively activate or deactivate BWCs, raising questions about potential bias in the recording process. Biases in determining when to record or cease recording, whether unintentional or purposeful, may influence the overall accuracy and dependability of documented events. **4.**Accountability and Transparency: The purpose of BWCs is to improve police accountability and openness. However, it is vital to ensure that the recorded footage is appropriately evaluated, analysed, and used in disciplinary proceedings. The issue here is to establish a strong mechanism for the use of the BWCs footage in a fair and responsible way so it maintains transparency and at the same time does not breach privacy. Coudert et al [11] see that the utilisation of BWCs significantly invades the privacy of both citizens and police officers. It can also affect fundamental freedoms like the freedom of movement and the right to privacy in the home, as recordings disclose locations and may occur in private dwellings. **5.**Data Storage and protection: Because BWC film frequently contains sensitive information, safe storage and restricted access are required. It is critical to maintain public trust and defend people's rights by ensuring that recorded data is protected from unauthorised access, misuse or manipulation. Body cameras rely on modern technology for automated cloud storage. Once the policeman enters the police station, the data is transferred [5]. This, in my opinion, raises questions about the security of this mechanism and its ability to address hackers' interceptions. The cameras may contain footage of the victims, or those present at the crime scene while they are in their worst condition. Leaking these sensitive videos, either by penetrating the cloud storage, or perhaps with the fall of one of these cameras from a policeman, will cause a very big crisis of trust in this technology and the police [5]. **6.** Accuracy: since the BWCs will come with an FRT technology, the issue of accuracy will arise, since AI algorithms may be sophisticated and vague, making it difficult to grasp how they make judgments or make predictions. According to Professor Farris, FRT could still make mistakes and there is still a high risk of discrimination by using this technology. [12]

2 CURRENT APPROACHES TO ENSURING ETHICAL AI

Several influential entities have developed various approaches and guidelines to promote the ethical implementation of AI. Outlined below are three prominent guidelines that serve as noteworthy examples:

- The European Commission Principles: formed six principles that focus on respecting human agency, privacy & data governance, fairness, social and environmental well-being, transparency, and accountability. They provide a solid foundation and explanation for ethical AI design, emphasising fundamental rights and values. European Commission, [13] The framework provided an overview of the stages involved in the development of artificial intelligence systems, outlining how ethical principles are applied throughout the process. It also described the mechanisms for monitoring and ensuring compliance.
- The Montreal Declaration For a Responsible Development Of Artificial Intelligence [14]: This declaration expands on the principles by emphasising well-being as (AIS) must help individuals to improve different aspects of their lives and not affect them negatively in any way, human autonomy, privacy, solidarity, democratic participation, equity To ensure that the AIS should not lead or generate any data based on any type of discrimination and must help to avoid any exclusion to the groups and individuals., diversity, prudence which is about maintaining the AIS less harmful, more beneficial, and that the system must strictly be reliable, secure., responsibility, and sustainability [14]. It introduces important considerations such as the avoidance of discrimination and the preservation of social cohesion.
- The Asilomar Approach [15]: The Asilomar principles encompass 23 ethics and values, including safety, transparency, responsibility, value alignment, and human values which refer that highly autonomous AI systems should be constructed in such a way that their aims and actions are guaranteed to fit with human values, personal privacy, shared benefit and prosperity as the AIS should empower and benefit as many people as possible, and the economic gains from AIS should be distributed widely, human control, non-subversion so AIS should improve, not undermine, social and civic processes. , and Promoting the prevention of developing lethal autonomous weapons [16]. These principles cover a broad range of ethical aspects and emphasise the societal impact of AI.

These approaches share common points such as respecting human rights, privacy, transparency, and accountability. They address key ethical considerations and provide valuable guidelines for responsible AI development. However, there may be slight variations and overlaps in the principles, leading to potential confusion or inconsistencies when implementing them. Harmonising and aligning the frameworks could improve their effectiveness and ease of application. Additionally, while these frameworks address ethical concerns, their effectiveness relies on their implementation and enforcement. Ensuring widespread adoption and adherence to these principles across the AI development community remains a challenge. It is essential to consistently monitor and evaluate these approaches in order to adapt them to ever-changing technological landscapes and emerging ethical challenges. Regular updates and collaboration are crucial in this process.

2.1 Ethical Principles for BWCs & Policing AI

From the previous approaches and frameworks, almost all of the principles and AI solutions are relevant to the BWCs and FRT, however, we can identify the most relevant principles or solutions when deploying technologies such as body-worn cameras and face recognition systems as following:

- Respect for Human Agency, including the fundamental human rights of autonomy, dignity, and freedom: emphasise the necessity of protecting individuals (including the stakeholders) rights and autonomy; they emphasise the need to guarantee that these technologies have no impact on people's rights and freedoms.

- Privacy and Data Governance: relates to the protection of individuals' privacy and the responsible handling of their data. It is crucial to consider privacy concerns and establish robust data governance practices to safeguard sensitive personal information.
- Fairness: entails ensuring that the use of BWCs and FRT is unbiased and does not result in discriminatory outcomes. It involves addressing issues related to algorithmic bias and ensuring that these technologies are deployed in a manner that treats all individuals fairly and equally.
- Transparency: It involves providing clear information about the use of BWCs and FRT, including their purpose, functionality, and potential implications for individuals' (policemen and civilians) rights and privacy. Transparent practices promote trust, accountability, and informed decision-making.
- Accountability and Audit: This highlights the importance of accountability mechanisms as well as adequate oversight of BWCs and FRT. It entails creating clear lines of accountability, guaranteeing compliance with ethical standards and laws, and offering channels for recourse and restitution in the event of misuse or injury.

The Data Protection Commission (DPC) [17] in Ireland has issued comprehensive guidance on the ethical use of body-worn cameras (BWCs) or action cameras while complying with data protection laws. The guidance emphasizes the importance of conducting a Data Protection Impact Assessment (DPIA) prior to implementation and establishing a lawful basis for processing personal data, including obtaining clear and informed consent. Transparency, data security, appropriate storage and retention periods, respect for individual rights, and accountability through training and mechanisms like audits are also highlighted. This guidance serves as a valuable resource for organizations and individuals involved in deploying BWCs or action cameras in Ireland. The DPC's guidance provides practical recommendations to ensure ethical and lawful practices while safeguarding individuals' privacy rights. It promotes transparency, consent, data security, and accountability in the deployment of BWCs or action cameras in Ireland [17].

In the same context, the ICCL's Submission on the Garda Síochána (Digital Recording) Bill [18] raises critical ethical concerns about the Irish police force's usage of digital recording equipment. The response emphasises the need of protecting individuals' privacy rights, complying with data protection regulations, preserving freedom of expression and assembly, ensuring openness and accountability, promoting ethical usage and training, and include the public in decision-making processes [18].

3 ETHICAL EVALUATION APPROACHES

-**Ethical Impact Assessment (EIA)**: a process in which an organisation, in collaboration with stakeholders, evaluates the ethical concerns or consequences of a new project, technology, law, or other effort in order to identify risks and solutions, however, it can be done with or without the participation of the stakeholders [19], it follows the procedural steps of: 1.Threshold Analysis, 2.EIA Plan Preparation, 3. Ethical Impacts Identification Assessment, 4.Evaluation of Ethical Impacts, 5.Formulate and Implement Remedial Action, 6.Review & Audit EIA Outcomes. The use of BWCs and FRT systems is leading to raising ethical issues such as privacy, monitoring, prejudice, and the potential for misuse, hence, (EIA) presents a systematic approach for assessing the ethical implications of BWCs and FRT systems implementation, and helps identify and evaluate the potential impact on individual rights, public trust, and community relationships [19].

-**Assessment List for Trustworthy AI (ALTAI)**: It was established by the European Commission to assist in determining if the AI system being developed, deployed, or utilised meets the following seven standards of Trustworthy AI: 1.Human Agency and Oversight, 2.Technical Robustness and Safety, 3.Privacy and Data Governance, 4.Transparency, 5.Diversity, Non-discrimination and Fairness, 6.Societal and Environmental Well-being, 8.Accountability.ALTAI is capable to evaluates the overall trustworthiness of AI systems, and that of course includes BWCs and FRT. As part of its assessment criteria, it covers ethical issues such as fairness, privacy, and social impact and helps mitigate and ensure privacy compliance [20]

-IEEE Ethically Aligned Design (EAD): Is an initiative led by the IEEE Global for Ethical Considerations in Artificial Intelligence and Autonomous systems. It provides a framework for developers and implementers of AI systems to assign importance to ethical considerations during the design and development stages. It establishes that the design implementation and development of AI should be guided by the general principles of well-being, human rights, accountability, awareness of misuse, and transparency. The approach is based on three main pillars: 1. Universal Human Values, 2. Political Self-Determination and Data Agency, 3.Technical Dependability [21]. EAD stresses the incorporation of ethical issues into AI system design and development, and that is applicable to the BWCs and FRT. also EAD guides developers in designing BWCs and FRT systems that align with ethical guidelines principles such as fairness, transparency, accountability, and privacy, etc. [21]

Standard ethical audits of systems in the domains of Body-Worn Cameras (BWCs) and Facial Recognition Technology (FRT) are required. [22] spotted the concerns of the ethical issues of bias, accountability & transparency, data Privacy & security, and Human Rights. Therefore Ethical audits are critical in assuring responsible and ethical procedures in the development, implementation, and application of these technologies. Here is why:

1.Addressing Ethical concerns: BWCs and FRT systems present serious ethical questions about privacy, surveillance, bias, and potential civil liberties violations. Ethical audits give an organised and methodical strategy for identifying, evaluating, and addressing these challenges, ensuring that technologies are utilised ethically and responsibly. **2.**Bias: Ethical audits evaluate algorithms, data collecting, and decision-making to discover and minimise biases, guaranteeing fair treatment and non-discrimination. Ethics Guidelines For Trustworthy AI [23] elaborates that The development, deployment, and utilisation of AI systems must prioritise fairness, ensuring the avoidance of any form of unfair bias, discrimination, or stigmatisation. **3.**Accountability and Transparency are enhanced through ethical audits, which promote fairness, protect rights, and assess compliance with legal and ethical standards in BWCs and FRT systems. Explicability is crucial for building and maintaining users' trust in AI systems [23]. **4.**Data Privacy and Security: Ethical audits examine how BWCs and FRT systems manage and safeguard personal information. They guarantee that privacy standards are followed, that data acquisition is necessary and consistent, and that security measures are in place to protect sensitive information. According to Ethics Guidelines For Trustworthy AI [23], AI systems must be designed in a way that avoids causing harm, exacerbating harm, or negatively impacting human beings. **5.**Human Rights and Autonomy Considerations: Ethical audits of BWCs and FRTs help look for potential abuses of human rights, such as the right to privacy, freedom of expression, and freedom of assembly. Audits assist in identifying any violations of these rights and enabling corrective steps to be performed. Preserving individual autonomy and promoting democratic participation are essential for humans interacting with AI systems [23]. **6.**Ecological impact (should be taken into consideration): Ethical audits of BWCs and FRT systems helps assessing ecological impacts, considering manufacturing, energy consumption, and environmental effects. According to Ethics Guidelines For Trustworthy AI [23] The environment should be regarded as a significant stakeholder throughout the entire life cycle of AI systems.

4 AUDITIN THE BWCS WITH AN EMBEDDED FRT USING (ALTAI AUDIT)

An Ethical Audit of Garda's Deployment of BWCs with Integrated FRT, using The Assessment List for Trustworthy Artificial Intelligence (ALTAI). [**]

Recommendations

Human agency and oversight

1.Develop specific guidelines and training programs for Garda officers on the use of BWCs with embedded FRT, focusing on the importance of human decision-making and oversight. **2.**Implement regular up to date courses and workshops to ensure officers understand the capabilities and limitations of the AI system and know how to exercise effective oversight. **3.**Establish a clear protocol for reporting and addressing instances where officers feel their autonomy is being inadvertently affected by the AI system. **4.**Collaborate with experts from psychology and social work to design measures that minimise the risk of addiction and promote the mental well-being of officers and the public. **5.**Establish detection and response mechanisms in case the AI system generates undesirable adverse effects for the end-user or subject. **6.**Give specific training to humans (human-in-the-loop, human-on-the-loop, human-in-command) on how to exercise oversight. **7**. Define who should and who shouldn't wear the BWCs. **8.** Define when the end user is allowed to turn the BWCs off.

Technical robustness and safety

1.Conduct a comprehensive risk assessment (by defining risk, risk metrics and risk levels) to identify specific risks associated with the deployment of BWCs with embedded FRT in the Garda's operational environment. 2.Create a fault-tolerant system design with multiple backups or alternative systems to ensure ongoing operation in the event of failures or technical issues. 3.Establish a robust process to monitor and document the accuracy and reliability of the BWCs with an embedded FRT system, ensuring it meets the expected standards and performance levels. 4.Implement regular testing and verification procedures to ensure the reproducibility of results in different operational contexts. 5.Create a well-defined procedure for reviewing and updating the technical robustness and safety measures as the AI system evolves or new risks are identified. 6.Identify the possible threats to the BWCs & FRT system (design faults, technical faults, environmental threats) and the possible resulting consequences. 7.Assess the dependency of the critical system's decisions on its stable and reliable behaviour.

Privacy and Data Governance

1.Prioritise the protection of personal data and privacy rights in the deployment and use of BWCs with embedded FRT, ensuring compliance with relevant data protection regulations, including the GDPR, EU regulations, etc. 2.Establish procedures for collecting and preserving data gathered by BWCs, including data retention policies and safe data disposal. 3.Conduct regular audits and assessments of data handling practices to ensure compliance and identify any potential privacy risks or data breaches. 4.Provide clear information to the public about the purposes, ownership, and aims of the BWCs with an embedded FRT system, promoting transparency and accountability. 5.Engage with data protection authorities and relevant stakeholders to ensure best practices in privacy and data governance are followed throughout the implementation.

Transparency

1.Create clear standards and practices for explaining BWCs with embedded FRT system choices to both the officers using the system and the individuals being monitored. **2.**Communicate with end users and the general public on a regular basis on the operation and capabilities of the AI system, ensuring that they understand the technology's limitations and possible effects. **3.**Implement mechanisms to gather feedback from users, allowing them to express their understanding of the system's decisions and addressing any concerns or misunderstandings. **4.**In the case of interactive BWCs with embedded FRT, clearly inform users that they are interacting with an automated system, to enhance transparency and manage expectations. **5.**Maintain a transparent approach during the development and deployment of the AI system, documenting the processes and decisions made to ensure accountability and build trust with stakeholders. **6.**Establish a culture within the Garda that promotes openness, transparency, and accountability throughout the development and implementation of BWCs with embedded FRT.

Diversity, non-discrimination and fairness

1.Assess the representativeness of data used in training the AI system to ensure it adequately reflects the diversity of the communities served by the Garda. **2.**Consult with impacted communities, such as representatives of elderly persons or persons with disabilities, to understand their perspectives and incorporate their input in defining fairness criteria. **3.**Implement quantitative metrics and evaluation methods to measure and test the applied definition of fairness, ensuring that the BWCs with embedded FRT system does not disproportionately impact certain groups. **4.**Conduct user surveys and feedback sessions to assess understanding and acceptance of the decisions made by the AI system, addressing any concerns related to fairness or discrimination. **5.**Regularly review and update the fairness assessment process, considering emerging research, evolving societal expectations, and feedback from affected communities.

Societal and environmental well-being

1.Consider the potential positive and negative impacts of BWCs & FRT system on the environment and establish mechanisms to evaluate this impact. **2.**Define measures to reduce the environmental impact of BWCs & FRT system's lifecycle and participate in competitions for the development of AI solutions that tackle this problem. **3.**Assess the potential positive and negative impacts of BWCs with embedded FRT on the environment, taking measures to reduce the environmental footprint of the system's life cycle. **4**.Actively participate in competitions and initiatives focused on developing AI (BWCs & FRT) solutions that promote environmental sustainability and contribute to societal well-being. **5.**Establish mechanisms to evaluate and address any social or environmental risks associated with the use of BWCs with embedded FRT, ensuring that the benefits outweigh any potential negative consequences. **6.**Consider the possibility of getting a consent before starting the BWCs.

Accountability

1.Establish clear mechanisms for third-party auditing of the BWCs with an embedded FRT system, allowing independent assessments of its compliance with ethical guidelines, legal requirements, and best practices. **2.**Implement a robust accountability framework that includes regular monitoring and evaluation of the system's performance, ensuring it aligns with intended objectives and operates within defined ethical boundaries. **3.**Document and explain any conflicts of values or trade-offs involved in the system's decision-making processes, providing transparency and justifying the reasoning behind key choices. **4.**Continuously update the risk management process by incorporating new findings and insights, allowing for timely revisions of risk assessments and quantitative analyses. **5.**Establish a culture of accountability within the organisation, where supervisors are obligated to conduct reviews of BWCs use and ensure compliance with established guidelines and procedures.

FOOTNOTES

[**] In the absence of specific documentation pertaining to BWCs and FRT, I relied on the GDPR, Code of Ethics for the Garda Síochána and the Vision for the Future of Policing in Ireland, and AI Here for Good. All the information that I extracted from these documents provide general guidelines, recommendations, and general information that are not detailed. It is noteworthy that I also benefited from previous audits on the same subject on The City of Denton's Police Department (Audit of Body-Worn Camera Usage, 2021), (Minneapolis Police Department Mobile and Body Worn Video Recording Equipment Program Audit, 2017), (Implementation of Body Worn Cameras | Rapid Review of Current Research and Practice). It is noteworthy thatI also benefited from previous audits on the same subject on the The City of Denton's Police Department (Audit of Body-Worn Camera Usage, 2021), (Minneapolis Police Department Mobile and Body Worn Video Recording Equipment Program Audit, 2017), (Implementation of Body Worn Cameras | Rapid Review of Current Research and Practice).

REFERENCES

[1] Stahl, B. C. (2021). Concepts of Ethics and Their Application to AI. In Springer eBooks (pp. 19–33). https://doi.org/10.1007/978-3-030-69978-9_3

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

[3] Saheb, T. (2022). Ethically contentious aspects of artificial intelligence surveillance: a social science perspective. AI And Ethics, 3(2), 369–379. https://doi.org/10.1007/s43681-022-00196-y

[4] Cavoukian, A. (2010). Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. Identity in the Information Society, 3(2), 247–251. https://doi.org/10.1007/s12394-010-0062-y

[5] Miranda, D. (2021b). Body-worn cameras 'on the move': exploring the contextual, technical and ethical challenges in policing practice. Policing & Society, 32(1), 18–34. https://doi.org/10.1080/10439463.2021.1879074

[6] Harris, S. (2023, February 7). Simon Harris explains push for Garda bodycams and facial recognition technology. Irish Mirror. Retrieved from https://www.irishmirror.ie/news/irish-news/garda-bodycams-simon-harris-29152447

[7 Department of Justice. (2023, February 1). Minister Harris introduces key legislation on Garda use of body worn cameras, ANPR and CCTV to the Dáil. Retrieved from https://www.gov.ie/en/press-release/6185a-minister-harris-introduces-key-legislation-on-garda-use-of-body-worn-cameras-anpr-and-cctv-to-the-dail/

[8] Iccl. (2019). Body-worn cameras for Gardaí would breach privacy and trust. Irish Council for Civil Liberties. https://www.iccl.ie/news/body-worn-cameras-for-gardai-would-breach-privacy-and-trust/

[9] Cross, M. S., & Cavallaro, A. (2020). Privacy as a Feature for Body-Worn Cameras [In the Spotlight]. IEEE Signal Processing Magazine, 37(4), 145–148. https://doi.org/10.1109/msp.2020.2989686

[10] Boivin, R., Gendron, A., Faubert, C., & Poulin, B. (2016). The body-worn camera perspective bias. Journal of Experimental Criminology, 13(1), 125–142. https://doi.org/10.1007/s11292-016-9270-2

[11] Coudert, F., Butin, D., & Métayer, D. L. (2015). Body-worn cameras for police accountability: Opportunities and risks. Computer Law & Security Review, 31(6), 749–762. https://doi.org/10.1016/j.clsr.2015.09.002

[12] Cox, J. (2023, May 7). FRT on Garda body cameras could open door to "mass surveillance," expert warns. BreakingNews.ie. https://www.breakingnews.ie/ireland/frt-on-garda-body-cameras-could-open-door-to-mass-surveillance-expert-warns-1471783.html

[13] European Commission. (2021). Ethics By Design and Ethics of Use Approaches for Artificial Intelligence. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf

[14] MONTRÉAL DECLARATION FOR A RESPONSIBLE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE. (2018). https://www.montrealdeclaration-responsibleai.com/_files/ugd/ebc3a3_506ea08298cd4f8196635545a16b071d.pdf

[15] Gillis, A. S. (2023). What is Asilomar AI Principles? - Definition from WhatIs.com. WhatIs.com. Retrieved from https://www.techtarget.com/whatis/definition/Asilomar-AI-Principles

[16] De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). Artificial Intelligence and the Future of Defense: Strategic Implications For Small- and Medium-Sized Force Providers. The Hague Centre for Strategic Studies.

[17] Data Protection Commission (DPC). (2020). Guidance on the Use of Body Worn Cameras or Action Cameras. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Body%20Worn%20Cameras%20or%20Action%20Cameras_Jan20.pdf

[18] ICCL (2021). ICCL Submission on the Garda Síochána (Digital Recording) Bill. https://www.iccl.ie/wp-content/uploads/2022/09/210813-FINAL-ICCL-Submission-Digitial-Recording-Bill-2.pdf

[19] Reijers W., Brey P., Jansen P., Rodrigues R., Koivisto R., Tuominen A. (2016). A Common Framework for Ethical Impact Assessment Annex 1 A reasoned proposal for a set of shared ethical values, principles and approaches for ethics assessment in the European context Deliverable D4.1. https://satoriproject.eu/media/D4.1_Annex_1_EIA_Proposal.pdf

[20] Home page - ALTAI. (n.d.). Altai.insight-Centre.org. https://altai.insight-centre.org/

[21] IEEE. (2019). Ethically Aligned Design - a Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems, 1–294. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9398613

[22] Miller, L., Toliver, J., & Police Executive Research Forum. (2014). Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned. Washington, DC: Office of Community Oriented Policing Services.

[23] High-Level Expert Group on Artificial Intelligence. (2019). ETHICS GUIDELINES FOR TRUSTWORTHY AI. European Commission. Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html

--The following references were used only for inspiration and support in completing the ALTAI audit evaluation, without any direct quote:

[24] HD Centre of Humanitarian Dialogue. (2021). Code of Conduct on Artificial Intelligence in Military Systems. Retrieved from https://hdcentre.org/insights/ai-code-of-conduct/

[25] An Garda Síochána Vision for the Future of Policing in Ireland. (n.d.). 2022 http://policereform.ie/en/POLREF/An%20Garda%20S%C3%ADoch%C3%A1na.pdf

[26] Code of Ethics for the Garda Síochána. (n.d.). Retrieved December 7, 2022, from https://www.garda.ie/en/about-us/publications/policy-documents/code-of-ethics-2020.pdf

[27] Skinner, I., Wuersch, L., Bamberry, L., Sutton, C., Neher, A., Hogg, R., O'Meara, P., & Dwivedi, A. (2022). Implementation of Body Worn Cameras: Rapid Review of Current Research and Practice. Regional Work and Organisational Resilience Research Group, Charles Sturt University, for NSW Ambulance. Retrieved from https://researchoutput.csu.edu.au/ws/portalfiles/portal/301473503/Final_Rapid_Review_Report.pdf

[28] Audit of the Department of Justice Policy on Body Worn Cameras. (2021). Retrieved from https://oig.justice.gov/sites/default/files/reports/21-085.pdf

[29] Baloun, B. (n.d.). INDEPENDENT AUDIT REPORT. Retrieved July 6, 2023, from https://www.ci.becker.mn.us/DocumentCenter/View/2374/2021-Audit-Report---Becker-PD-Final-PDF

[30] Rorschach M., CIA, CGAP, Audit of Body-Worn Camera Usage, (n.d.) 2023, from https://www.cityofdenton.com/DocumentCenter/View/6728/Audit-of-Body-Worn-Camera-Usage-PDF

[31] Government of Ireland. (2021). AI - Here for Good: A National Artificial Intelligence Strategy for Ireland. Retrieved from https://enterprise.gov.ie/en/Publications/Publication-files/National-AI-Strategy.pdf

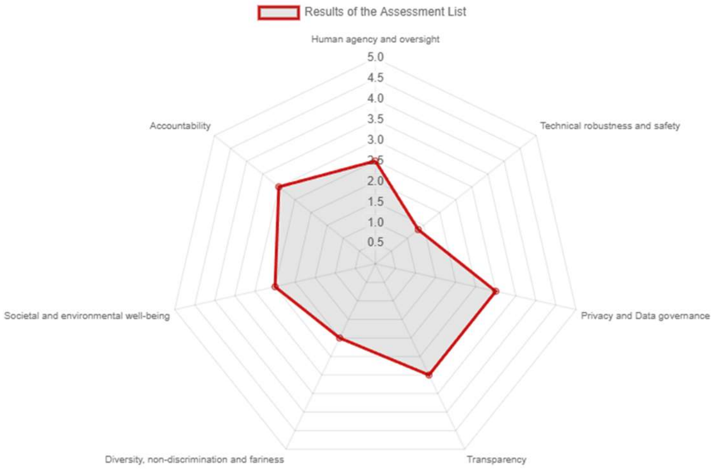
[30] Implementing a Body-Worn Camera Program Recommendations and Lessons Learned. (2014). Retrieved from https://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/implementing%20a%20body-worn%20camera%20program.pdf

[31] Minneapolis Police Department Mobile and Body Worn Video Recording Equipment Program Audit City of Minneapolis -Internal Audit Department. (2017). Retrieved from https://mn.gov/mdhr/assets/2017.09.19%20Oversight%20Commission%20-%20Video%20Recording_tcm1061-457058.pdf

A APPENDICES

A1. ALTAI Audit evaluation recommendations:

The following is the (raw) result of the ALTAI Audit before tailoring it to the subject of BWCs with an embedded FRT:



Recommendations

Human agency and oversight

- Put in place procedures to avoid that end users over-rely on the AI system.
- Put in place any procedure to avoid that the system inadvertently affects human autonomy.
- Take measures to minimize the risk of addiction by involving experts from other disciplines such as psychology and social work.
- Take measures to mitigate the risk of manipulation, including providing clear information about ownership and aims of the system, avoiding unjustified surveillance, and preserving autonomy and mental health of users.
- Give specific training to humans (human-in-the-loop, human-on-the-loop, human-in-command) on how to exercise oversight.
- Establish detection and response mechanisms in case the AI system generates undesirable adverse effects for the end-user or subject.
- Deploy a “stop button” or procedure to safely abort an operation when needed.

Technical robustness and safety

- Define risk, risk metrics and risk levels of the AI system in each specific use case.
- Identify the possible threats to the AI system (design faults, technical faults, environmental threats) and the possible resulting consequences.
- Assess the dependency of critical system’s decisions on its stable and reliable behaviour.
- Plan fault tolerance via, e.g., a duplicated system or another parallel system (AI-based or “conventional”).
- Develop a mechanism to evaluate when the AI system has been changed enough to merit a new review of its technical robustness and safety.Develop a mechanism to evaluate when the AI system has been changed enough to merit a new review of its technical robustness and safety.
- Put in place a series of steps to monitor and document the AI system’s accuracy.
- Put in place processes to ensure that the level of accuracy of the AI system to be expected by end-users and/or subjects is properly communicated.

- Put in place a well-defined process to monitor if the AI system is meeting the goals of the intended applications.
- Test whether specific contexts or conditions need to be taken into account to ensure reproducibility.
- Clearly document and operationalize processes for the testing and verification of the reliability and reproducibility of the AI system.
- Define tested failsafe fallback plans to address AI system errors of whatever origin and put governance procedures in place to trigger them.

Privacy and Data Governance

- Consider the privacy and data protection implications of the AI system's non-personal training-data or other processed non-personal data.

Transparency

- Consider explaining the decision adopted or suggested by the AI system to its end users.
- Consider continuously surveying the users to ask them whether they understand the decision(s) of the AI system.
- In case of interactive AI system, consider communicating to users that they are interacting with a machine.

Diversity, non-discrimination and fairness

- Consider diversity and representativeness of end-users and or subjects in the data.
- Identify the subjects that could potentially be (in)directly affected by the AI system, in addition to the (end)-users.
- Your definition of fairness should be commonly used and should be implemented in any phase of the process of setting up the AI system.
- Consider other definitions of fairness before choosing one.
- Consult with the impacted communities about the correct definition of fairness, such as representatives of elderly persons or persons with disabilities.
- Ensure a quantitative analysis or metrics to measure and test the applied definition of fairness.
- You should ensure that the AI system corresponds to the variety of preferences and abilities in society.
- You should assess whether the AI system's user interface is usable by those with special needs or disabilities or those at risk of exclusion.
- You should ensure that Universal Design principles are taken into account during every step of the planning and development process, if applicable.
- You should assess whether the team involved in building the AI system engaged with the possible target end-users and/or subjects.
- You should assess whether there could be groups who might be disproportionately affected by the outcomes of the system.
- You should assess the risk of the possible unfairness of the system onto the end-user's or subject's communities.

Societal and environmental well-being

- Consider the potential positive and negative impacts of your AI system on the environment and establish mechanisms to evaluate this impact.

- Define measures to reduce the environmental impact of your AI system's lifecycle and participate in competitions for the development of AI solutions that tackle this problem.

Accountability

- To facilitate 3rd party auditing can contribute to generate trust in the technology and the product itself. Additionally, it is a strong indication of applying due care in the development and adhering to best practices and industrial standards.
- If AI systems are increasingly used for decision support or for taking decisions themselves, it has to be made sure these systems are fair in their impact on people's lives, that they are in line with values that should not be compromised and able to act accordingly, and that suitable accountability processes can ensure this. Consequently, all conflicts of values, or trade-offs should be well documented and explained
- A risk management process should always include new findings since initial assumptions about the likelihood of occurrence for a specific risk might be faulty and thus, the quantitative risk analysis was not correct and should be revised with the new findings.