AP4AI: accountability principles for artificial intelligence in the internal security domain

AKHGAR, Babak <http://orcid.org/0000-0003-3684-6481>, BAYERL, Petra Saskia <http://orcid.org/0000-0001-6113-9688>, MOUNIER, Grégory, LINDEN, Ruth and WAITES, Ben

AP4AI: Accountability Principles for Artificial Intelligence in the Internal Security Domain

Babak Akhgar
Petra Saskia Bayerl[1]
Centre of Excellence in Terrorism, Resilience, Intelligence and Organized Crime Research (CENTRIC), Sheffield Hallam University, Sheffield

Grégory Mounier
Ruth Linden
Ben Waites
Europol Innovation Lab, The Hague

Abstract
The challenge for internal security practitioners including law enforcement and the justice sector is to determine how to capitalise on the opportunities offered by Artificial Intelligence (AI) and Machine Learning to improve the way investigators, prosecutors, judges or border guards carry out their mission of keeping citizens safe and rendering justice while, at the same time, safeguarding and demonstrating true accountability of AI use towards society. The AP4AI (Accountability Principles for Artificial Intelligence) Project addresses this challenge by offering a global *Framework for AI Accountability for Policing, Security and Justice.* The AP4AI Framework is grounded in empirically verified Accountability Principles for AI as carefully researched and accessible standard, which supports internal security practitioners in implementing AI and Machine Learning tools in an accountable and transparent manner and in line with EU values and fundamental rights. The principles are universal and jurisdiction-neutral to offer guidance for internal security and justice practitioners globally in support of existing governance and accountability mechanisms through self-audit, monitoring and review. This paper presents the project approach as well as current results of the project and their relevance for the internal security domain..

Keywords: Artificial Intelligence, Accountability, Accountability Principles, Internal Security, AP4AI

1 Corresponding author's email: p.s.bayerl@shu.ac.uk.

Introduction

Artificial Intelligence (AI) has become a versatile tool in the arsenal of internal security actors such as law enforcement agencies (LEAs) as it can offer effective means to protect society and save lives, e.g., by improving police performance and efficiencies. It finds application in a wide range of fields such as the pre-processing of unstructured data, machine translation, named entity extraction, image classification, the early detection of unusual patterns (e.g., in the context of cybercrime, child sexual exploitation or counter terrorism challenges), the fast identification of potential threats amongst massive amounts of data points (such as faces in a crowd or the assessments of insider threats) or the deployment of smart autonomous vehicles to secure events or borders. AI can further support strategic forecasting of crime trends. AI capabilities may thus provide crucial support for LEAs across core functions of their work.

At the same time, AI use in the internal security sector also give rise to concerns and fears in some parts of society. Negative societal reactions are often based on a perceived lack of transparency of AI technologies and their usage, as well as fears of biased decision making (e.g., around gender or ethnicity) which may disproportionally affect certain groups in society. Also, a perceived mis- or over-use of AI can threaten the legitimacy of law enforcement efforts. Examples are campaigns such as 'Reclaim Your Face', 'Campaign Against Advanced AI' or even 'Stop Killer Robots'.[2] From a fundamental rights standpoint, scholars and policymakers (EU Commission, 2020) point to potential additional risks of AI use by LEAs, especially to the rights to privacy and data protection, freedom of expression and association, non-discrimination and the rights to an effective remedy and fair trial.

Important legislative processes are ongoing.[3] Yet, practical guidance for internal security practitioners on the best ways to apply evolving norms is still lacking. Also, the question of establishing legitimacy is not made easier by a dearth of governance models focused on AI deployments by internal security practitioners (Babuta et al., 2018).

The solution cannot be to reject AI. Rather solutions are needed which ensure that societal, legal, ethical and operational requirements equally inform and support the potential of AI to enhance LEA and judicial missions and actions. For this to happen, ***a reproducible but adaptive mechanism*** is needed to accomplish and sustain this ambition.

The Accountability for AI (AP4AI) Project develops solutions to help internal security practitioners across the full AI lifecycle, i.e., research, design, assessment, review and revision of AI-led applications as well as the evidencing of appropriate AI usage in case of challenges. The solutions aim to be both internally consistent and externally compatible with the respective jurisdictions of widely differing organisations in the internal security domain, while safeguarding AI accountability in line with EU values and fundamental rights. To this end, AP4AI offers a Framework for security and justice practitioners which integrates central indefeasible tenets that, if adopted, will provide practitioners, legal and ethical experts as well as citizens with a high degree of reassurance and redress. In this way, the AP4AI Framework will allow practitioners to capitalise on available AI capabilities, whilst demonstrating meaningful accountability towards society and oversight bodies.

AP4AI objectives and products

AP4AI will deliver concrete products to support internal security practitioners in their deployment of AI:

- A robust set of agreed and validated Accountability Principles for AI, which integrate practitioners' as well as citizens' positions on AI;
- Implementation guidelines and toolkit including supporting software tool to give practitioners and oversight bodies practical, actionable compliance and assessment tools to assess and review AI capabilities from design to deployment;
- Training and policy briefings for the internal security community and oversight bodies on how to apply the AP4AI Framework, as well as broader insights from AP4AI research;

2 Reclaimyourface.eu; https://twitter.com/againstASI; https://www.stopkillerrobots.org

3 The European Commission launched a new 10-year economic strategy, called Europe 2020, to boost European economy and promote a smart, sustainable and inclusive growth, based on a greater coordination of national and European economic policy. One of the main priorities for the EU is to create "A Europe fit for digital age", where the development of trustworthy AI plays a crucial role.

- A set of reports and documentation as reference for the internal security and judiciary community, as well as oversight bodies and the public;

- Engagement with national and EU-funded projects to inform ongoing and future research efforts on AI with respect to AI Accountability needs and applications.

AP4AI partners

The AP4AI Project is jointly conducted by CENTRIC and Europol and supported by Eurojust, the EU Agency for Asylum (EUAA), the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) and the EU Agency for Police Training (CEPOL) and advised by the EU Agency for Fundamental Rights (FRA) in the framework of the EU Innovation Hub for Internal Security.

Why Accountability as guiding principle?

AP4AI focuses on accountability as a guiding standard under the premise that in the field of security and justice, functional AI Accountability is as important as the technology itself. Currently no known efforts exist that address accountability as a process that manages to integrate the complexities of AI applications in the law enforcement and justice sector. There is thus a profound ***accountability gap*** with respect to societal, organisational, legal and ethical aspects to understand and sustainably manage the complexities of AI in the internal security sector in a way that affords monitoring ***and*** enforcement towards human-centred AI.

We argue for the primacy of accountability as guiding framework for AI use in the internal security domain as it is the only concept that binds organisations to enforceable obligations and thus provides a foundation that has actionable procedures at its core. The notion of accountability therefore offers vital benefits compared to other instruments and frameworks.

Accountability comprises in itself the three aspects of monitoring, justification and enforcement (Schedler, 1999), and in a legal perspective is defined as the "acknowledgement and assumption of responsibility for actions, decisions, and their consequences" (Thomas Reuters Practical Law, 2021). It thus has at its very core the notion of negotiation across disparate legitimate interests, the observation of action and consequences and the possibility for redress, learning and improvement. The acknowledgement of disparate legitimate interests is of particular relevance for AI capabilities in the internal security domain, where safeguarding one section of society may potentially infringe on rights and freedoms of others.

Accountability is a practical mechanism as it is bound to enforceable obligations and thus actionable. Using AI Accountability as framework hence ensures that legitimate interests (as well as concerns, fears and hopes) of stakeholders are factored in and engaged with throughout the full decision-making process about AI capabilities in the internal security domain. Using accountability as primary lens reinforces an organisation's responsibility to act in accordance with the legitimate expectations of diverse stakeholders and the acceptance of the consequences – legal or otherwise – if they fail to do so. In this context liability, or rather 'answerability', is the basis for meaningful accountability as it creates a foundation for the creators and users of AI to ensure that their products are not only legally fit for the legitimate purpose(s) for which they are deployed but also invite scrutiny and challenge and accept the consequences of using AI in ways that communities may find morally or ethically unacceptable. There is further the responsibility to ensure the avoidance of misuse and malicious activity in whatever form by both the relevant security practitioners and their contractors, partners and agents.

AP4AI approach to accountability

AP4AI's approach to accountability is shaped by two tenets: firstly, *accountability as a process;* secondly, *accountability as a network of mutual obligations.*

1. ***Accountability as a process:*** Accountability can be defined as a responsibility for the fulfilment of obligations towards one or multiple stakeholders, in the understanding that not meeting these obligations will lead to consequences. To create accountability requires several steps from defining what someone (a person, organisation or group) is accountable for and to whom to setting clear parameters by which to measure fulfilment of obligations and linking them to consequences, monitoring progress, dis-

pensing consequences and redressing divergences. Any divergences need to be identified as early as possible, as scholars have rightly claimed that relying on "the big red button" as emergency stop is insufficient (Arnold & Scheutz, 2018). AP4AI, therefore, builds its AI-focused accountability process as procedure parallel to the AI system lifecycle starting from initial idea to the potential decisions for the system's retirement as well as the need to evidence appropriate use. This process perspective ensures that accountability is not a 'one-off exercise' but an ongoing effort of justification, monitoring and enforcement. In this way, accountability becomes solidly embedded into internal security applications of AI from start to end.

2. *Accountability as a network of mutual obligations:* Accountability is a relational concept in that obligations are directed towards particular stakeholders or groups. In a security context, discussions of accountability tend to be focused on police accountability towards citizens. This is insufficient given the complexity and the scale of effects security applications of AI have on individuals, communities, societies and organisations (LEAs and others) as well as on local, national and international levels. AP4AI acknowledges this complexity by extending accountability into a network of mutual obligations. For instance, the ethical and lawful development of AI will need to take into account not only a legitimate expectation that data will be provided by internal security actors as part of the latter's accountability towards civil society, but also situations whereby LEAs dependent upon citizens' data. The creation of such relationships may well carry a legitimate expectation on behalf of internal security actors that citizens will attract some degree of accountability for the data they contribute. Accountability obligations do therefore not only flow from internal security actors to citizens but also the other way around. In the same way, LEA organisations and their personnel have mutual obligations (for example, safeguarding officers' long-term employability on the one hand and adherence to fair procedures in decision-making on the other).

The primary challenge to the implementation of AI accountability in the internal security domain is that there is little clarity on what AI Accountability means in a societal, legal, ethical and operational sense. While organisational accountability in policing is a widely discussed concept (e.g., UNODC, 2011), at present no firm definition of accountability in the context of AI in the internal security domain exists. Also, currently no clear legal definition of 'accountability' in the EU jurisprudence (where it is rather a principle as evident in the GDPR) is available. Unsolved remains further how accountabilities interrelate throughout the process of an AI system's lifecycle including the development of disparate AI tools, applications and platforms for practitioners.

AP4AI offers a definition of AI Accountability by putting forward 12 constituting principles that together describe the scope and content of AI Accountability in the internal security domain.

Defining AI Accountability in the internal security domain: The AP4AI Principles

AP4AI puts forward 12 Accountability Principles which define the requirements that need to be fulfilled to assure Accountability for AI utilisation in the internal security domain. The 12 Principles are the foundation on which all other AP4AI activities and solutions are built. The following list provides the overview of the 12 Principles:

1. ***Legality:*** Legality means that all aspects of the use of AI should be lawful and governed by formal, promulgated rules. It extends to all those involved in building, developing and operating AI systems for use in a criminal justice context. Where any gaps in the law exist, the protection and promotion of fundamental rights and freedoms should prevail.

2. ***Universality:*** Universality provides that all relevant aspects of AI deployments within the internal security community are covered through the accountability process. This includes all processes, including design, development and supply, domains, aspects of police mission, AI systems, stages in the AI lifecycle or usage purposes.

3. ***Pluralism:*** Pluralism ensures that oversight involves all relevant stakeholders engaged in and affected by a specific AI deployment. Pluralism avoids homogeneity and thus a tendency or perception for the regulators to take a one-sided approach.

4. ***Transparency:*** Transparency involves making available clear, accurate and meaningful information about AI processes and specific deployment pertinent for assessing and enforcing accountability. This represents full and frank disclosure in the interests of promoting public trust and confidence by enabling those directly and indirectly affected, as well as the wider public, to make informed judgments and accurate risk assessments.

5. ***Independence:*** Independence refers to the status of competent authorities performing oversight functions in respect of achieving accountability. This applies in a personal, political, financial and functional way, with no conflict of interest in any sense.

6. ***Commitment to Robust Evidence:*** Evidence in this sense refers to documented records or other proof of compliance measures in respect of legal and other formal obligations pertaining to the use of AI in an internal security context. This principle demonstrates as well as facilitates accountability by way of requiring detailed, accurate and up to date record-keeping in respect of all aspects of AI use.

7. ***Enforceability and Redress:*** Enforceability and redress requires mechanisms to be established that facilitate independent and effective oversight in respect of the use of AI in the internal security community, as well as mechanisms to respond appropriately to instances of non-compliance with applicable obligations by those deploying AI in a criminal justice context.

8. ***Compellability:*** Compellability refers to the need for competent authorities and oversight bodies to compel those deploying or utilizing AI in the internal security community to provide access to necessary information, systems or individuals by creating formal obligations in this regard.

9. ***Explainability:*** Explainability requires those using AI to ensure that information about this use is provided in a meaningful way that is accessible and easily understood by the relevant participants/audiences.

10. ***Constructiveness:*** Constructiveness embraces the idea of participating in a constructive dialogue with relevant stakeholders involved in the use of AI and other interested parties, by engaging with and responding positively to various inputs. This may include considering different perspectives, discussing challenges and recognising that certain types of disagreements can lead to beneficial solutions for those involved.

11. Conduct: Conduct governs how individuals and organisations will conduct themselves in undertaking their respective tasks and relates to sector-specific principles, professional standards and expected behaviours relating to conduct within a role, which incorporate integrity and ethical considerations.

12. ***Learning Organisation:*** Learning Organisation promotes the willingness and ability of organisations and people to improve AI through the application of (new) knowledge and insights. It applies to people and organisations involved in the design, use and oversight of AI in the internal security domain and includes the modification and improvement of systems, structures, practices, processes, knowledge and resources, as well as the development of professional doctrine and agreed standards.

Together the above AP4AI Principles constitute a universal, empirically validated Framework for AI in the law enforcement and justice sector to fundamentally assess and enforce legitimate and acceptable usage of AI by the internal security community.

Development of the AP4AI Principles

The principles were developed in an exploratory 'bottom-up' manner. This means principles were identified and refined by engaging directly and intensely with the people who are either using, designing, regulating or are affected by AI in an internal security context, i.e., practitioners in the security, policing and justice domain, oversight bodies, law makers, industry, researchers and research institutions, as well as citizens.

The project is conducted in three cycles which are implemented as consecutive steps for the exploration, integration and validation of findings. The sequential approach was chosen to ensure the robust development and validation of the AP4AI Framework and products. The three cycles are:

- ***Cycle 1 – Development of the AP4AI Principles (completed):*** The first cycle consisted of two activities: (a) a review of existing frameworks aiming to guide or

regulate AI and (b) expert consultations with subject-matter experts from law enforcement, justice, legal, fundamental rights, ethical and technical fields identified by the AP4AI partners. Results of the expert consultations are reported in the ***AP4AI Summary Report on Expert Consultations*** (Akhgar et al., 2022a).

- ***Cycle 2 – Citizen consultation for validation and refinement of the Principles (completed):*** An online consultation was conducted in 30 countries (all 27 EU members states, UK, USA and Australia, resulting in answers from 6,774 participants) to collect citizen input on the AI Accountability Principles developed in Cycle 1, as well as insights into possible accountability mechanisms. A blueprint was published on the basis of the results, including preliminary results of the citizen consultation (Akhgar et al., 2022b).

- ***Cycle 3 – Expert consultation for validation and contextualisation of the AP4AI Framework (ongoing):*** The AP4AI Framework goes through continued validations by subject matter experts using structured feedback collection, hands-on implementation workshops, as well as case creation for the operationalisation of the Framework into practice.

AP4AI was from the start conceptualised with an international focus. The international focus is required as AI use in the internal security domain – whether at practitioner or citizen level – is strongly affected by the national contexts in which AI capabilities are deployed. The project has so far brought together expertise from experts and citizens across 32 countries.

The chosen methodology, which integrates security, legal, ethical as well as citizens' perspectives by design, allows AP4AI to develop a robust and application-focused Framework that offers a step-change in the application of AI by the internal security community.

High-level view on AP4AI implementation

From the outset, the AP4AI Project aimed at translating the Accountability Principles (as the conceptual representation of AI Accountability requirements) into actionable steps and processes in support of internal security practitioners. This translation step into guidance for practical application is the second core element of the AP4AI Framework. To this end, each of the 12 Principles has been contextualised for AI deployments within the internal security domain, providing legal and practical consideration, as well as examples (see section on ***'Principle-specific guidance'***). The tangible realisation of the Principles is demonstrated through the provision of an implementation container – the ***AI Accountability Agreement*** – which will serve as a universal mechanism for the implementation of the principles. It further offers concrete accountability narratives that will permit flexibility for local implementations at the organisational level.

AI Accountability Agreement (AAA)

AP4AI advocates for an ***AI Accountability Agreement (AAA)*** that specifies formal and implementable processes for the implementation of the Accountability Principles for different applications of AI within the internal security domain.

An AI Accountability Agreement (AAA) should be viewed as a social contract underpinned by legal obligations between internal security organisations and its stakeholders including citizens, oversight bodies, suppliers, consumers of AI services (e.g., other agencies) and others, as applicable. The AAA should address all AP4AI Principles and their realisation in an operational setting for the specific application of AI. The AAA can thus be understood as an implementation container or reference architecture, which drives the implementation of the 12 Principles in a practical and operational setting within internal security organisations. It hence serves as a mechanism to bring the abstract nature of the Principles into the implementable environment of internal security organisations and their wider ecosystem (e.g., oversight bodies and government agencies).

Every AAA should clearly set out and formalise the following four steps:

1. The accountability must-haves (non-negotiables), should-haves and could-haves within the specific application of AI;

2. Definition of who will be Responsible, Accountable, Consulted and Informed (RACI index) in relation to each of the AP4AI Principles for each application of AI and who has been Consulted and Informed about the purpose and development of the AI application (with a summary of what they have said);

3. The materiality thresholds and tolerances to allow for practical variance (dates, changes in personnel, etc.), the range of acceptability and for assessing the proportionality of disclosure, consultation, and publishing of information;

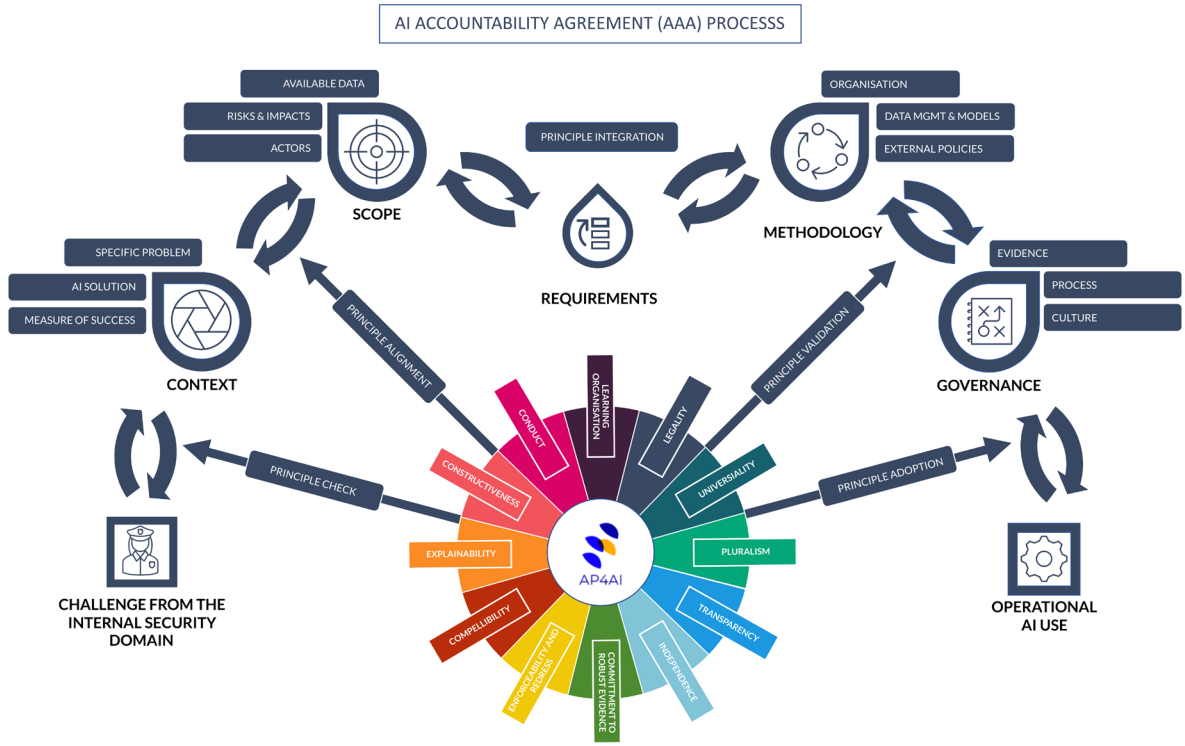
4. The process that must be followed before making any variation to the specific application of AI.

In order to pave the way for the implementation of the 12 Accountability Principles, AP4AI utilises the concept of Materiality. ***Materiality*** is an assessment of the relative impact that something may have on accountability within the context of an application of AI in the internal security ecosystem. Materiality allows to set ***materiality thresholds***, i.e., impacts below which AI Accountability processes may be required only to a limited extend or not at all. Material thresholds acknowledge that the material importance and impact of a specific AI capability or application will very much depend on the nature of the AI project (e.g., automating the logistics of ordering police uniforms versus calculating potential re-offending of a person to inform a bail decision).

The AAA is designed to be created and validated prior to any programme of work that encompasses the application of AI. Each application of AI involves one or more stages of the AI lifecycle: scoping, planning, research, design, development, procurement, customisation, deployment, modification, maintenance and decommissioning. It can also be employed for evidencing the appropriate use of AI capabilities in case of challenges.

To achieve this, the AAA must include, as a baseline, the four components: *context, scope, methodology,* and *accountability governance*. Each phase in the AAA should adopt the application of all 12 Principles and use them as a milestone to progress to the next stage. Figure 1 gives an overview of the stages involved in the development of an AI Accountability Agreement.

Figure 1. Stages of development for an AI Accountability Agreement (source: Akhgar et al., 2022b)



Principle-specific guidance

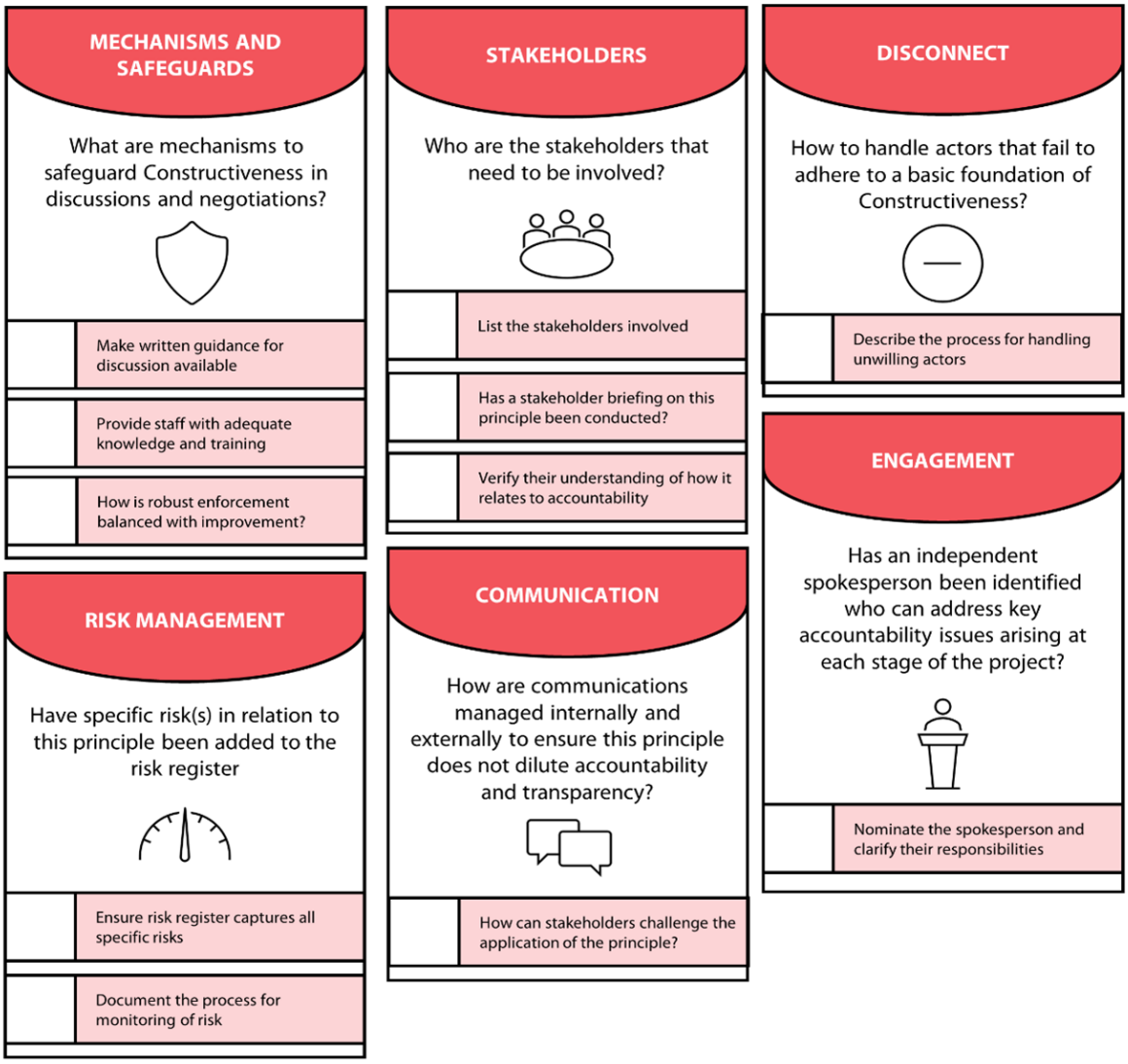
Next to the AAA as overarching mechanism, AP4AI further provides structured, semantic representation guidance on each of the individual Accountability Principles. The template used to present each principle consists of eight elements which collectively provide the core requirements for its implementation. The template is designed in a way that it can be extended and refined throughout the AP4AI Project yet maintain its conceptual foundation which is grounded in the evidence-based research conducted previously as well as the input from expert and citizen consultations described above. The granularity (e.g., set of purposeful questions) and visual representation of the 'implementation guide' for each principle supports the development of practical guidance and application mechanisms such as a dedicated software tool.

In detail, the guide consists of the following elements for each Principle:

- ***Name:*** principle name
- ***Meaning:*** provides the principle's definition contextualised for AI and the internal security domain
- ***Materiality threshold:*** offers an assessment of the relative impact that something may have on accountability within AI development or utilisation
- ***Examples of applicable law:*** lists examples of applicable law pertinent to AI Accountability in the internal security domain
- ***Note on Human Right Impact Assessment (HRIA)***: provides an initial direction for HRIAs and alerts the reader about the pivotal role of HRIAs in the context of AI Accountability Principles
- ***Note on Data Protection Impact Assessment (DPIA, where applicable)***: alerts the reader to legal and ethical requirements of conducting a DPIA and, where applicable, a Privacy Impact Assessment (PIA)
- ***Implementation guide:*** identifies the processes, activities, tasks, documentations, assessments, actions and communication needed for the realisation of the principle
- ***Operational considerations:*** provides clarification and further consideration about implementation of the principles for the operational environment

Figure 2 provides an example of the implementation guide and operational considerations for the principle "Constructiveness".

Figure 2. Illustration of the implementation guide and operational considerations for the Constructiveness principle (source: Akhgar et al., 2022b)



Operational considerations: It may be useful to pre-emptively document how particular issues will be dealt with, for example, who is accountable for fixing critical flaws in the AI system should they occur. Security practitioners and oversight bodies should have mechanisms and resources in place to ensure a constructive outcome is given in a reasonable time period.

Next steps and outlook

The main aim of the AP4AI Project is to offer concrete and practical tools that support LEAs and justice practitioners in assessing and evidencing the accountability of current and future AI capabilities as well as to enrich ongoing policy and legal discussions.

Our currently ongoing work focuses on:

- Further validation and instantiation of the AI Accountability Agreement using real examples and challenges of internal security practitioners;
- Extension of use cases and application scenarios for AI deployments (most critically CSE/CSEM, cyber-dependent crime, serious and organised crime activities including cross-border issues, harmful internet content such as terrorist generated internet content, protection of public spaces and communities, terrorism related offences, financial crime, procurement of AI solutions by internal security practitioners, research and development for AI either by the internal security actors or a third party intended to create the solution to be deployed for the internal security domain);

- Development of a software application as a supporting mechanism for the implementation of AP4AI;
- Input into ongoing policy and legal discussions.

Conclusions

The AP4AI Project is guided by an enabling philosophy. The fundamental premise which drives AP4AI and its outcomes is that AI is a critical and strategic asset for internal security practitioners. It thus aims to support internal security practitioners in the appropriate and legitimate management of AI capabilities, both before and during AI deployments.

The AP4AI Framework is specifically designed for security and justice practitioners, including LEAs, and offers validated AI Accountability Principles as a fundamental mechanism to assess and enforce legitimate and acceptable usage of AI. The AP4AI Project has the ambition to become a globally known standard of quality for the research, design, development and deployment of accountable AI use in the internal security domain.

The core foundation of the AP4AI Project is that of policing by consent whereby the burden of trust as a mutual obligation between police and society is enshrined within the notion of accountability. The challenge for internal security practitioners is how to capitalise on new technological capabilities that derive from AI in response to societal expectation and demands while, at the same time, demonstrating true accountability and compliance, assuaging societal concern at the use of advanced technology such as AI and automated processing. AP4AI aims to offer solutions to this complex issue for organisations within the security and justice sector.

Acknowledgements and funding

We are grateful to the experts and citizens, who have generously given their time and input to AP4AI. No specific funding from external funding agencies or funding bodies has been received for the project. The research outcomes, the opinions, critical reflections, conclusions and recommendations do not necessarily reflect the views of authors' organisations. The project received ethics approval by the university ethics board of Sheffield Hallam University, where CENTRIC is located as academic lead of the AP4AI Project.

References

- Akhgar, B., Bayerl, P.S., Bailey, K., Dennis, R., Heyes, S., Lyle, A., Raven, A., Sampson, F., & Gercke, M. (2022a) AP4AI Report on Expert Consultations.
  Available at: https://www.ap4ai.eu/node/6
- Akhgar, B., Bayerl, P.S., Bailey, K., Dennis, R., Gibson, H., Heyes, S., Lyle, A., Raven, A., & Sampson, F. (2022b) AP4AI Framework Blueprint.
  Available at: https://www.ap4ai.eu/node/14
- Arnold, T. & Scheutz, M. (2018) 'The "big red button" is too late: An alternative model for the ethical evaluation of AI systems', Ethics and Information Technology, 20, pp. 59–69. https://doi.org/10.1007/s10676-018-9447-7
- Babuta, A., Oswald, M. & Rinik, C. (2018) 'Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges', Whitehall Report 3-18, RUSI.
- EU Commission. (2020) White Paper on Artificial Intelligence: A European Approach to Excellence and Trust.
  Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
- Schedler, A. (1999) 'Conceptualizing Accountability', in: Schedler et al. (eds), The Self-restraining State: Power and Accountability in New Democracies (pp. 13-28).
- Thomas Reuters Practical Law (2021) Accountability Principles.
  Available at: https://uk.practicallaw.thomsonreuters.com/w-014-8164
- United Nations Office on Drugs and Crime (UNODC). (2011) Handbook on Police Accountability, Oversight and Integrity. Criminal Justice Handbook Series. United Nations Publishing, New York.
- More information
  Project website: https://www.ap4ai.eu
  Twitter: @ap4ai_project