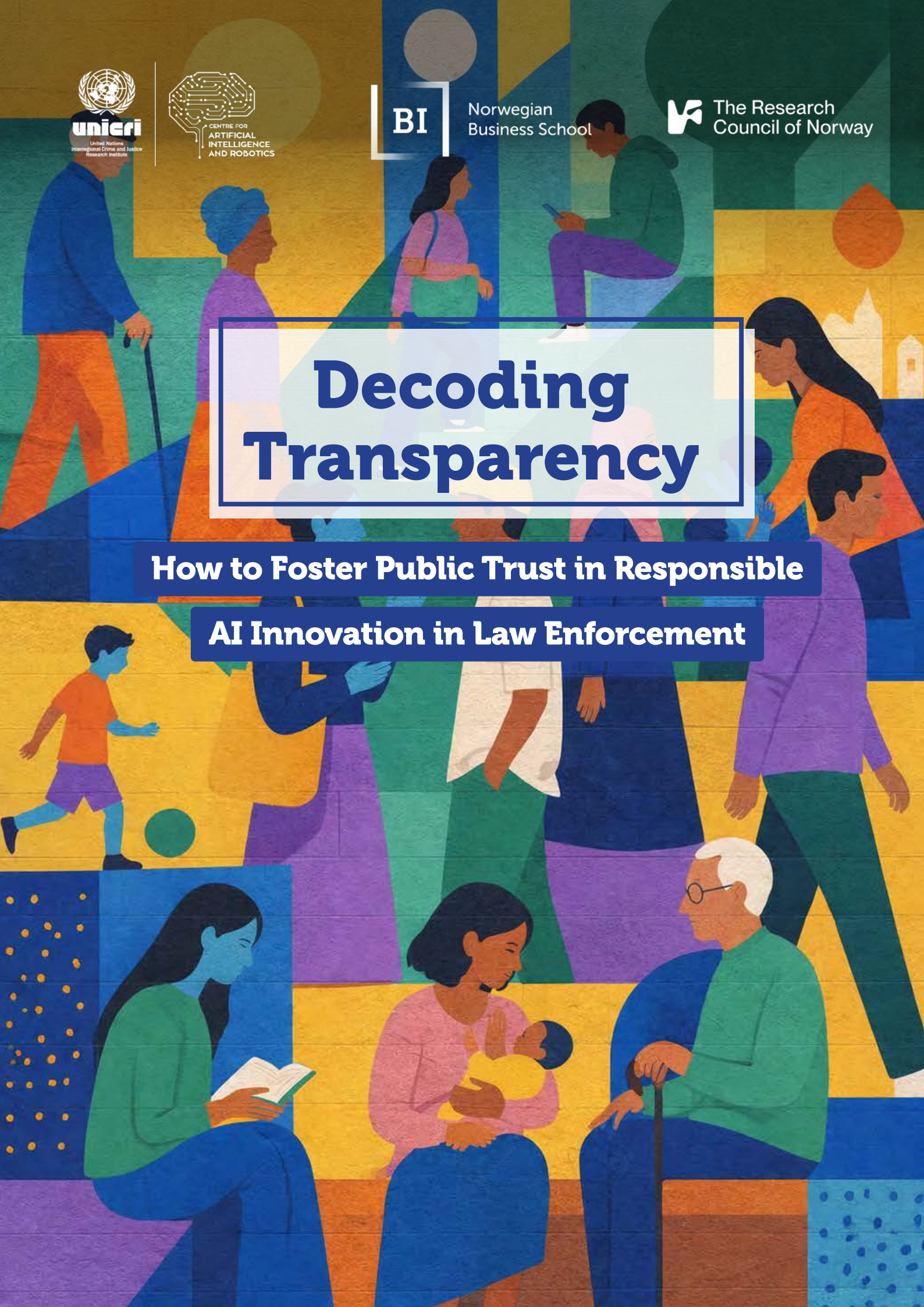

unicri
United Nations Interregional Crime and Justice Research Institute
CENTRE FOR ARTIFICIAL INTELLIGENCE AND ROBOTICS
BI Norwegian Business School
The Research Council of Norway
Decoding Transparency
How to Foster Public Trust in Responsible AI Innovation in Law Enforcement

United Nations Interregional Crime and Justice Research Institute

CENTRE FOR ARTIFICIAL INTELLIGENCE AND ROBOTICS

BI Norwegian Business School

The Research Council of Norway

Decoding Transparency

How to Foster Public Trust in Responsible AI Innovation in Law Enforcement

Table of Contents

Executive summary

To achieve legitimacy and effectiveness, law enforcement demands public trust – a requirement which grows in importance when law enforcement agencies adopt AI systems. Public attitudes towards AI in policing remain cautious, and trust in law enforcement agencies can strongly influence whether they agree to new technologies. Therefore, it is up to law enforcement agencies to act effectively and, above all, fairly when making decisions about whether, when and how to adopt and implement AI systems.

In particular, they need to exhibit transparency – that is, clear, open communication about which AI systems they are using, for which purposes and according to what rules and guidelines. In addition to improving trust in how law enforcement agencies use AI systems, transparency is essential to safeguarding human rights, scrutiny and system quality, as well as encouraging sustainable adoption. Yet transparency is commonly challenged by organizational cultures, operational confidentiality, vendor restrictions and limited resources. To achieve and ensure transparency, indispensable for maintaining public confidence and institutional legitimacy, law enforcement agencies using AI for public safety should:

- Act responsibly and transparently when introducing AI systems, ensuring decisions are fair, unbiased, and protective of human rights.
- Invest resources in transparency, with the recognition that doing so can strengthen legitimacy, innovation and public confidence.
- Seek stakeholder perspectives through surveys, consultations and ongoing feedback to tailor transparency efforts to community needs.
- Build trust over time, while acknowledging that trust is fragile and requires sustained, reliable and consistent behaviour across all interactions.
- Start transparency efforts early, communicating before, during and after AI adoption, and offer proactive updates to prevent misinformation.
- Communicate positive, truthful narratives about how AI systems support public safety while also openly addressing risks and disclosing safeguards.
- Acknowledge and address mistakes through accountability, corrective action and reliance on oversight bodies.
- Clarify what cannot be disclosed and why, respecting operational secrecy needs while still sharing purposes, rules and safeguards.
- Embed transparency clauses in vendor contracts.
- Respond quickly and accurately, prepare clear answers in advance, ensure informed representatives address public concerns and continuously refine transparency practices.

Because transparency is inherently a two-way process, it requires strong, clear communication from law enforcement agencies about their use of AI systems, combined with effective public engagement that allows communities to contribute and shape how law enforcement uses AI systems.

First, by communicating openly, consistently and thoughtfully, law enforcement can strengthen trust, promote responsible AI innovation, and ensure that communities feel informed, respected and involved. Some practical recommendations for effective, clear communication about the use of AI systems include the following:

- **Clearly disclose uses of AI systems.** Explain how they serve the public interest and provide accessible information about governance, oversight, risk mitigation, procurement and accountability mechanisms.
- **Tailor communication efforts to audiences**. General audiences need simple, plain-language explanations of purpose, benefits, risks, data use and rights. Expert audiences require more technical details, such as system performance metrics, data sources, safeguards and oversight processes.
- **Engage in early communication, well before AI deployment, and continue throughout the AI system's life cycle.** Long-term, proactive communication strategies and consistent information sharing help prevent misinformation and build durable trust.
- **Exploit different communications channels** to reach different audiences and avoid excluding any group, including websites, printed materials, signage, social media, broadcast media, community forums and visible system identification on sites.
- **Use simple, clear language.** Avoid overwhelming details, acknowledge concerns and provide layered information to help audiences learn at their own pace.
- **Communicate in an engaging, human manner,** using visual tools, real-world examples, interactive formats and clear options for follow-up, to make AI systems more understandable and approachable.

Second, public engagement is an equally important, core pillar of trust. Sharing information outward alone is insufficient; law enforcement agencies must gather information by listening, responding to and meaningfully involving communities. Engagement must be sincere, inclusive and grounded in the understanding that they earn trust through dialogue. Practical recommendations for fostering effective public engagement include the following:

- **Ensure the engagement is meaningful,** by actively listening to stakeholder feedback, explaining when and why certain suggestions cannot be implemented, remaining open to changing course and adopting a self-critical stance that welcomes co-creation with communities.
- **Involve the entire organization.** All law enforcement personnel should have basic training in dialogue, bias awareness and community interaction.

- **Engage inclusively and broadly,** across all levels of government and with all stakeholder groups, including technology providers, civil society organizations, academics, intermediaries, mediators and communities directly affected by AI systems.
- **Prioritize vulnerable and underrepresented communities.** Incorporate their perspectives, maintain continuous dialogue, establish safe feedback mechanisms, and communicate clearly about safeguards against profiling, mass surveillance and systemic bias. Early engagement with distrustful or vulnerable groups is crucial to prevent further alienation and reinforce safeguards against discrimination.
- **Use diverse formats and modalities for engagement,** from informal community meetings and coffee chats to structured forums, expert roundtables, closed-door sessions and hands-on demonstrations.
- **Gather feedback through inclusive channels.** Input may be written, oral, digital or in community-specific formats, and invitations to provide feedback should be widely disseminated across both physical and digital platforms.
- **Start small and build trust progressively.** Small expert groups might create safe spaces for dialogue. Neutral settings can foster candid conversations and constructive negotiation about sensitive topics.
- **Provide education and real-world exposure** through public information sessions, training workshops, community forums and station visits that demonstrate how AI systems operate in practice and how they support public safety.
- **Strengthen community-level structures and platforms** to encourage recurring dialogue, accountability and representation.
- **Ground all engagement in relatability, respect and accessibility.** Work with trusted local actors, address concerns empathetically, recognize cultural dynamics, and ensure that engagement practices reduce fears, tensions and exclusion.

Introduction

Public trust is the bedrock for legitimate, effective law enforcement. Contemporary law enforcement, grounded in the principle of *policing by consent* and characterized by approaches such as *community-oriented policing,* relies on public approval and cooperation to prevent and respond to crime.[1] Trust drives such cooperation, yet it is remarkably hard to gain and sustain.

To encourage it, transparency is essential, especially for law enforcement agencies seeking to introduce artificial intelligence (AI) to their practices. Although AI systems already support various law enforcement tasks, reflecting agencies' efforts to enhance their efficiency and strengthen resource allocation,[2] the pairing of AI with law enforcement remains uniquely challenging. Issues such as algorithmic bias and expanded surveillance capabilities pose inherent human rights risks and raise concern among the public.[3] In such a setting, transparency – meaning the extent to which agencies disclose relevant information about the decision-making processes, procedures, performance and outcomes related to their AI innovation endeavours –[4] can be a crucial enabler of appropriate governance, scrutiny and accountability.[5, 6]

The need for openness is especially critical today, considering evidence from a global survey (with around 34,000 respondents from 28 countries) that 70% of people worry that leaders and institutions intentionally mislead the public and 60% report moderate to high grievances towards institutions.[7] Beyond such general distrust, public perceptions of AI are even more concerning. Most people indicate an unwillingness to trust AI systems, particularly in advanced economies, and trust levels appear to be declining over time (e.g., by 17% between 2022 and 2025).[8] Yet AI perceptions also tend to depend on the context, and people's understanding of benefit–risk trade-offs seems limited, resulting in varied, nuanced attitudes towards AI use across different public sector settings. The same underlying technology might be rejected in some cases but accepted in others, depending on the public service for which it is deployed.[9,10]

1 United Nations Department of Peacekeeping Operations Department of Field Support. (2018). Manual community-oriented policing in united nations peace operations. Ref. 2018.04. Accessible at: https://police.un.org/sites/default/files/manual-community-oriented-poliicing.pdf

2 UNICRI and INTERPOL. (revised February 2024). Toolkit for responsible AI innovation in law enforcement: Introduction to responsible AI innovation. Accessible at: https://ai-lawenforcement.org/sites/default/files/2025-03/Intro_Resp_AI_Innovation_Mar25.pdf

3 UNICRI. (2024). Not just another tool: Public perceptions on police use of artificial intelligence. Accessible at: https://unicri.org/Publications/Public-Perceptions-AI-Law-Enforcement

4 Albert Meijer. (2013). Understanding the complex dynamics of transparency. *Public Administration Review*, *73*(3), 429-439. Accessible at: https://dspace.library.uu.nl/bitstream/handle/1874/407242/puar.12032.pdf Stephan G. Grimmelikhuijsen & Erik W. Welch. (2012). Developing and testing a theoretical framework for computer-mediated transparency of local governments. *Public Administration Review*, *72*(4), 562-571. Accessible at: https://dspace.library.uu.nl/bitstream/1874/252024/1/GrimmelikhuijsenDevelopingandTesting.pdf

5 Tom R. Tyler. (2006). *Why people obey the law*. Princeton University Press. Accessible at: https://www.researchgate.net/publication/220011500_Why_do_People_Obey_the_Law

6 Tero Erkkilä. (2020, May 29). Transparency in public administration. In *Oxford research encyclopedia of politics.* Oxford University Press. Accessible at: https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-1404.

7 Richard Edelman. (2022). 2022 Edelman Trust Barometer: The cycle of distrust. Edelman. Accessible at: https://www.edelman.com/trust/2022-trust-barometer

8 The study adopted the International Monetary Fund's (IMF) classification of advanced and emerging economies. The advanced economies surveyed were Australia, Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Netherlands, New Zealand, Norway, Portugal, Republic of Korea, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom. The emerging economies surveyed are Argentina, Brazil, Chile, China, Colombia, Costa Rica, Egypt, Hungary, India, Mexico, Nigeria, Poland, Romania, Saudi Arabia, South Africa, Türkiye, and the United Arab Emirates. Nicole Gillespie, Steve Lockey, Alexandria Macdade, Tabi Ward & Gerard Hassed. (2025). Trust, attitudes and use of artificial intelligence: A global study 2025. The University of Melbourne and KPMG. Accessible at: https://mbs.edu/-/media/PDF/Research/Trust_in_AI_Report.pdf?rev=0ee82285b2b0439bba524dbddc58214a

9 Matilda Dorotic, Emanuela Stagno & Luk Warlop. (2024). AI on the street: Context-dependent responses to artificial intelligence. *International Journal of Research in Marketing, 41*(1), 113-137. Accessible at: https://doi.org/10.1016/j.ijresmar.2023.08.010

10 Roshni Modhvadia, Tvesha Sippy, Octavia Field Reid & Helen Margetts. (2025). How do people feel about AI?. Ada Lovelace Institute and The Alan Turing Institute. Accessible at: https://attitudestoai.uk/

When it comes to law enforcement agencies' uses of AI, the way they engage with and communicate about the systems can powerfully shape public attitudes. A comprehensive survey of public perceptions of AI uses by law enforcement, conducted by the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the International Criminal Police Organization (INTERPOL) revealed a correlation between trust in authorities and AI acceptance. In addition, acceptance increased if safeguards were in place, and human oversight and strong legal frameworks emerged as essential to public confidence. Yet the survey participants consistently cited a lack of information about how their local law enforcement agencies were using AI.[11] This gap may stem, at least in part, from a lack of guidance regarding how to devise transparency requirements. Which information should law enforcement agencies convey to the public to assure them of the trustworthiness of AI systems and the entities that design, deploy or operate them?

Answering this question and bridging the public perception gap represent a governance imperative. Any innovation might be rejected if it is not presented with openness, respect for human rights and responsible practices. For example, controversial uses of AI can undermine its promise to enhance crime prevention and investigation efforts, erode the public's confidence in law enforcement agencies and ultimately compromise the pursuit of justice. Successful endeavours require public cooperation. Therefore, deploying opaque or harmful AI systems risks fostering misunderstanding and damaging the very relationships required by effective policing. In an attempt to avoid such failures and facilitate success, this report offers comprehensive guidance to help law enforcement decision makers and related actors build and maintain public confidence, through transparency, during their responsible implementation of AI systems to enhance public safety.

About this report

This report is the result of joint research conducted by UNICRI, through its Centre for Artificial Intelligence and Robotics, and BI Norwegian Business School (BI), under the project *AI4Citizens: Legal, Ethical, and Societal Considerations of Implementing AI Systems for Anonymized Crowd Monitoring to Improve Public Safety*. It received financial support from the Norwegian Research Council. It builds on UNICRI's extensive research into responsible AI innovation, including the *Toolkit for Responsible AI Innovation in Law Enforcement (AI Toolkit)* and the *AI-POL: Advancing Innovation, Governance and Responsible AI in Law Enforcement*.[12] Launched in 2024 by UNICRI and INTERPOL, with funding from the European Union, the AI Toolkit guides law enforcement agencies worldwide on how to integrate AI systems responsibly into their work. AI-POL is a joint initiative of UNICRI and INTERPOL, funded by the European Union, which seeks to translate the guidance in the AI Toolkit into practical support for participating agencies.

11 UNICRI. (2024).

12 UNICRI and INTERPOL. (Revised February 2024). Toolkit for Responsible AI Innovation in Law Enforcement: README file. Accessible at: https://ai-lawenforcement.org/sites/default/files/2025-03/README_File_Mar25.pdf

Overview and objective

To inform decision makers in law enforcement and other public safety institutions about effective approaches to fostering public trust, through enhanced transparency surrounding responsible of AI innovation, this report contains three focused chapters.

First, it outlines key drivers of public trust in law enforcement, including transparency, which is both a principle and an organizational attitude (> CHAPTER 1). Second, this report considers two dimensions of transparency that operate in tandem to enable law enforcement agencies to build and maintain public confidence:

Communication: providing clear, accessible information to the public about AI use (> CHAPTER 2).

Public engagement: establishing meaningful, two-way dialogue with communities, including vulnerable groups (> CHAPTER 3).

Each chapter includes a conceptual overview of the topics and a set of practical, action-oriented recommendations to support implementation.

Methodology

The research relied on six main methods:

1. **Desk-based research.** A comprehensive literature review supported all stages of this research and ensured contextual grounding and analytical relevance.
2. **Analysis of a hypothetical use case.** UNICRI analysed an AI system designed for crowd monitoring and anomaly detection in public spaces. With a responsible AI innovation perspective and building on technical work performed for the broader project *AI4Citizens: Responsible AI for Citizen Safety in Future Smart Cities*,[13] it undertook a comprehensive analysis of the human rights considerations associated with implementing privacy-preserving AI-enhanced surveillance. The resulting Use Case Description and Analysis[14] outlined critical considerations from the point of view of human rights and responsible AI innovation. The case study informed the research questions for the semi-structured interviews, as well as the final recommendations.

13 Project funded by the Research Council of Norway, in which the Norwegian University of Science and Technology (project owner), BI Norwegian Business School, the University of Agder, the University of Sussex and several partners from public institutions and businesses join forces to contribute to the global dialogue on the societal security challenges and potential solutions when implementing AI from multistakeholder perspectives. Accessible at: https://prosjektbanken.forskningsradet.no/en/project/FORISS/320783

14 UNICRI. (2026). AI4Citizens use case description and analysis. Accessible at: https://unicri.org/sites/default/files/2026-01/USE_Cases-AI4Cit.pdf

3. **Semi-structured interviews.** UNICRI conducted 48 interviews with 52 participants across five geographic regions: Europe, Americas, Africa, Asia and Oceania. The interviews targeted multidisciplinary experts, mainly with backgrounds in law enforcement, human-rights and ethics, communications and public relations, sociology and political science. ***Unless otherwise indicated, the findings presented in this report draw primarily from these semi-structured interviews.*** The expert interviews explored key considerations for implementing AI systems in law enforcement. In particular, they addressed how transparency, accountability, communication and engagement can foster trust in responsible uses of AI systems for public safety, including public trust in AI-based crowd monitoring. The distinct sets of questions developed for each area of expertise prompted the experts' feedback on the use case scenario, based on their professional experience with AI systems, public safety or communication (> SEE ANNEX).

4. **Qualitative analysis.** The analysis of information derived from the semi-structured interviews, performed jointly by UNICRI and BI Norwegian Business School, relied on a qualitative research approach. It leveraged several technical tools, including NVivo software, to help analyse the qualitative data. For privacy and data security, the software applied only to anonymized interview data, and no external servers were used for storage. The results then were incorporated into the study recommendations.

5. **Experimental studies.** Members of BI Norwegian Business School conducted a dozen experimental studies as part of the overall research process. They examined in detail the various drivers of public acceptance of AI systems, trade-offs between perceived benefits and costs, the impacts of trust in government and various aspects of transparency. The findings of these experimental studies are being published separately, but their relevant insights are incorporated into the recommendations.

6. **Consultations with stakeholders and experts.** Finally, peer reviews of the draft recommendations took place between September 2025 and January 2026. Both key stakeholders and experts offered detailed feedback, which has been integrated into the final version of this report.

Target audience

The report and its recommendations are intended primarily for decision makers in law enforcement agencies and other actors concerned with public safety that have implemented or plan to implement AI systems responsibly and that seek effective approaches on how to be transparent. For the sake of narrative flow, this report refers primarily to law enforcement agencies; however, this does not exclude from its scope other actors concerned with public safety that are not classified as such (such as local governments).

This report may also be relevant to policymakers, civil society organizations, academic researchers, human rights lawyers, ethics experts, technology providers and other stakeholders interested in issues of public trust in AI and law enforcement, transparency and accountability.

Key concepts

This report adopts the following definitions from the Toolkit for Responsible AI Innovation in Law Enforcement:

Law enforcement agencies are primarily the police and other state authorities that exercise police functions, such as investigating crimes, protecting individuals and property, and maintaining public order and safety.[15]

Artificial intelligence refers to the field of computer science dedicated to studying and developing technological systems that can imitate human abilities such as visual perception, decision-making and problem-solving.[16]

AI systems are computer systems that use AI algorithms to achieve specific goals, with a certain degree of autonomy.[17]

AI innovation refers to the wide range of activities organizations undertake when implementing AI systems in their work. This includes all stages of the AI life cycle, from planning to deployment, use and monitoring, and anything else it may involve.

Explainability is a principle for responsible AI innovation in law enforcement that makes it possible for people to understand an AI system from a technical standpoint, including how the AI system makes decisions and generates outputs (i.e., *explainability in a narrow sense*) and why a certain result has been generated (i.e., *interpretability*).[18]

Background and scope

This report forms part of the broader project *AI4Citizens: Responsible AI for Citizen Safety in Future Smart Cities*, funded by the Research Council of Norway – a multidisciplinary research effort involving the development and responsible deployment of AI systems for public safety. The project brings together the Norwegian University of Science and Technology (project owner), BI Norwegian Business School, the University of Agder, the University of Sussex and several public and private partners to advance global dialogue about societal security challenges and the implementation of AI from a multistakeholder perspective.[19]

This collaborative effort conducted research into privacy-preserving crowd monitoring AI systems. A specific scenario was developed to ground the research in a concrete operational context. A version of this scenario was shared with interview participants. In parallel, UNICRI conducted an assessment of the scenario's ethical and legal dimensions, which was published separately.[20] ***The Use Case Snapshots included in this report build on this scenario to illustrate the provided guidance. The AI***

15 UNICRI and INTERPOL. (Revised February 2024). README file.

16 UNICRI and INTERPOL. (Revised February 2024). Introduction.

17 Ibid.

18 UNICRI and INTERPOL (2024). Principles.

19 More information is available at https://prosjektbanken.forskningsradet.no/en/project/FORISS/320783

20 UNICRI. (2026).

system referenced in the snapshots was devised exclusively for scientific and research purposes. All deployment characteristics, operational workflows, and system details are fictional and crafted for the purposes of this report. They do not represent or imply any real-world deployment or commercialization of the described AI system.

Use Case Snapshot 1:
The AI4Citizens Crowd Monitoring and Anomaly Detection AI System

The hypothetical use case scenario analysed under AI4Citizens focuses on an AI system for crowd monitoring and anomaly detection in public spaces, designed with human rights compliance and responsible innovation principles in mind.

Deployment scenario:

A law enforcement agency identifies strategic high-traffic areas where crowd monitoring is essential for public safety. It applies the AI system to pre-existing closed-circuit television (CCTV) cameras which capture live video. To reduce privacy impacts, the AI system immediately anonymizes CCTV footage by masking individual figures **–anonymization algorithm.** It subsequently identifies anomalies, defined as events that may indicate threats to public safety **– anomaly detection algorithm –** and issues alerts to human operators in law enforcement monitoring centres.[21] The algorithms operate as illustrated in the figure below:

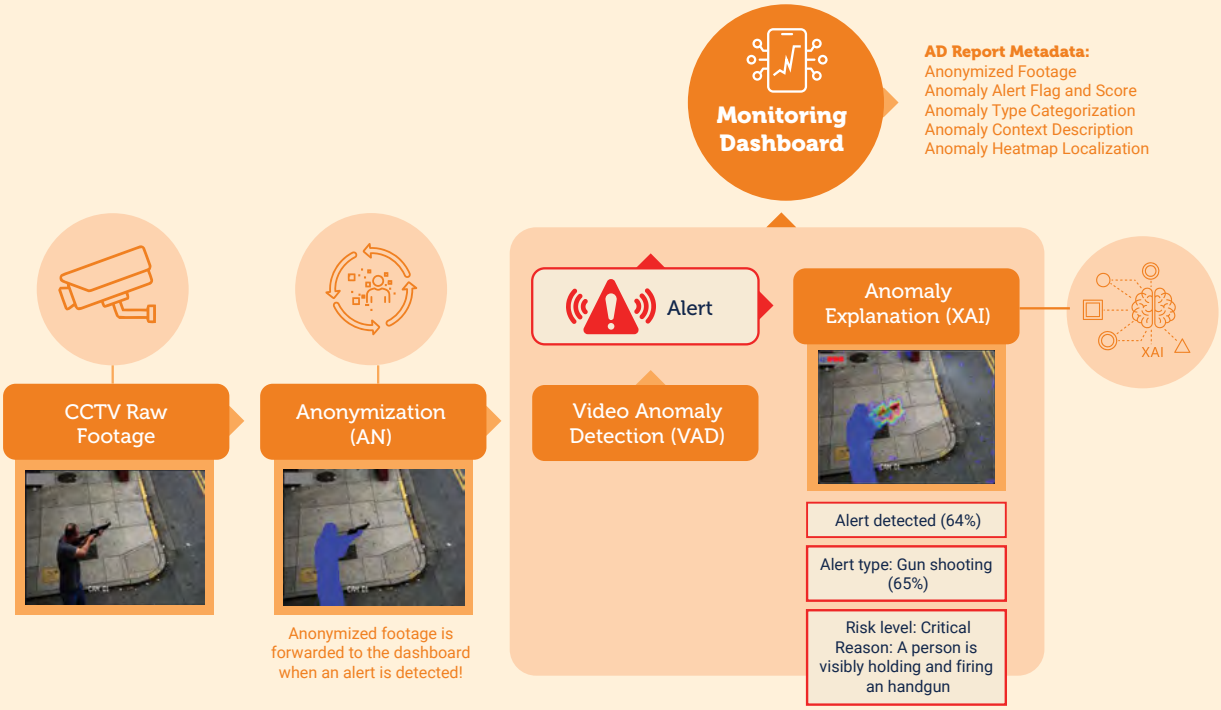


Figure 1– The real-time Anonymization-Anomaly Detection approach proposed in AI4Citizens

21 Mulugeta W. Asres, Lei Jiao & Christian W. Omlin. (2025). Low-Latency Video Anonymization for Crowd Anomaly Detection: Privacy vs. Performance. In IEEE Transactions on Information Forensics and Security. Accessible at: https://ieeexplore.ieee.org/document/11231379.

Operators assess the alert and decide whether further action, such as dispatching a patrol, is required.

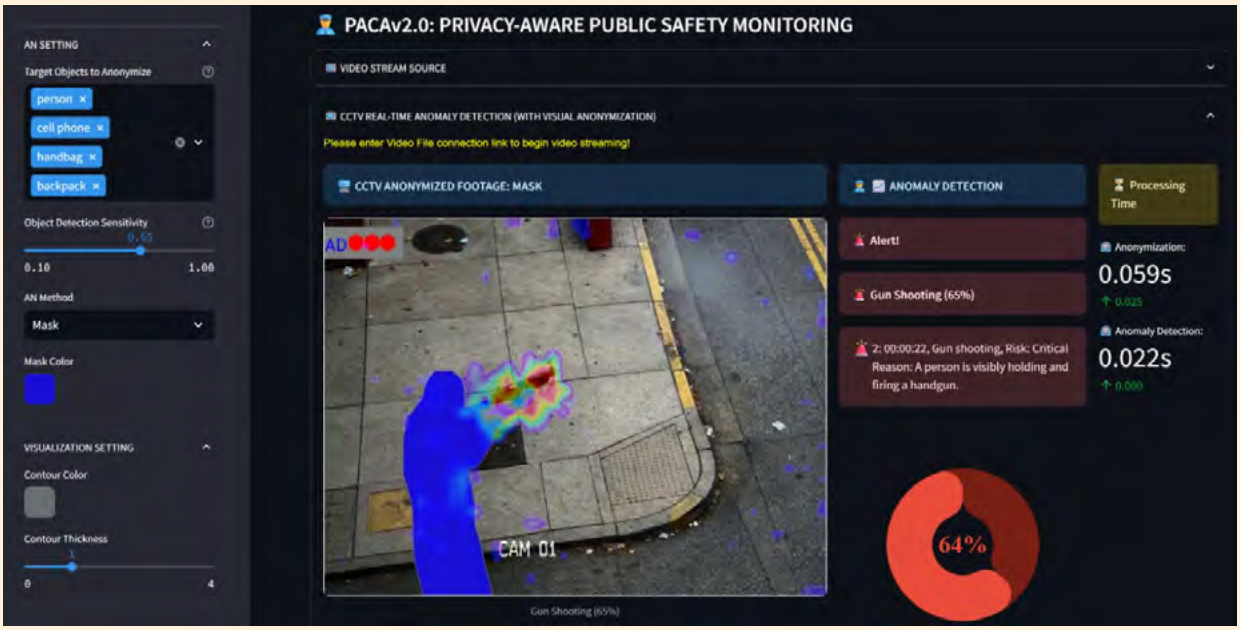


Figure 2 – Screenshot of the AI system's experimental dashboard, accessible at: https://ai4citizens.uia.no

For instance, in a crowded train station, the AI system detects a sudden act of vandalism. The anomaly detection algorithm detects this anomaly, triggering an alert that notifies the monitoring officer. The operator reviews the anonymized footage and makes an informed decision on whether to dispatch personnel to the scene.

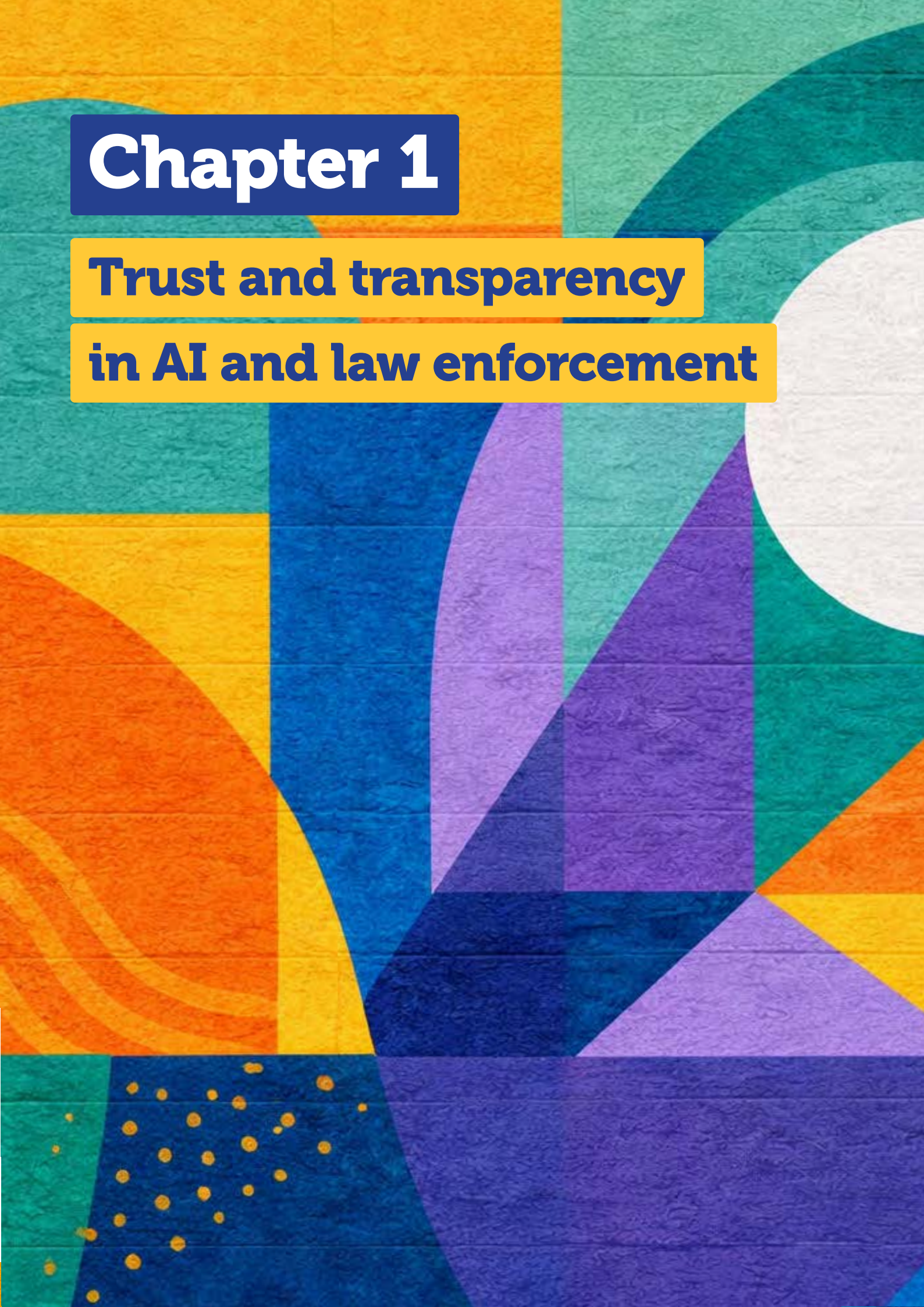
Benefits and risks:

The implementation of the AI system in this scenario aims to provide several benefits for law enforcement agencies: by recognizing specific motions and actions, the system helps officers detect anomalies in public spaces more systematically, which should reduce human fatigue, strengthen incident monitoring capabilities and improve patrol deployment efficiency. It thus has the potential to enhance public safety by reacting to threats in a timely manner, while maximizing the efficient use of available human resources (> SEE USE CASE SNAPSHOT 5).

To address foreseeable risks, such as privacy intrusions, over-surveillance, opacity in automated decision-making, reinforced biases or overreliance on automated outputs, the hypothetical scenario incorporates built-in organizational safeguards, including privacy-protecting body masking, mandatory human oversight and clear restrictions on automated decision-making (> SEE USE CASE SNAPSHOT 2).

Although the research was grounded in the scenario detailed in **> USE CASE SNAPSHOT 1,** the recommendations in this report extend beyond this specific application. They refer to the wider landscape of AI uses in law enforcement, which might include, among others, other forms of image processing, text and speech analysis, risk assessments and predictive analytics, as well as more recent content generation uses that rely on large language models (LLM). When responsibly developed and deployed, such technologies can enhance operational efficiency and support more informed and timely decision-making, while reducing physical and psychological strain on human personnel. However, the integration of AI into law enforcement also raises significant concerns. As noted, AI systems may reproduce or amplify biases present in training data, leave decision-making processes opaque and generate far-reaching and less visible impacts. In law enforcement contexts, these risks may translate into exacerbated discrimination, intrusive or disproportionate surveillance, privacy and personal data breaches and chilling effects on freedoms of assembly and expression, among other concerns.

Noting both these opportunities and risks, the importance of transparency, accountability and trust is clear, for any and all uses of AI in law enforcement. The recommendations presented in this report aim to support such transparency around responsible AI innovation, regardless of the specific technology or operational context.


Chapter 1
Trust and transparency
in AI and law enforcement

1. What is trust, and why does it matter?

Trust determines the legitimacy of law enforcement agencies. Without it, their ability to perform their mission is compromised. Broadly, trust refers to the willingness of one party to be vulnerable to the actions of another party,[22] given the expectation that the latter party is likely to act in a reasonable, reliable and appropriate manner.[23] Such a broad definition can be insightful, but it also lacks precision and specific application to different contexts or social groups.[24] Therefore, this section introduces the unique concept of public trust in law enforcement and the factors that drive it. It also considers what happens to public trust when law enforcement agencies introduce AI systems.

1.1 Understanding public trust in law enforcement

Trust in law enforcement refers to expectations held by individuals, communities and/or the wider public about how agencies will behave, in specific interactions or more generally (i.e., how they treat others or certain segments of the population). People trust law enforcement agencies when they regard them as competent, just, genuinely caring about the people they serve and consistent in doing the right thing. Thus, trust is linked to perceptions of:

- **Effectiveness.** People trust agencies more if they believe they perform their job well – catching criminals, responding quickly when called, solving local problems and so on.[25] The expert interviews reinforced this view and also added that perceived ineffectiveness, particularly when police actions do not address root causes of crime, drive distrust.
- **Fairness**. Perceptions of effectiveness alone cannot guarantee trust though, because it also depends on perceptions of how law enforcement agencies interact with people and make decisions (or *procedural justice*; **> SEE LEARN MORE BOX 1**), not just the outcomes of those decisions.[26] The experts identified several drivers of distrust rooted in people's perceptions of a lack of fairness, as when the public regards the police as an arm of the state rather than a protector of people and believes personnel are biased towards protecting the interests of privileged groups.

Procedural justice requires meaningful and consistent demonstrations; merely superficial or insincere observance can backfire. As a study of police-community relations in Zimbabwe illustrated, citizens'

22 Roger C. Mayer, James H. Davis & F. David Schoorman. (1995). An integrative model of organizational trust. *The Academy of Management Review, 20*(3), 709–734. Accessible at: https://doi.org/10.2307/258792.

23 Diego Gambetta (1988). *Can we trust trust?* In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 213–237). Blackwell. Accessible at: https://www.researchgate.net/publication/255682316_Can_We_Trust_Trust_Diego_Gambetta

24 Mayer, Davis & Schoorman (1995). Ibid.

25 Jonathan Jackson & Jacinta M. Gau. (2015). Carving up concepts? Differentiating between trust and legitimacy in public attitudes towards legal authority. In *Interdisciplinary perspectives on trust: Towards theoretical and methodological integration* (pp. 49-69). Springer International Publishing. Accessible at: https://dx.doi.org/10.2139/ssrn.2567931 Kristina Murphy, Lorraine Mazerolle & Sarah Bennett. (2014). Promoting trust in police: Findings from a randomised experimental field trial of procedural justice policing. *Policing and Society, 24*(4), 405-424. Accessible at: https://doi.org/10.1080/10439463.2013.862246. Julia Yesberg, Ian Brunton-Smith & Ben Bradford. (2023). Police visibility, trust in police fairness and collective efficacy: A multilevel Structural Equation Model. *European Journal of Criminology*, *20*(2), 712-737. Accessible at: https://journals.sagepub.com/doi/10.1177/14773708211035306

26 Tyler. (2006).

trust in and willingness to cooperate with law enforcement agencies related directly to the fairness and consistency with which law enforcement officers exercised discretion in applying rules. On the other hand, those discretionary powers also appeared vulnerable to an organizational culture which framed the police as an extension of state power, as well as political influence and structural constraints (e.g., resource limitations or weak oversight). These pressures seemingly undermined the consistency and impartiality of officers' behaviours, thereby eroding public trust in the police as an instrument of procedural justice.[27]

Learn More Box 1:
Psychology's view on institutional trust

Psychologists have studied institutional trust from two main angles. Organizational psychologists ask about which conditions need to exist for people to trust an institution at all. Social psychologists ask about what authorities need to do to earn that trust. Together, these perspectives suggest a way to understand public trust in law enforcement, in terms of what people need to *believe* about an agency and how agencies can *demonstrate* it.

Trust in an institution draws on three pillars, as described by a framework known as the **Ability, Benevolence and Integrity (ABI) model**.[28] Applied to law enforcement, these pillars can be defined as follows:

1. **Ability:** The agency has the specialized skills, knowledge and psychological readiness to perform its mandate effectively.
2. **Benevolence:** The agency's primary orientation is the welfare of the people it serves; its actions are motivated by a sincere desire to protect the community rather than a desire to assert dominance or meet bureaucratic quotas.
3. **Integrity:** The agency consistently lives up to its stated values and adheres to a stable, predictable moral and legal compass, regardless of external pressures or internal convenience.

Closely related to *benevolence* and *integrity* is the social psychology concept of **procedural justice,** which recognizes that people consider the fairness of the process to judge authorities, rather than just the outcomes of authorities' decisions. By considering why people comply with legal authorities, researchers have identified four pillars of procedural justice: voice, neutrality, respect and trustworthiness.[29]

27 Joshua Foma, Riska Sri Handayani & Husnul Fitri. (2025). Understanding police discretion in Zimbabwe: Institutional drivers and consequences for community relations in Harare Metropolitan Province. *Journal of Social Research*, *4*(12), 2001-2015. Accessible at: https://doi.org/10.55324/josr.v4i12.2885 Ishmael Mugari & Emeka E. Obioha. (2018). Patterns, costs, and implications of police abuse to citizens' rights in the Republic of Zimbabwe. *Social Sciences*, *7*(7), 116. Accessible at: https://doi.org/10.3390/socsci7070116

28 Mayer, Davis & Schoorman. (1995).

29 Tom R. Tyler. (2003). Procedural justice, legitimacy, and the effective rule of law. *Crime and Justice, 30*, 283-357. Accessible at: https://www-jstor-org.leidenuniv.idm.oclc.org/stable/1147701?seq=68 Steven Blader & Tom R. Tyler. (2003). A four-component model of procedural justice: Defining the meaning of a "fair" process. *Personality and Social Psychology Bulletin*, *29*(6), 747-758. Accessible at: https://doi.org/10.1177/0146167203029006007

Applied to the law enforcement context, this means that agencies can engage in procedural justice by:

- *Giving people a* voice and allowing individuals and communities to express their perspectives, so as to take them into account in decision-making.[30]
- *Acting* neutrally by making decisions consistently across groups, based on facts rather than personal opinions or institutional biases.[31]
- Treating people with *dignity and* respect.[32]
- *Showing* trustworthiness, genuine care and a commitment to lawful and appropriate uses of authority, in the interest of the community, such as respecting the rule of law and human rights, exercising powers proportionately and refraining from abuses.[33]

The particular importance of trust for law enforcement results from the power imbalances inherent in policing. To ensure public welfare and safety, law enforcement agencies are allowed to (proportionately) use force or impose serious consequences to freedom of movement and expression, such as detaining people. Ordinary people cannot opt out of this relationship in a rule of law-based society. Yet modern law enforcement also relies on the principle of "policing by consent", such that people voluntarily submit to police powers because they believe (trust) these powers are appropriate, lawful and justified, and that agencies will use them fairly to maintain a sense of common public safety.[34] Trust is the very foundation of the legitimacy of law enforcement agencies' authority.[35]

In practical terms, effective **law enforcement requires public cooperation, and trust is a key driver of cooperation.** Greater public trust correlates with greater deference in face-to-face encounters, voluntary collaboration with authorities and compliance with the law. Even a single, brief, personal interaction, such as a stop for a random alcohol breath test, can improve trust, as long as officers use fair and respectful procedures. If people have repeated, positive interactions with members of law enforcement agencies over time, it increases their willingness to cooperate and their sense of obligation to comply even further.[36]

Such outcomes are not guaranteed though. As one expert put it, trust is difficult to build and easy to break. As this point makes clear, public trust in law enforcement agencies is both complex and dynamic. It evolves over time, and new expectations continually emerge. What might have been acceptable decades ago may no longer suffice today. Even within the same time frame, trust is subjective, based

30 Murphy, Mazerolle & Bennett. (2014).

31 Ibid.

32 Jackson & Gau. (2015). Murphy, Mazerolle & Bennett. (2014). Yesberg, Brunton-Smith & Bradford. (2021).

33 Jackson & Gau. (2015). Murphy, Mazerolle & Bennett. (2014). Yesberg, Brunton-Smith & Bradford. (2021).

34 The concept of "policing by consent" derived from the ideas prominently articulated in the Anglo policing tradition by Sir Robert Peel. See: Sarah Tudor. (2023). Police standards and culture: Restoring public trust. Accessible at: https://lordslibrary.parliament.uk/police-standards-and-culture-restoring-public-trust/#heading-1

35 Jackson & Gau. (2015).

36 Murphy, Mazerolle & Bennett. (2014). Yuning Wu & Ivan Y. Sun. (2009). Citizen trust in police: The case of China. *Police Quarterly*, *12*(2), 170-191. Accessible at: https://www.researchgate.net/publication/247748694_Citizen_Trust_in_Police_The_Case_of_China.

on public perceptions and expectations. Individual perceptions result from past experiences[37] and "gut feelings."[38] Even if a person has not personally experienced police violence, one interviewed expert acknowledged that knowing someone else who has suffered such treatment can reduce individual trust in the police. Immigrants' negative experiences with the police in their home country continue to influence their perceptions of the police in their country of residence.[39] Societal experiences also matter. The wider national context, both current and historical, shapes judgements too. A documented history of human rights violations significantly influences how a community assesses the trustworthiness of law enforcement.

1.2 What happens to public trust when law enforcement agencies introduce AI systems?

As described in the Introduction, people tend to be cautious and sceptical about AI. Law enforcement agencies that plan to introduce AI systems thus need to consider the public's general attitudes towards AI. But they should also recognize that when people develop performance expectations, they base them on their beliefs about how effectively the AI system will be in performing its assigned tasks.[40] Research shows that, thus far, **people simply do not believe that AI is effective in contexts that involve moral judgements**.[41] When those judgements also threaten meaningful risks, as is true in law enforcement contexts, the public likely rejects AI systems[42] and prefers human decision makers, whom they see as more trustworthy for tasks that demand judgement and empathy. A 2021 study in the United Kingdom revealed that people trusted police officers' decisions more than those by AI algorithms, especially if the decisions had a community-wide impact.[43]

Thus, to build public trust in their uses of AI systems, law enforcement agencies must realize that multiple, complex factors interact to shape their technology perceptions:

The context. Trust in technology varies with the context.[44] The same AI system can prompt trust or distrust, depending on its perceived purpose. Facial recognition software might seem fine to unlock a mobile phone, potentially acceptable to monitor traffic and totally unacceptable to surveil people on the street. People tend to be more trusting and accepting of privacy-intrusive technologies deployed by airport security for border control than of uses by local police for general monitoring of public

37 Ibid.

38 Jackson & Gau. (2015).

39 Wu & Sun. (2009).

40 Berkeley J.Dietvorst. (2025). Understanding when laypeople adopt predictive algorithms. *Nature Human Behaviour*, *9*(5), 851-853. Accessible at: https://dx.doi.org/10.2139/ssrn.5280790

41 Yochanan E. Bigman & Kurt Gray. (2018). People are averse to machines making moral decisions. *Cognition*, *181*, 21-34. Accessible at: https://cdr.lib.unc.edu/downloads/4q77g7072

42 UNICRI and INTERPOL. (2024).

43 Human decision-making was especially valued in a fictional scenario where a crime hotspot was identified and a police officer needed to decide whether or not to dispatch officers to the hotspot. Interestingly, the same did not apply in a scenario where a single police officer observed suspects and needed to decide whether to conduct a stop and search. See Zoë Hobson, Julia A. Yesberg, Ben Bradford & Jonathan Jackson. (2021). Artificial fairness? Trust in algorithmic police decision-making. *Journal of Experimental Criminology*, *19*(1), 165-189. Accessible at: https://link.springer.com/article/10.1007/s11292-021-09484-9

44 Mayer, Davis & Schoorman. (1995). Dorotic, Stagno & Warlop. (2024).

spaces.[45] A comprehensive survey of public perceptions of AI use by law enforcement, conducted by UNICRI and INTERPOL between November 2022 and June 2023, indicated that people appear more comfortable with retrospective uses, such as analysing past events, than with predictive or real-time decision-making.[46]

The actor that deploys the technology. Europeans indicate greater acceptance of high-risk AI applications (e.g., surveillance) implemented by public rather than corporate entities.[47]

Group norms and demographics. Different groups interpret the same technologies in conflicting ways. One group might regard cameras as tools to support public safety, but another may see them as tools of oppression that disproportionately target minority populations.

Historical and cultural context. Studies across the United States of America, United Kingdom and Australia showcase the influences of existing, historical factors on acceptance of surveillance technologies (e.g., facial recognition, body-worn cameras [BWCs]) and trust. Overall, United States residents are more accepting of surveillance technology but less trusting of the police than residents of the United Kingdom and Australia.[48] They express scepticism about whether BWCs can improve police–citizen relationships, reflecting existing tensions between police and minority communities, and cite law enforcement agencies' discretionary uses of BWC as a key obstacle, despite evidence that BWCs can document interactions accurately.[49, 50]

Institutional trust in law enforcement agencies thus strongly influences support for their adoption of AI systems.[51,52] When law enforcement agencies already enjoy trust, they can readily justify their AI implementation efforts and counter the scepticism normally evoked by this technology. The previously cited UNICRI–INTERPOL study identified a correlation between people who believe law enforcement agencies respect the law and individual rights and their support for AI adoption. Their acceptance also increased when safeguards were in place; the study suggested that transparency, human oversight and strong legal frameworks were essential for establishing public confidence.[53] Another study of public attitudes towards police uses of face recognition technology reached a similar conclusion: trust in law enforcement related positively to acceptance of the AI-driven technology.[54]

45 Ada Lovelace Institute and The Alan Turing Institute. (2023). *How do people feel about AI? A nationally representative survey of public attitudes to artificial intelligence in Britain.* (2023). Accessible at: https://www.turing.ac.uk/sites/default/files/2023-06/how_do_people_feel_about_ai_-_ada_turing.pdf

46 UNICRI. (2024).

47 Dorotic, Stagno & Warlop. (2024).

48 Kay L. Ritchie, Charlotte Cartledge, Bethany Growns, An Yan, Yuqing Wang, Kun Guo, Robin S. S. Kramer, Gary Edmond, Kristy A. Martire, Mehera San Roque & David White. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. *PloS One*, *16*(10), e0258241. Accessible at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0258241

49 William H. Sousa, Terance D. Miethe & Mari Sakiyama. (2018). Inconsistencies in public opinion of body-worn cameras on police: Transparency, trust, and improved police–citizen relationships. *Policing: A Journal of Policy and Practice, 12*(1), 100–108. Accessible at: https://doi.org/10.1093/police/pax015

50 Cynthia Lum, Christopher S. Koper, David B. Wilson, Megan Stoltz, Michael Goodier, Elizabeth Eggins, Angela Higginson & Lorraine Mazerolle. (2020). Body-worn cameras' effects on police officers and citizen behavior: A systematic review. *Campbell Systematic Reviews*, *16*(3), e1112. Accessible at: https://doi.org/10.1002/cl2.1043

51 Anna Sagana, Mengying Zhang & Melanie Sauerland. (2026). Public attitudes towards police use of AI-driven face recognition technology. *Computers in Human Behavior, 174*, 108821. Accessible at: https://www.sciencedirect.com/science/article/pii/S0747563225002687

52 Ritchie et al. (2021).

53 UNICRI. (2024).

54 Sagana, Zhang & Sauerland. (2025).

Integrity, achieved when law enforcement agencies demonstrate their fairness and ability to perform tasks, thus appears to drive public trust in the agencies' AI implementation.[55] Expert interviews echoed these findings. Public perceptions of government and law enforcement agencies influence their views of the use of AI in policing. These insights combine to establish an important point**: trust in law enforcement agencies (or a lack thereof) can spill over into attitudes towards AI adoption by law enforcement agencies, reinforcing the critical importance of cultivating and preserving trust.**

When AI contributes to decision-making, it could undermine perceptions of procedural justice, because it implies that human actors are less involved in the decision. In this scenario, exposing people to repeated examples of effective, well-justified AI decision-making might offer another route to build trust and increase acceptance.[56] As noted, trust develops on the basis of real experiences and perceptions of fairness and effectiveness, so positive experiences with AI might be an effective way to foster trust. According to one study, United Kingdom participants exposed to successful algorithmic decision-making expressed more support for law enforcement agencies' uses of the technology.[57]

Ultimately, law enforcement agencies should work to prompt broad public perceptions of themselves as credible and reliable, rather than focusing just on how to secure trust for a specific AI system. When detailing the specific AI systems they use, though, they also need to implement measures and mechanisms that can convincingly prevent or mitigate the risks to individuals and communities, as exemplified in **> USE CASE SNAPSHOT 2.**

Use Case Snapshot 2: Technical and organizational safeguards

To address the potential risks and harms related to the use of AI in law enforcement – such as, but not limited to, privacy intrusions, algorithmic bias, over-surveillance, and opaque automated decision-making – the AI4Citizens use case included an analysis of which ethical and human rights considerations need to be accounted for when implementing the AI system. They included both technical and organizational safeguards, such as those detailed below.

The AI system was designed to comply with the applicable legal requirements, such as relevant privacy and data protection laws. The implementing law enforcement agency should ensure safeguards such as the following:

- All footage is anonymized upon capture, to protect the right to privacy and personal data of depicted people. If raw footage must be retained (e.g., due to a court order), strict compliance with applicable laws must govern its storage duration and access.

55 Theo Araujo, Natali Helberger, Sanne Kruikemeier & Claes H. de Vreese. (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & Society*, *35*(3), 611-623. Accessible at: https://link.springer.com/article/10.1007/s00146-019-00931-w. Robin G. Li. (2025). *Your faces matter: Facial recognition technology (FRT) in AI-enabled public services and provision*, doctoral dissertation, Arizona State University. Accessible at: https://ascelibrary.org/doi/10.1061/JLADAH.LADR-1435. Jackson & Gau. (2015).

56 Hobson, Yesberg et al. (2023).

57 Ibid.

- Training data, performance metrics and potential impacts on different demographics are documented and communicated to law enforcement agencies.
- Regular reviews of the system's performance check for system integrity and involve tests among different demographic contexts to ensure fairness.
- Law enforcement personnel that are the end-users of the AI system are well-trained in the system's capabilities and limitations and ethical and legal considerations, including recognition that anomalies detected by the AI system are context-specific and not conclusive of criminal behaviours.
- End-users critically assess AI outputs, avoid overreliance on automation and work to mitigate the risk of bias. They see the AI system as a support tool and remain in control of and responsible for decision-making.

2. Transparency as a tool for building trust

Transparency, as used in this report, refers to the openness by law enforcement agencies regarding their AI innovation efforts – i.e., which AI systems they use or intend to use, for what purposes and with which processes. In this sense, transparency involves a reciprocal interaction between law enforcement and relevant stakeholders, not a unidirectional process.

In the expert interviews, transparency consistently emerged as a key enabler of public trust. Transparency about AI systems is particularly important, given the significant potential impacts of law enforcement agencies' decisions on individuals, communities and society at large. Yet law enforcement agencies appear to struggle to establish transparency, particularly in their AI implementation efforts. Several studies corroborate this observation, highlighting persistent transparency deficits, limited public oversight, an absence of impact assessments and overreliance on opaque discreet procurement processes, seemingly to avoid public scrutiny.[58]

These issues stem from a range of underlying challenges, including an incomplete understanding of what transparency is and why it is essential. To address such questions, this section details the meaning of transparency in law enforcement uses of AI, while also acknowledging the practical constraints on agencies attempting to provide meaningful transparency surrounding their AI innovation.

58 Ben Bradford, Julia A. Yesberg, Jonathan Jackson, & Paul Dawson. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *British Journal of Criminology, 60*, 1502–22. Accessible at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7454338/ H. Bloch-Wehba. (2021). Visible policing: Technology, transparency, and democratic control. *California Law Review*, 109(3), 917-978. Accessible at: https://doi.org/10.31228/osf.io/4pcf3

2.1 Defining transparency

Transparency relates to the openness of an entity by revealing information about its decision-making processes, procedures, performance and outcomes.[59] Even if it only sometimes appears enshrined in law, transparency represents an ethical imperative for initiatives with a public impact, such as introducing AI systems. The concept can however be ambiguous, without any uniformly accepted definition across disciplines, jurisdictions or stakeholders. For governance actors, transparency is tied to accountability; for civil society, it implies openness and communication; for technical communities, transparency results from explainable models and methods. Even the expert interviews reflect this ambiguity. Most of the experts defined transparency as communication and openness and emphasized visibility and honest descriptions of uses of AI systems. But others associated the concept with what can also be defined as "explainability", meaning the ability to understand how an AI system works and why it produces certain outputs. Such technical views of transparency increasingly permeate regulatory debates. As a result, determining the scope of transparency and translating it into operational practice often results in contested and ambiguous discussions.

By illustrating some of the various definitions of transparency, drawing on both expert interviews and empirical studies,[60] this section suggests ways to leverage transparency in practice to strengthen public trust in law enforcement agencies' uses of AI. Starting broadly and then addresses more specific applications of transparency, the following senses of transparency are explored:

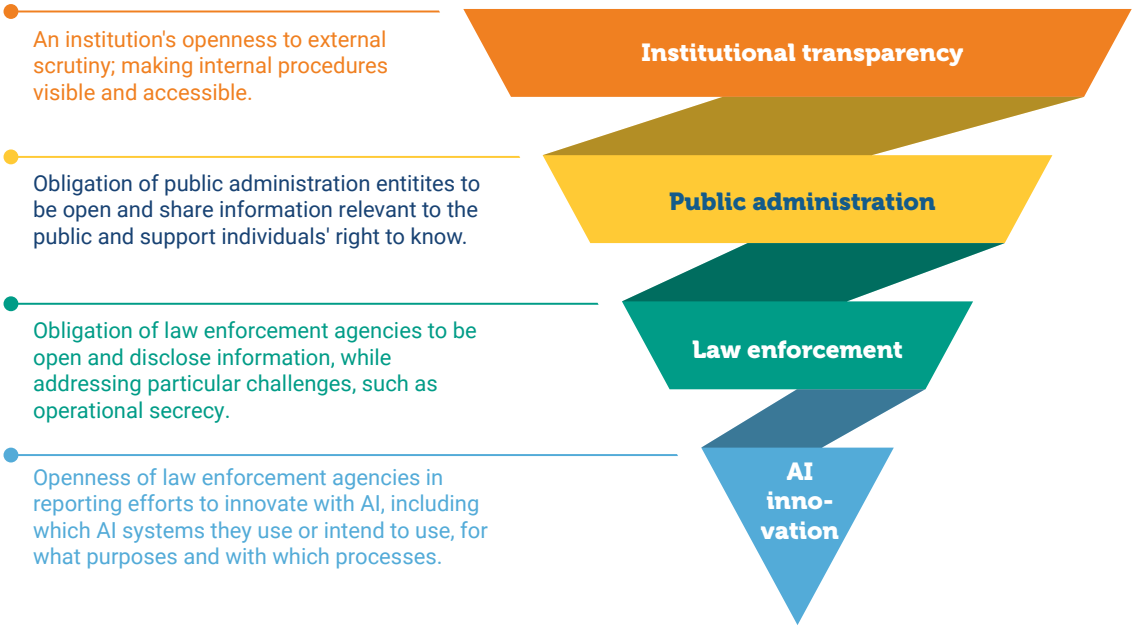


Figure 3 – The different senses of transparency explored in the report

59 Meijer. (2013). Grimmelikhuijsen & Welch. (2012).

60 Dorotic, Stagno & Warlop. (2024). Dorotic et al. (2025) experimentally test how moral judgements shape the perceived permissibility of high-risk AI systems and the effectiveness of privacy-protection solutions. See Matilda Dorotic, Tuan Viet Do & Yochanan E. Bigman. (2025). *Impact of moral judgments on permissibility of high-risk AI and effectiveness of privacy-protection solutions*. BI Norwegian Business School working paper. Accessible at: https://hdl.handle.net/11250/5333378. See also Dorotic, Stagno & Warlop. (2024).

Institutional transparency in public administration

As an overriding concept, *institutional transparency* refers to any institution's openness to external scrutiny.[61] Such openness results from making its internal procedures visible and accessible.[62] In public administration, transparency is a cornerstone for good governance and public administration accountability.[63] Openness allows individuals and civil society organizations to uncover wrongful or problematic conduct by public authorities, question their decisions and hold them responsible for their actions. According to the *OECD Principles of Public Administration*, transparency guarantees the right to access public information; it also imposes an obligation on public authorities to make it easy for individuals to obtain that information. Access may be denied only for information that has been classified, based on compelling reasons clearly specified by law. Transparency also requires proactive disclosures of information "which is relevant, complete, accurate and up to date, accessible, understandable, machine-readable, in open-format and reusable."[64]

According to academic literature and the expert interviews, transparency cannot be limited to one-way disclosures by public entities that offer information they are willing to share. Instead, it demands complex, dynamic interactions of information disclosure, interpretations and institutional accountability. During such interactive processes, individuals must be able and willing to understand and act on information, and institutions must remain responsive and prepared to engage.[65] Understanding these interactive considerations is essential. Transparency can enhance trust and acceptance, but it might also heighten security vulnerabilities or amplify people's concerns and uncertainty **(> SEE CHAPTER 1 – SECTION 2.3).**

Institutional transparency in the law enforcement

Law enforcement agencies are public entities, subject to the principle of transparency for public administration in general. In addition, transparency surrounding their activities can raise unique considerations. The dual roles of law enforcement agencies often create tension between transparency and confidentiality. On the one hand, they act as regular public bodies, responsible for maintaining public order through preventive functions such as street monitoring. In this capacity, there is a strong public interest in transparency, especially in how the publicly funded entity exercises its powers. On the other hand, they operate within the judicial sphere and perform criminal investigations. In this role, they must conceal information and/or policing practices whose release could jeopardize ongoing operations.

Legal frameworks generally acknowledge that, given the nature of their work, law enforcement agencies may need to maintain a certain level of secrecy, to avoid revealing any information that could

61 Christopher Hood & David Heald (Eds.). (2006). *Transparency: The key to better governance?* Liverpool University Press. Accessible at: https://www.davidheald.com/coverage/PA%20Raab%202008.pdf

62 Cornelia Moser. (2001). How open is "open as possible"? Three different approaches to transparency and openness in regulating access to EU documents. IHS Political Science Series, No. 80. Accessible at: https://irihs.ihs.ac.at/id/eprint/1389/1/pw_80.pdf. Meijer. (2013).

63 Defined as all documented information held by the public administration (individuals or legal persons who exercise public authority). See Organisation for Economic Co-operation and Development (OECD). (2023). The Principles of Public Administration, OECD, Paris. Accessible at: https://www.sigmaweb.org/publications/Principles-of-Public-Administration-2023.pdf; Principle 15. Hood & Heald. (Eds.). (2006).

64 OECD. (2023).

65 Meijer. (2013).

compromise public safety.[66] Yet such necessary operational secrecy cannot serve as a justification for the absence of two-way communication to aid their accountability. Transparent engagement still can take place, without revealing sensitive operational details, by focusing on purposes, principles and safeguards rather than information that must remain confidential.

Transparency in AI innovation

As AI becomes increasingly complex and ubiquitous, the relevance of transparency has grown correspondingly. For AI systems, which operate through software that can run inconspicuously in the background, it is entirely possible – and often the case – for them to be embedded in decision-making workflows without the knowledge of users or entities subject to the decisions.[67] This inherent *invisibility* elevates transparency to a core principle in AI ethics, which calls for openness and disclosures of AI systems' development and use that enable meaningful oversight and accountability.[68]

The UNICRI-INTERPOL Toolkit for Responsible AI Innovation in Law Enforcement defines transparency as promoting good communication practices across an AI system's life cycle; sharing clear, accessible and complete information with all stakeholders; and ensuring that individuals who interact with AI systems have sufficient knowledge and understanding of how those systems function so that they can safeguard their autonomy.[69] In addition, expanding beyond ethical principles, transparency increasingly appears in binding laws, as **> LEARN MORE BOX 2** explains.

Learn More Box 2: Transparency as a legal requirement in AI implementation

The European Union's (EU) AI Act explicitly defines transparency as AI systems' development and use "in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights."[70] To operationalize this principle, the AI Act establishes transparency obligations for providers and deployers of certain AI systems.[71] It requires developers of high-risk AI systems, including many

66 For example, Council of Europe (2018). Convention 108+:Convention for the protection of individuals with regard to the processing of personal data. *Explanatory Report,* para. 92. Accessible at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. (2024), para. 104. Accessible at: https://rm.coe.int/1680afae67

67 UNICRI and INTERPOL. (2024). Introduction.

68 United Nations Educational, Scientific and Cultural Organization (UNESCO). (2022). Recommendation on the Ethics of Artificial Intelligence. Accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000381137 Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Christopher Nagy & Madhulika Srikumar. (2020). Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center Research Publication No. 2020-1. Accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482

69 UNICRI and INTERPOL (2024). Principles.

70 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). (EU AI Act). Recital 27.

71 These obligations are not yet in effect as of the time of this publication.

law enforcement use cases, to design and develop them to provide sufficient operational transparency and enable deployers to interpret the system's output and use it appropriately. In turn, high-risk AI systems must be accompanied by clear, relevant, comprehensible instructions for use that enable deployers to understand the system's capabilities, limitations and proper applications.[72] A notable feature of the AI Act is its creation of an EU database, managed by the European Commission, that houses information about high-risk AI systems registered by providers and public authorities that deploy them. The database is intended to be publicly accessible, though exceptions apply to AI systems for law enforcement, which instead must be recorded in a secure, non-public section that is accessible only to the Commission and national authorities.[73]

Beyond the European Union, other jurisdictions have also sought to embed transparency into law. For instance, transparency is central to South Korea's AI Basic Act, which imposes transparency obligations, requires clear labelling of AI-generated content, and obliges AI operators and developers to comprehensively document measures they have taken to ensure AI safety and reliability.[74] Brazil's proposed AI Bill also identifies transparency as a key principle and imposes corresponding obligations on developers and users, with particular emphasis on AI systems used by public entities. This draft bill also includes individual rights to transparency, such as the right to information when interacting with AI systems.[75] Transparency already has been codified in Brazil, in a federal ordinance governing the use of AI in criminal investigations, which addresses appropriate processes for federal security forces to procure AI systems.[76]

Transparency regarding technical aspects versus explainability and interpretability

Transparency is often intertwined with terms such as "explainability" and "interpretability",[77] but it is important to disentangle them. Both transparency and explainability are instrumental principles for safeguarding *human autonomy*, or the capacity and right of every individual – law enforcement personnel, victims, suspects, criminals, citizens – to exercise self-governance. Such autonomy requires that those individuals have sufficient knowledge and understanding of the AI systems that affect them.[78]

Because this report focuses on transparency as a desired attribute of law enforcement agencies, it approaches transparency in AI implementation as part of the broader concept of institutional transparency, so it entails the relational and communicative practices that any institution uses when adopting and deploying AI systems. Such a perspective certainly requires openness about technical

72 EU AI Act, Article 13.

73 EU AI Act, Articles 49 (4) and 71.

74 Sakshi Shivhare & Kwang Bae Park. (April 18, 2025). South Korea's new AI Framework Act: A balancing act between innovation and regulation. *Future of Privacy Forum*. Accessible at: https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/

75 Projeto de Lei n° 2338, de 2023.https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Most recent text is available here: https://legis.senado.leg.br/sdleg-getter/documento?dm=9915448&ts=1742240908123&disposition=inline

76 Portaria 961/2025. Accessible at: https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-em-investigacoes-criminais-e-inteligencia-de-seguranca-publica/portaria-mjsp-no-961-de-24-de-junho-de-2025-portaria-mjsp-no-961-de-24-de-junho-de-2025-dou-imprensa-nacional.pdf

77 Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Christopher Nagy & Madhulika Srikumar. (2020). Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center Research Publication No. 2020-1. Accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482

78 UNICRI and INTERPOL. (2024). Principles.

elements – the types of algorithms used, performance indicators, training data, but the focus is not on such elements of explainability per se. Rather, *explainability* is an attribute of the AI system itself. For example, AI systems are often described as "black boxes", because their inner workings are so intricate that even expert developers struggle to explain how they produce specific outputs.[79]

In AI literature, explainability thus refers to the *technical* capacity to understand how an AI system makes decisions and generates outputs, which might be labelled *explainability in a narrow sense*, along with why certain results emerge, which is sometimes called *interpretability*.[80] The distinction matters in practice. A perfectly explainable algorithm implemented without any public disclosure or engagement remains opaque in ways that matter for good governance and accountability. An agency might be highly transparent about its uses of a particular AI system, the policy framework governing its use and the safeguards in place, but the underlying model, in technical terms, could remain a black box.

2.2 Taking a closer look at transparency in law enforcement and AI

In the interviews, the centrality of transparency for both AI uses and law enforcement was obvious, particularly for the policy, ethics and human rights experts. Law enforcement activities inherently affect people's rights, and the introduction of AI systems frequently amplifies such impacts. Transparency can function as a fundamental safeguard of human rights in this context. Provided that adequate accountability and redress mechanisms are in place, when the persons affected by AI-supported decisions are aware of its use and have clear information about it, they can meaningfully question the use of AI systems, assess whether outputs are accurate and challenge them as needed.[81] Without such visibility, as one law enforcement expert cautioned, personnel may be tempted to shift accountability for their decisions to the AI system and away from themselves.

Learn More Box 3: Surveillance and the risk of "chilling effects"

Deploying AI systems for surveillance represents more than an incremental upgrade to existing practices; AI fundamentally changes the nature of surveillance. Surveillance shifts from targeted observation to large-scale, often indiscriminate data collection. The information gathered involves not just individuals suspected of wrongdoing but anyone in the broader population.

For law enforcement agencies, surveillance tactics are essential to criminal investigations. Surveillance includes a range of activities, such as monitoring, which consists of short-term, preliminary observation to detect crime, and covert surveillance, which uses more invasive approaches during an investigation.[82] Different techniques, whether they rely on AI systems, CCTV cameras

79 UNICRI and INTERPOL. (2024). Introduction.

80 UNICRI and INTERPOL. (2024). Principles.

81 UNESCO. (2022).

82 International Association of Chiefs of Police (IACP). (April 2009). Surveillance. Law Enforcement Policy Center. Accessible at: https://www.theiacp.org/sites/default/files/2020-06/Surveillance%20FULL%20-%2006222020.pdf

or physical stop-and-search policies, all aim to increase law enforcement effectiveness and make communities feel safer. Yet, their unintended consequences often have the opposite effect.

In particular, uncertainty about the presence or extent of surveillance and fears of being monitored can undermine trust and strain social relationships. Surveillance also increases threats to human rights, particularly privacy, which can induce a "chilling effect" and cause people to refrain from exercising other rights and freedoms. That is, concerned about the risks of surveillance, people might stop exercising their freedom of movement and assembly, freedom of expression and participation in public life and political activities, the right to protest, or the freedom of conscience and religion. Excessive surveillance even might produce counterproductive outcomes, such as exacerbating the public's fear of criminal activity.

Transparency as a human rights safeguard takes a particularly critical role during court proceedings. Parties in criminal proceedings need access to information to ensure a fair trial. Access to adequate information about AI system uses is essential for victims and their families to seek appropriate redress, for suspects to verify the chain of evidence and build defences, and for courts to duly access the evidence presented.[83]

External scrutiny promises to enhance AI uses by law enforcement agencies. The AI market is highly competitive, and technology providers have strong incentives to release products quickly, often at the expense of thorough safety validation. In practice, then, law enforcement agencies might purchase AI systems that appear to offer impressive technical capabilities but that have not undergone sufficient real-world testing or proactive assessments of their impacts on various stakeholders.[84] But transparency supports independent evaluations, such as by academic institutions and civil society groups. These external safeguards can protect law enforcement agencies from inadvertently adopting ineffective AI systems. When law enforcement agencies involve external stakeholders in their AI innovation plans from an early stage, they gain diverse perspectives and encourage insightful discussions. Such stakeholder engagement ultimately supports the integration of AI systems that are more reliable, compliant and effective.

In addition to these safeguarding roles, transparency can enable trust. For some interviewed experts, transparency constitutes the very starting point for building trust, and trust is not possible without transparency. In general, if decision-making processes are transparent, they may also seem procedurally fair, so people are more willing to accept the resulting decisions.[85] If the public participates meaningfully in adoption and implementation decisions, law enforcement agencies can introduce their AI systems more smoothly, sustainably and in a socially accepted manner. As an interviewed expert noted, by improving public acceptance of AI uses in law enforcement, transparency can have the secondary effect of strengthening the broader AI innovation ecosystem of a country.

83 UNESCO. (2022).

84 Besides being frequently mentioned by expert interviewees, these concerns have been expressed in several white papers. See OECD. (2023). *The impact of artificial intelligence on the public sector: Risks and opportunities,* ibid.; European Commission. (2020). *White paper on artificial intelligence: A European approach to excellence and trust*. Publications Office of the European Union. Accessible at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

85 Jenny de Fine Licht. (2014). Transparency actually: How transparency affects public perceptions of political decision-making. *European Political Science Review*, *6*(2), 309-330. Accessible at: http://dx.doi.org/10.1017/S1755773913000131

Yet the expert interviews also repeatedly raised warnings about the potential for a lack of transparency to undermine public trust. When people suspect that technology is being used but do not know how, or whether it is being applied to them, their fears of misuse increase, and so does public distrust **(> SEE LEARN MORE BOX 3)**. If law enforcement agencies fail to be or take too long to become transparent, this can spark social unrest that threatens to undermine their AI usage plans. Public backlash has prompted several agencies to revise their policies.[86]

The challenges surrounding transparency about law enforcement uses of AI persist **(> SEE CHAPTER 1 – SECTION 2.3).** But some encouraging developments are also emerging, signalling cultural changes and broader recognition of the need for transparency. Most government bodies now maintain institutional websites, which they can use to disclose information about the technologies they employ. Granted that while many agencies share little or no detail, some exceptions are notable. For example, a police service, described by an expert, has created a dedicated web page, describing its AI trials, which offers unusually comprehensive insights into its ongoing technological experiments.

External initiatives can contribute to public understanding too. A promising institutional approach involves algorithmic registers. That is, in some countries, police must disclose information to supervisory bodies about the systems they use, including details about data processing.[87]

The indirect effects of external oversight mechanisms also appear pertinent. When public procurement rules require law enforcement agencies to publish their calls and contracts, journalists and researchers can investigate what technologies they are purchasing and from whom. Supervisory bodies often have the authority to review law enforcement activities, ask detailed questions and conduct investigations, which creates another layer of accountability and transparency. A recent study in the Netherlands revealed that informing the public that an independent external body was overseeing the uses of predictive algorithms by law enforcement agencies significantly increased trust. Simply highlighting the existence of legal safeguards, mentioned alone or together with oversight, did not meaningfully boost trust though.[88]

2.3 Practical limitations and challenges

Notwithstanding its importance, transparency about AI innovation in law enforcement settings is no guaranteed path to public trust. The average, overall effect of transparency on trust might be positive, but these outcomes also depend on the context and the method used to implement transparency.[89] Both existing literature and several interviewed experts have emphasized important limitations.

86 Ritchie et al. (2021). Ibid. The Equality and Human Rights Commission. (2025). Accessible at: https://www.equalityhumanrights.com/met-police-use-facial-recognition-tech-must-comply-human-rights-law-says-regulator. Jeff Larson. (2016). How we analyzed the COMPAS recidivism algorithm. *ProPublica*. Accessible at: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

87 The Netherlands maintains a national register for reports by public authorities, including police, about their automated systems and human oversight requirements. The level of detail varies, and the requirements remain somewhat unclear, but even just creating a register can spark cultural change because it requires public organizations to reflect on their use of AI. In addition, civil society groups can use the register to foster dialogue and public debates about responsible AI deployment. The register is accessible at: https://algoritmes.overheid.nl/en

88 E. N. Nieuwenhuizen, V. Trehan & G. Porumbescu. (2025). Does institutional transparency affect citizen trust in predictive policing? Evidence from a survey-experiment in The Netherlands. *Public Administration*, forthcoming. Accessible at: https://doi.org/10.1111/padm.70034

89 Qiushi Wang & Zhen Guan. (2023). Can sunlight disperse mistrust? A meta-analysis of the effect of transparency on citizens' trust in government. *Journal of Public Administration Research and Theory*, *33*(3), 453-467. Accessible at: https://doi.org/10.1093/jopart/muac040

- First, meaningful transparency requires some *baseline level* of trust that law enforcement agencies act fairly and in accordance with responsible AI principles. Because transparency can uncover shortcomings and risks associated with AI uses, its positive effects will be limited if the implementation lacks clear governance and regulatory mechanisms or robust standards for the development, procurement and use of the technology. Efforts to build trust and increase transparency always take place within the specific historical and social context of the community, which strongly influences how the public will perceive law enforcement agencies' efforts to introduce new technology.
- Second, the benefits of transparency depend on *what information is disclosed* and how much detail is provided. Transparency about decision-making processes, for example, might lead to negative effects, because it can undermine perceptions of government competence.[90] Access to information might represent a form of transparency, but if the revealed information is not comprehensible, it is unlikely to produce positive outcomes. Information about AI systems can be particularly difficult for non-specialist audiences to interpret, such that it could increase their anxiety rather than their confidence.[91]
- Third, the effects of transparency depend on the *channel* through which it is communicated. Digital media channels (e.g., government websites, social media) might be less effective than face-to-face or community-building efforts. In addition, simply depositing and passively storing information in digital repositories can be counterproductive. Large volumes of unsorted material and overwhelming disclosures can alienate the audience and reduce trust by prompting uncertainty, confusion and frustration.

Even if law enforcement agencies recognize these determinants of effective transparency measures, persistent institutional and contextual constraints can complicate their efforts to achieve transparency in practice. Persistent fears and uncertainties can affect how law enforcement agencies are able – or unable – to be transparent about their AI innovation practices. An especially salient challenge arises from inherently bureaucratic cultures that institute a broad reluctance to open up, as can be reinforced by an organizational culture of secrecy among law enforcement agencies. Operational pressures, limited resources and competing priorities can easily sideline long-term institutional reforms. These constraints do not reduce the importance of transparency, but they can inform the development of strategies that are realistic, sustainable and responsive to operational realities, as the practical recommendations that follow will suggest. Common constraints that law enforcement agencies encounter are outlined below.

90 Stephan Grimmelikhuijsen, Gregory Porumbescu, Boram Hong & Tobin Im. (2013). The effect of transparency on trust in government: A cross-national comparative experiment. Public Administration Review, 73(4), 575-586. Accessible at: https://doi.org/10.1111/puar.12047

91 Dorotic, Stagno & Warlop (2024). Ibid. Anca Florentina Vatamanu, & Mihaela Tofan. (2025). Integrating artificial intelligence into public administration: Challenges and vulnerabilities. Administrative Sciences, 15(4), 149. Accessible at: https://www.mdpi.com/2076-3387/15/4/149

Figure 4 – Common challenges to a transparency-first mindset

Organizational culture

Law enforcement agencies often struggle to be transparent in practice. The experts, across diverse backgrounds, including law enforcement, painted a generally discouraging picture of the current state of transparency and a deeply ingrained culture of secrecy. Historically prevalent beliefs have tended to assume that law enforcement agencies know what they are doing, that their activities are a matter for internal handling and oversight, and that all information is by default confidential. The resulting institutional culture discourages proactive information sharing.

The law enforcement experts noted specifically that details about AI system usage generally would be released only after the systems were in place. They described public engagement efforts, where existent, as *ad hoc*. The result is a one-way flow of information. Law enforcement agencies roll out new technologies, policies or procedures, without substantively revealing their rationales. Such disclosures fall short of meaningful transparency because they do not provide the public with opportunities to debate or scrutinize systems that have already been put in place. Only after the public learns and forms opinions about the AI systems, usually based on third-party information, do the law enforcement agencies offer explanations, which also creates difficulty for the agencies to make a convincing case for justifying their uses.

Operational secrecy

Legitimate and practical reasons limit transparency, particularly those related to national security and operational secrecy requirements. Law enforcement agencies must withhold information that might undermine investigations, endanger personnel or victims, facilitate crime displacement or otherwise compromise ongoing operations. Experts acknowledged though that this rationale is frequently overused, such as to shield their practices from scrutiny rather than protect legitimate operational interests. As one law enforcement expert clarified, most law enforcement activities can be revealed without detriment to public security or law enforcement work.

However, some interviewed law enforcement experts expressed concerns about the disclosure of technical details, arguing that it might defeat the purpose of introducing the AI system altogether

by exposing its vulnerabilities or facilitating reverse-engineering. Malicious actors could use such details to break into or exploit the system. Law enforcement agencies remain uncertain about which technical information they can release without creating new safety risks.

Operational secrecy and system security concerns grow strongest, and more legitimate, in relation to active investigations. Revealing methods could compromise evidence-gathering efforts. When law enforcement agencies are engaged in sensitive investigations, they can share information with judicial authorities under the strictest of confidentiality. A law enforcement expert described how their organization conducted internal reviews to determine whether and why certain technologies could not be publicly disclosed, with careful documentation of the reasoning for such secrecy.

An expert from the security sector added though that secrecy does not necessarily prevent exploitation by malicious actors, who often find vulnerabilities regardless of what is publicly disclosed. Instead, greater transparency can stimulate external stakeholders to provide relevant feedback for strengthening the system's robustness and safety, which ultimately contributes to, rather than eroding, public security. As these contrasting perspectives highlight, and as > USE CASE SNAPSHOT 3 clarifies, tensions thus persist and vary, depending on the type of technology implemented and the risks for public safety.

Use Case Snapshot 3:
Tension between public accountability and operational effectiveness

When implementing AI systems for surveillance, transparency creates a complex, persistent tension between public accountability and operational effectiveness. On the one hand, disclosing too much technical detail can enable individuals to alter their behaviours and evade the systems. As one law enforcement expert put it, informing the public that certain public spaces are under surveillance can deter crime, but it might also displace those crimes towards unmonitored "blackout" zones rather than resulting in a real reduction. On the other hand, transparency is critically important when AI systems are used for surveillance, because this involves monitoring entire populations rather than specific suspects, creating heightened risks for privacy and other human rights (> SEE LEARN MORE BOX 3).

Regarding the AI4Citizens use case scenario specifically, the experts generally identified no compelling reasons to withhold the use of the AI system. They did not anticipate any significant reduction in efficiency due to public knowledge of how the system works. Thus, they proposed that transparency should prevail. As a law enforcement expert emphasized, given the widespread deployment of cameras in public spaces, there are few security risks associated with transparency. Yet, in this hypothetical scenario, it would be sufficient to inform that AI systems are deployed to analyse footage of CCTV cameras in a particular area, without disclosing the precise location of the CCTV cameras. Experts drew a parallel with other widely used AI systems such as automatic number license plate recognition systems, which the public generally knows and accepts, without needing information about precise camera locations.

Commercial secrecy

The AI systems used by law enforcement agencies are sometimes developed by private-sector entities, often through public–private partnerships. In these scenarios, the private entities (which understand the AI systems and possess all technical information) retain a commercial interest in them, which incentivizes them to highlight the positive features of their products. Reflecting this commercial goal, the private-sector entities might insist on contract provisions that prevent law enforcement agencies from publicly revealing product information. They might also withhold some technical details from the law enforcement agencies, in an effort to protect their proprietary and commercial interests. Notably, a recent survey showed that 84% of surveyed United Kingdom citizens expressed their fear that, in developing AI regulations, governments would prioritize partnerships with large technology companies over the public interest.[92]

A key area in which the public seeks transparency is the procurement process and the suppliers of technical equipment. Civil society organizations and human rights experts highlight the persistent lack of information about which AI systems law enforcement agencies use, the processes through which those systems were developed and acquired, and the identity of the actors that control or are responsible for the system. For a law enforcement expert, public–private partnerships remain too opaque. Public announcements of projects rarely include information about which private companies are involved, how public funds have been allocated or the results of the implementation.

Insufficiency of legal requirements

Existing legal obligations require law enforcement agencies to share information. But they appear insufficient to induce meaningful information sharing. Through Freedom of Information (FOI) requests, any person can request access to information held by public authorities. In response to FOI queries about law enforcement agencies' uses of AI systems though, the answers often are meagre. It appears that law enforcement often is treated like an exception to transparency requirements, whether due to long-standing legal exceptions for national security or to ongoing investigations. As noted previously though, it also appears that law enforcement agencies invoke "operational secrecy" as a default explanation. They believe that detailing how they collect information, connect data points or conduct certain investigative steps would jeopardize ongoing operations or provide criminals with ideas for evading detection. One law enforcement expert went as far as to warn that publicly disclosing which AI systems are in use would unintentionally reveal what systems they lack and their vulnerabilities, information of value to criminal actors.

Resource constraints

As public entities, law enforcement agencies tend to be overburdened, understaffed and faced with competing priorities, so transparency is rarely their top priority. Furthermore, meaningful transparency practices, such as adequate communication campaigns and public engagement, are resource intensive. They require a skilled communications team and consulting experts, whereas many agencies lack any in-house communication experts at all, much less those trained in complex, technical subjects. Securing the necessary human and financial resources may be beyond the capacity of law enforcement agencies, especially at local levels.

92 Nuala Polo & Roshni Modhvadia. (2025). Great (public) expectations. *Policy Briefing. Ada Lovelace Institute.* Accessible at: https://www.adalovelaceinstitute.org/policy-briefing/great-expectations/

Fear of public backlash

With their conservative cultures and bureaucratic structures, law enforcement agencies are typically slow to adopt new technologies. By the time they do, the public may have developed preconceived (negative) views that complicate the agencies' efforts to be transparent about their AI implementation. This situation increases the resources required to be open about AI systems, because it tends to initiate multiple waves of inquiries – informally during public engagement activities and formally through continued FOI requests. They also tend to express reluctance to open themselves to outside scrutiny, especially when the risk of backlash is high. Without clear guidelines or binding obligations to communicate proactively, their information-sharing likely becomes an afterthought rather than a routine practice.

3. Recommendations: Cultivating a transparency-first mindset

Law enforcement agencies need consistent, coherent communication and a culture of openness, across their hierarchies, to achieve alignment and reinforce their collective public security mission. This section offers key considerations for how to develop and maintain an organization-wide culture of transparency that reflects these values.

Be responsible and trustworthy

To foster and maintain public trust, you need to act fairly, openly and responsibly at all times, including when introducing AI systems. This means working in good faith and in the best interest of people, protecting their well-being and human rights, and making decisions that are consistent and unbiased, without favouring certain groups over others. It is not possible to build public trust on the technical capabilities of the AI systems you use. You must explain openly why you are using that particular AI system, and you must outline what safeguards are in place.

To establish these practices, you should engage in responsible AI innovation whenever you plan, develop, purchase or use AI systems. This entails taking steps such as the following:

- Agree on the purpose of introducing an AI system, through the participation of all relevant stakeholders, before introducing it.
- Build necessary AI literacy skills in the organization so that anyone communicating about the AI has received adequate training and understand of how the system works.
- Establish responsible governance processes.
- Conduct impact assessments.
- Monitor and evaluate the system continuously, even after it is implemented, to ensure it works as intended and does not create new risks.

These internal processes, some of which are invisible to the public, will help you minimize risks associated with AI implementation and lessen the potential for public backlash, which in turn can strengthen public trust and confidence.

Invest in transparency

There is no getting around it: fostering a culture of transparency demands resources. To initiate a cultural change, from secrecy to transparency, you need proper processes, and to develop them, you need to invest time, personnel and monetary resources. Virtually every law enforcement agency struggles with resource constraints, as well as an essential core mission that cannot be compromised. However, investing in transparency will pay off in the long run. It strengthens the reputation and legitimacy of your organization, and it also fosters innovation by improving the public's general perceptions of AI and uptake of new technology.

Understand both the context and public needs

Key stakeholders have views on both your agency and AI, and these two perspectives interact in meaningful ways. Public attitudes might range from hopeful to fearful, and these starting points shape how people receive the disclosures you offer. Transparency is more likely to build trust if a baseline level of confidence already exists. In addition, revealing too much, or overly complex, information can be counterproductive and lead to confusion instead of confidence. Use available surveys, public consultations, interviews, focus groups and social media analyses to learn what the people you serve expect, what concerns them and what they prioritize. Do so on a recurring basis. This way, you can keep aligning your transparency practices with the reality of your context.

Be patient. Be consistent

Trust is hard to gain and easy to lose. The gradual, dynamic process of building trust demands consistency and commitment over time. Expect to keep undertaking sustained action to demonstrate the reliability and accountability of your organization. To cultivate and maintain trust, it is up to you to stay attentive to the diverse needs and expectations of different individuals and communities, as well as their current and historical experiences with law enforcement.

Get an early start, then stay ahead

Start pursuing transparency as early as possible. A previously prepared communication vision and plan can help you stay focused on your goals. Waiting for the public to discover your uses of AI systems is likely to backfire. Instead, involve lots of people in the conversation from the outset, even before making the AI system adoption decision. Make these affected individuals and communities feel legitimately included in the effort to identify and find solutions to the problems at hand. Then, after

the AI systems have been implemented, continue to embrace this proactive approach. Voluntarily, proactively share information, instead of waiting for questions or FOI requests for disclosure. Doing so not only maintains trust but also limits the spread of disinformation. The first story told generally is more visible and persuasive than the correction. It is also easier to inform than to debunk. Regular updates should highlight key milestones, critical results (e.g., risk assessments, findings from third-party evaluations) and success stories.

Tell positive, truthful stories

The public needs to hear about how introducing AI has supported the agency's mission to serve the common good and public safety. You might particularly emphasize its potential for crime prevention and responsible investigations. Because law enforcement is such a complex and sensitive context for AI implementation, it requires relatable examples rather than abstract claims. When possible, ground success stories in concrete, real-world examples and data (i.e., show, don't tell). Describe specific moments when the AI system contributed to a positive community outcome. But avoid unrealistic narratives.

Tell realistic stories of challenges and mistakes too

Provide the public with honest acknowledgements of the risks and limitations associated with AI. No AI system is infallible; every system requires appropriate measures taken to prevent and minimize harm. Explain your ongoing efforts and the safeguards in place to prevent discrimination, profiling or misuses of the technology. If errors or misuses arise, acknowledge the problem openly, take accountability and detail the action you will take, such as investigating thoroughly, assigning responsibility and reassessing uses of the AI system. If necessary, commit to enhancing broader organizational readiness too. In addition to communicating these corrective measures, invite external oversight bodies or stakeholders (e.g., ombudsman offices, data protection authorities, community representatives) to take part. Addressing mistakes properly and promptly and exhibiting a willingness to learn and improve is empowering and beneficial for the organization. It can also strengthen public trust and support for responsible innovation.

Specify what you cannot share and why

In a law enforcement context, not all information can or should be disclosed. Operational secrecy, ongoing investigations and system vulnerabilities may require confidentiality. However, secrecy about *what* is being done should not extend to *why* it is being done, according to which rules and safeguards. If you cannot share specific details publicly, purposefully explain the reasons for non-disclosure. Where required, share such sensitive information with judicial authorities or independent oversight bodies, with strict confidentiality guardrails, and highlight that practice to the public. Although your contracts with technology providers might impose additional constraints, do your best to integrate transparency obligations into procurement contracts too, to avoid a situation in which contractual obligations prevent your agency from disclosing information that the public has a right to know.

Prepare to respond

When interested parties ask questions or raise concerns, it is your responsibility to respond quickly, with well-prepared answers. To do so, you should anticipate common questions and prepare clear, accurate responses in advance. The responses need to reflect your genuine understanding of the AI systems in use, their limitations and risks, their advantages and their broader impacts. These responses should come from well-trained human representatives, not automated systems, to signal accountability and credibility. Ready-made answers might not be possible in unforeseen scenarios, but you should still develop a substantial response as soon as possible, balancing urgency against sufficient internal investigations and thorough information checks.

Always keep improving

Mistakes are inherent to innovation and growth; approach them as opportunities to learn and improve. Transparency and trust are never static; they require continuous effort and adaptation. Design your transparency initiatives to include continuous progress control and updating elements, because every new communication will affect public trust and perceived openness. Use the lessons you have learned and solicit continuous feedback to review your processes, assess risks, evaluate results and then iterate accordingly.

Chapter 2

Communicating about AI innovation

1. What is the point of public communication?

Public authorities have the duty and responsibility to ensure the right to access to information and implement adequate institutional measures to guarantee this right.[93] Sharing information, through communication, ideally increases understanding among people or groups too.[94] With regard to the focus of this report, it implies providing details about the objective and reasons for using AI systems. In particular, law enforcement agencies have **positive obligations to explain** their AI innovation policies and practices to individuals and communities, as well as how they align with the public interest. Effective communication about AI, by law enforcement agencies acting in good faith for the purposes of protecting the community and creating a safe environment, is vital to fostering trust and acceptance of AI implementation decisions.[95]

Given the inherent power imbalance between law enforcement agencies and the general population, any communication failures can be especially detrimental, triggering suspicion and concerns about the possible harms to human rights. This may also be exacerbated by any disparity between public expectations of rigorous AI governance, responsible use and their capability to understand the complex technical capabilities and limitations of AI systems.[96] These negative effects undermine **public trust and confidence** in law enforcement agencies, which already are held to a higher **standard of trust** than private companies[97] and rely on trust to achieve "policing by consent." It is thus not sufficient for law enforcement agencies to use AI systems only in a lawful, ethical and effective way. They also must ensure that the public perceives their uses as lawful, ethical, responsible and effective. That outcome demands proactive, continuous and clear communication about AI adoption, use and existing safeguards, addressed to all audiences and at all stages.

When law enforcement agencies communicate, they aim to **signal their reputation** of being approachable and open. Such communications can establish that the agencies are not tech-resistant or sceptical but instead are realistic about the potential of AI systems. Beyond their own reputation, communications can influence public perceptions of the AI systems being used. Although people likely have **preexisting perceptions of AI**, those views tend to be vague and shaped by unverified information, obtained from diverse, non-expert sources (e.g., social media, press articles, previous encounters with AI). The unregulated practices and lack of due diligence among private-sector actors can create further confusion, such as when they institute unannounced updates, make non-transparent and untraceable amendments to terms of service or offer only highly technical documentation. Thus, even if seemingly outside their core objectives, law enforcement agencies must also take responsibility to communicate about **responsible uses of technologies** to support public safety, particularly in relation to the safeguards associated with the use of AI systems.

93 The Tashkent Declaration on Universal Access to Information, CI/UAI/2022/55, 28-29 September 2022, UNESCO, Accessible at: unesdoc.unesco.org/ark:/48223/pf0000383211/PDF/383211eng.pdf.multi

94 Cambridge Dictionary, Accessible at: https://dictionary.cambridge.org/dictionary/english/communication.

95 Sagana, Zhang & Sauerland. (2025). Miller. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence, 267*, 1-38.

96 Ada Lovelace Institute. (2025).

97 In evaluations of diverse AI applications across public and commercial contexts, the similar technical solutions have been evaluated with higher scrutiny and seen more exploitative if used by public entities, particularly for law enforcement-intended applications. See Dorotic, Stagno & Warlop. (2024).

Use Case Snapshot 4: The importance of clear and transparent information

The mere presence of cameras in public areas does not establish widespread understanding of their functioning or use by law enforcement agencies. Without clear, readily available information, people likely develop misconceptions that might trigger greater fears of surveillance or human rights abuses. For example, when people see camera installations in the streets, they might mistakenly assume everything is being recorded, and the acquired data are stored indefinitely. In the use case scenario though, the cameras do not undertake indiscriminate video monitoring or store data permanently. An AI system that supports anonymization and anomaly detection is installed on preexisting cameras. Moreover, organizational safeguards such as limited storage times, requirements for human oversight and training on legal and ethical requirements are in place. Such measures indicate due diligence and responsible innovation by the law enforcement agency deploying the AI system. Thus, communicating such AI system's function and purposes proactively, as well as protective measures and safeguards, seems critical as it can help the public understand agencies' efforts to protect their rights. On the other hand, providing such information only in service or technical documentation is unlikely to be sufficient.

Many people lack the technical background needed to read and comprehend user agreements, cookie messages, legislative acts or registers of AI systems. Some struggle to understand what new technologies do and fail to realize when they are interacting with AI systems. Such concerns tend to be exacerbated among older populations, populations who lack access to certain communication channels and those suffering from inequalities in access to education. Communication should be designed to raise **awareness** and even **literacy** about the AI systems being used for public safety,[98] which in turn can enhance perceived trustworthiness and accountability.[99] The deploying agency therefore should take the lead in clearly and truthfully explaining its usage of such technologies, especially if they differ from people's reasonable expectations or preexisting assumptions (> SEE USE CASE SNAPSHOT 4). People who are affected by a new device or application should not be required to engage with complicated policies, but they should receive information about them, in a way that improves understanding and supports informed acceptance of these AI systems.[100]

In addition, various groups perceive law enforcement agencies differently, particularly if they have experienced a prior history of over-policing or biased decision-making.[101] To establish and encourage dynamic, context-dependent forms of trust, law enforcement agencies need to identify and respect such variations, which can help them craft more effective communication strategies. Ignoring them risks alienating individuals and communities and undermining compliance. Meaningful communication demands more than a tick-box exercise to display basic compliance with legal requirements or policies. It must be based in transparency and trust. Only then can it help maintain public confidence and trust in law enforcement agencies' implementation of AI systems.

98 Sousa et al. (2018).

99 Sagana et al. (2026).

100 Office of the Privacy Commissioner of Canada. (2025). 2025 G7 Data Protection and Privacy Authorities Roundtable Statement: Promoting Responsible Innovation and Protecting Children by Prioritizing Privacy. ,paras. 7-8. Accessible at: https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2025/js-dc-g7_20250619.

101 Sousa et al. (2018). Florentina & Tofan. (2025).

2. Effective communication strategies

The interviewed experts cautioned that communications about technology are unique, especially in a public context. This section presents communication approaches that can support effective communication with the public when AI is at stake.

2.1 Define the problem

Before any thoughts of AI implementation, responsible AI innovation requires that law enforcement agencies raise and answer a fundamental question: *What specific problem do we seek to solve with this technology, that is, for which purpose do we need this system?*[102] Accordingly, before a law enforcement agency approaches the public regarding its plans to use AI systems, it should define the problem that needs solving. Then, it can identify alternative solutions, establish why other options are not sufficient and why AI is the best choice. The purpose and the problem must be defined through a public needs and benefits lens, not in relation to internal needs or the mere availability of new technological capabilities.

Immediate assumptions that AI is the best or only solution can lead to hasty implementations that lack the necessary degree of transparency and accountability, skip necessity and proportionality analysis and ignore privacy and data protection requirements.[103] Therefore, the initial consideration must involve whether AI should be deployed at all. If that analysis suggests it should be, the next step is considering if and how it might be genuinely useful, in a public policy sense, as depicted in **> USE CASE SNAPSHOT 5.** Law enforcement agencies must be able to answer, internally or externally, fundamental questions such as, *Do we need AI to solve the identified (public benefit) problem? What risks to human rights or public wellbeing might this system impose? Will it create any risks to our reputation? Are there any less invasive means available to achieve the same objective?* To convince the public about the appropriateness of a decision to implement AI, law enforcement needs to be perceived as trustworthy; it requires just as much trust to support the decision *not* to implement AI systems.

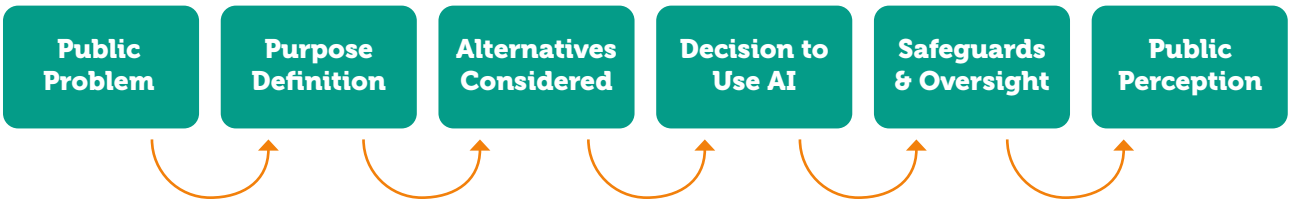


Figure 5 – Problem definition

102 UNICRI and INTERPOL. (Revised February 2024). Toolkit for Responsible AI Innovation in Law Enforcement: Organizational Roadmap. Accessible at: https://ai-lawenforcement.org/sites/default/files/2025-03/Organizational_Roadmap_Mar25.pdf

103 Luca Belli, Walter Britto Gaspar & Nicolo Zingales (2024). Regulating facial recognition in Brazil: Legal and policy perspectives. Working paper, Getulio Vargas Foundation Law School Rio de Janeiro. Accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5204265. Rita Matulionyte & Monika Zalnieriute (Eds.) (2024). *The Cambridge handbook of facial recognition in the modern state*. Cambridge University Press.

Understanding the problem and formulating a clear purpose for the use of an AI system can also inform insights into the audience and support an appropriate communication strategy, laying the groundwork for meaningful, effective stakeholder engagement.[104]

Use Case Snapshot 5: Added value of the AI system

In the use case scenario, the responsible local authority identified strategic, high-traffic areas where crowd monitoring appeared essential for public safety. The live video captured by the cameras is immediately processed by an anonymization algorithm that transforms individuals into non-identifiable silhouettes. An anomaly detection algorithm then analyses the anonymized feed in real-time, looking for predefined abnormal behaviour that could warrant further action. Law enforcement personnel, trained in the system's functionality, as well as in its ethical and legal considerations, monitor the anonymized video feeds from a secure control centre and assess the alerts, deciding whether further action is required or whether the system issued a false alarm.

The goal of this AI system is to increase responsiveness to public needs, reduce crimes in crowded places and minimize burdens on personnel. The related public benefits should be at the forefront when communicating about its introduction. Such communications can also outline alternatives that were rejected as deemed less beneficial:

- Increasing police patrols of public spaces, which would have been expensive and financially burdensome for taxpayers.
- Assigning human operators to monitor public spaces constantly through live cameras, which would require additional police and costs while also increasing surveillance and privacy infringements. Human observers are also prone to mistakes, such as when fatigue increases the likelihood of missing anomalies.

104 European Centre for Not-for-Profit Law. (2025). Framework for Meaningful Engagement. Accessible at: https://ecnl.org/publications/framework-meaningful-engagement-20

2.2 Understand the audience

During the interviews, communication experts emphasized the importance of establishing the targets of the communication. All communication should reflect what people already know, how they feel about AI systems and their uses, whether they feel threatened by this technology and the source of any fear or lack of trust. In addition to identifying varying levels of technical and AI literacy, audiences' cultural, socio-political and personal characteristics influence their perceptions of communicated messages.

Beyond their perceptions of the message, diverse groups express distinct views on the institution implementing the AI system. As discussed previously, information gets filtered through preconceived judgements and trust in law enforcement agencies.[105] Therefore, communication experts call for efforts to understand people's concerns and then highlight attempts to resolve those concerns or underlying issues. Communicating openly about such identified fears and concerns signals that the agency takes them into account.

Furthermore, communication about an AI system should reflect audience evaluations of their usefulness and appropriateness, along with psychological responses to AI in general. People express fears about not understanding the inner workings of AI systems, overconfidence in humans' capabilities and uniqueness, concerns that AI cannot perform contextually complex tasks and worries that AI threatens human autonomy and sense of control.[106]

Different audience segmentation tactics can help define effective communication methods **(> SEE LEARN MORE BOX 4).** Segmenting audiences by their expressed trust levels or aligning messages with their psychological needs might enable law enforcement agencies to move past mere persuasion and towards shared opinions and genuine partnership. According to the interviewed experts, most people want to trust law enforcement and would welcome good communications that provide adequate assurances.

105 Stephan Grimmelikhuijsen, Gregory Porumbescu, Boram Hong & Tobin Im. (2013). The effect of transparency on trust in government: A cross-national comparative experiment. *Public Administration Review*, *73*(4), 575-586. Accessible at: https://psycnet.apa.org/doi/10.1111/puar.12047. Lum et al. (2020). Ritchie et al. (2021).

106 Julian De Freitas, Stuti Agarwal, Bernd Schmitt & Nick Haslam. (2023). Psychological factors underlying attitudes toward AI tools. *Nature Human Behaviour*, *7*(11), 1845-1854. Accessible at: https://pubmed.ncbi.nlm.nih.gov/37985913/ Chiara Longoni, Andrea Bonezzi & Carey K. Morewedge. (2019). Resistance to medical artificial intelligence. *Journal of Consumer Research*, *46*(4), 629-650. Accessible at: https://doi.org/10.1093/jcr/ucz013

Learn More Box 4:
A trust-based, three-way audience segmentation approach

In marketing, audiences may be segmented according to high or low levels of trust and of commitment to services provided by firms.[107] Applied to communication in the law enforcement context, that framework would look as follows:[108]

1. Among **people who trust law enforcement agencies,** with the belief that they are competent and act in accordance with the interests of the community, communication should focus on reinforcing their confidence by highlighting transparent decision-making and showcasing success stories. While this group does not require further convincing of the trustworthiness of law enforcement or AI uses, it may be receptive to further community engagement. To identify and target such people may be relatively less productive in law enforcement contexts though, because this audience already supports the agency and its deployment of AI.

2. **People who are sceptical or actively critical of law enforcement** likely seek out and follow information about AI-related activities. They might also possess the knowledge and expertise to identify shortcomings or raise difficult questions. This group is more challenging for communication, but they are not a threat to law enforcement efforts. Their motivations often align with the goals of law enforcement agencies, namely, promoting a safe and secure society in which law enforcement agencies act in the interests of all communities. Some communication experts call for prioritizing this group, because gaining their trust can have positive effects on other sceptics. To gain their trust though, simple reassurance is not enough. They demand reliable evidence, provided through clear and factual messaging that avoids technical jargon. Claims addressed to this group should appear together with independent audits, expert endorsements and other trustworthy resources. Cues of competence and reliability tend to resonate with people who fear misuses of power or institutional inefficiency.[109] Thus, these communications should emphasize existing safeguards, adherence to regulations or widely recognized guidelines, third-party oversight and proactive approaches for reducing the risks to the groups most vulnerable to and at risk of being disadvantaged or discriminated against.

2. **People who fall somewhere in the middle** often constitute the largest audience group and the majority of the population. This group might exhibit some variation in their levels of engagement and caution, but in general, they remain cautious or even sceptical about the use of AI by law enforcement agencies, even as they indicate their openness to being reassured of the trustworthiness of both the law enforcement agencies and the AI itself. Communication with this subgroup requires dedicated effort to reassure the audience and signal consistency, good faith, expertise and shared values.

107 Bertil Hultén. (2007). Customer segmentation: The concepts of trust, commitment and relationships. Journal of Targeting, Measurement and Analysis for Marketing 15, 256–269. Accessible at: https://doi.org/10.1057/palgrave.jt.5750051.

108 United Kingdom Home Office (2025). Public attitudes to police use of facial recognition technology. Accessible at: https://www.gov.uk/government/publications/public-attitudes-to-police-use-of-facial-recognition-technology/public-attitudes-to-police-use-of-facial-recognition-technology

109 Mayer et al. (1995).

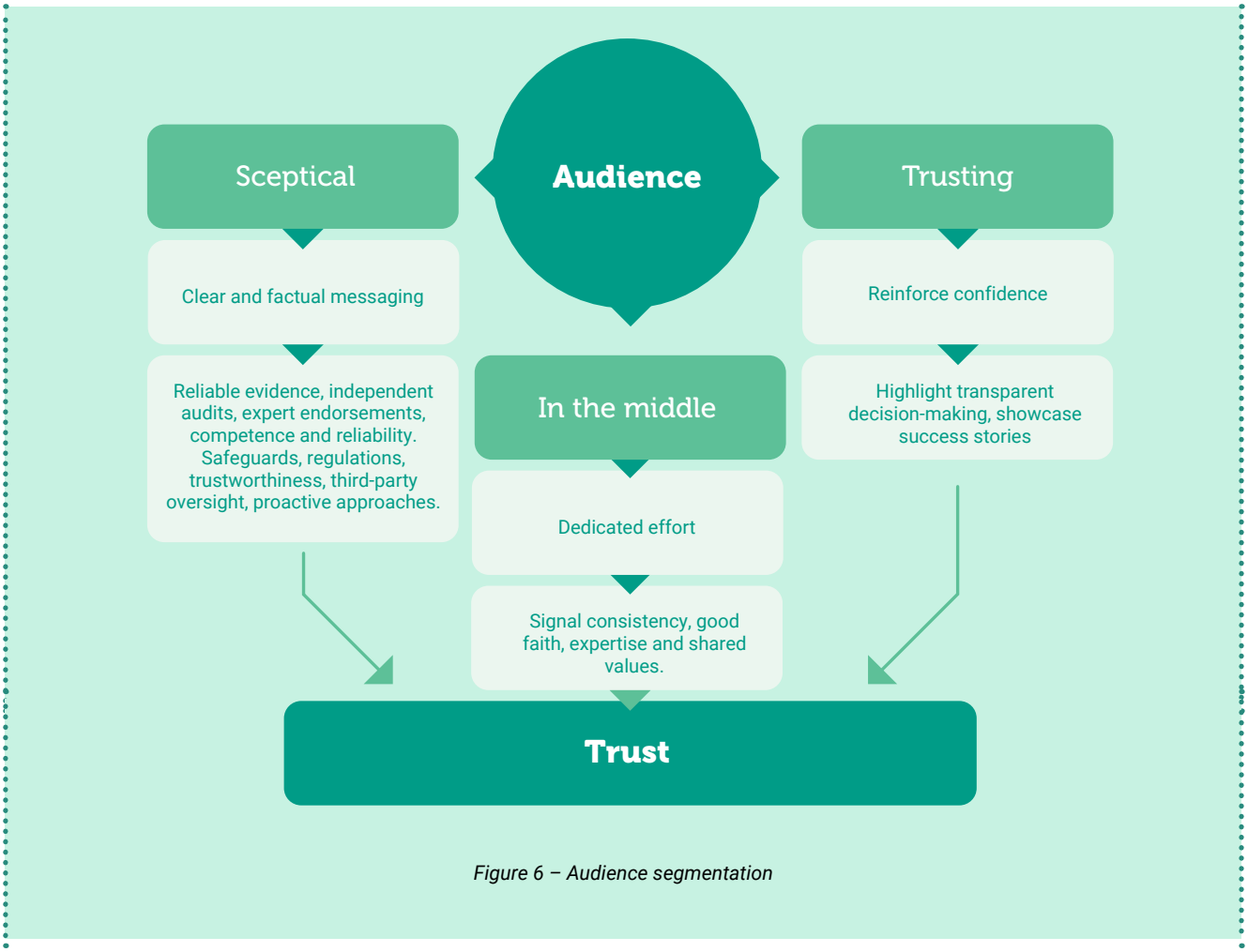


Figure 6 – Audience segmentation

2.3 Develop a communication strategy

Developing an effective communication strategy requires careful consideration of the overall communication goals, target audiences, and organizational capacity. Establishing such strategy early on, then applying it uniformly across all stages of AI adoption, can ensure that the provided information is consistent. It also creates space for feedback mechanisms. The communication strategy should act like a guide, mapping out core messages while also outlining plans for future activities involving specific target audiences (> SEE CHAPTER 2 – SECTION 2.2).

In detail, the strategy should specify the overarching **communication goals**, including when and how to share information with various stakeholders. A well-defined communication strategy can ensure common directions and alignment across diverse stakeholders and groups, consistent communication across different channels and initiatives, and ongoing considerations of the long-term integration of different initiatives. In particular, an integrated communication strategy holistically accounts for long-term goals, spanning not just a single AI implementation, channel or audience but instead encompassing a long-term vision for multiple communication plans that can implement the

Learn More Box 5:
Integrated communication strategy

A communication strategy might indicate: "We will run a social media campaign to promote our new AI system." An integrated communication strategy would add: "We will launch a campaign where social media, email, public relations (PR), internal newsletters, and influencer outreach all share the same core message and timing to create a unified message." That is, an integrated communication strategy ensures consistent tone, messaging and organizational images across multiple platforms and departments (e.g., marketing, PR, internal communications, digital). It spans internal and external communication efforts, such that each channel reinforces others for maximum impact.

If a law enforcement agency has an overarching message that it needs to communicate to different audience segments, such as about its responsible AI innovation, it should adopt an integrated communication strategy and rely on diverse media. The choice of each specific channel should reflect its goals for targeting specific audiences. Digital communication through social media platforms also provides expansive possibilities to fine-tune messages and target specific groups, based on their interests and concerns, which suggests it may be a good choice when introducing a single AI system.

The expert interviews and literature on public administration indicate that a common shortcoming in public sector communications about AI systems is the lack of clear, measurable goals. Instead, they exhibit an overemphasis on internal, administrative needs that prompt AI innovation.[110] In line with best practices in commercial settings, appropriate communication goals might include creating awareness (of the general AI strategy of the law enforcement agency and the specific AI system); conveying detailed information; describing tangible and intangible benefits; building trust through transparency, openness and accountability; and inspiring action and shared perceptions of common social values.[111]

In addition to specifying clear goals for communications, the strategy should establish key performance indicators that can measure the extent to which it has achieved these goals **(> SEE LEARN MORE BOX 6).**

110 Bernd W. Wirtz, Jan C. Weyerer & Carolin Geyer. (2019). Artificial intelligence and the public sector—applications and challenges. *International Journal of Public Administration*, *42*(7), 596-615. Accessible at: https://doi.org/10.1080/01900692.2018.1498103

111 Adopted from the marketing communication models of Batra and Keller. See Rajeev Batra & Kevin Lane Keller. (2016). Integrating marketing communications: New findings, new lessons, and new ideas. *Journal of Marketing*, *80*(6), 122-145. Accessible at: https://doi.org/10.1509/JM.15.0419

Learn More Box 6:
Six criteria for assessing communication effectiveness

Communication effectiveness and impact can be assessed according to six criteria:[112]

- **Coverage,** or the proportion of the audience reached by the communication, as well as who or which groups have been missed.
- **Contribution,** which assesses the effects on the audience, spanning both the outcomes it generates and the extent to which it produces the intended response.
- **Commonality,** reflecting the consistency of messages across channels.
- **Complementarity,** or the extent to which communication options reinforce one another in conveying a coherent message. It includes consistency across channels (e.g., websites, social media, public releases) and across personnel, units or departments within law enforcement agencies.
- **Confirmability,** reflecting whether the communication remains relevant and effective across citizen groups, regardless of their unique needs or vulnerabilities. Uniform communication may provide too much information for some groups and too little for others.
- **Costs,** which balance performance across the preceding criteria but cannot justify the absence of a long-term communication strategy.

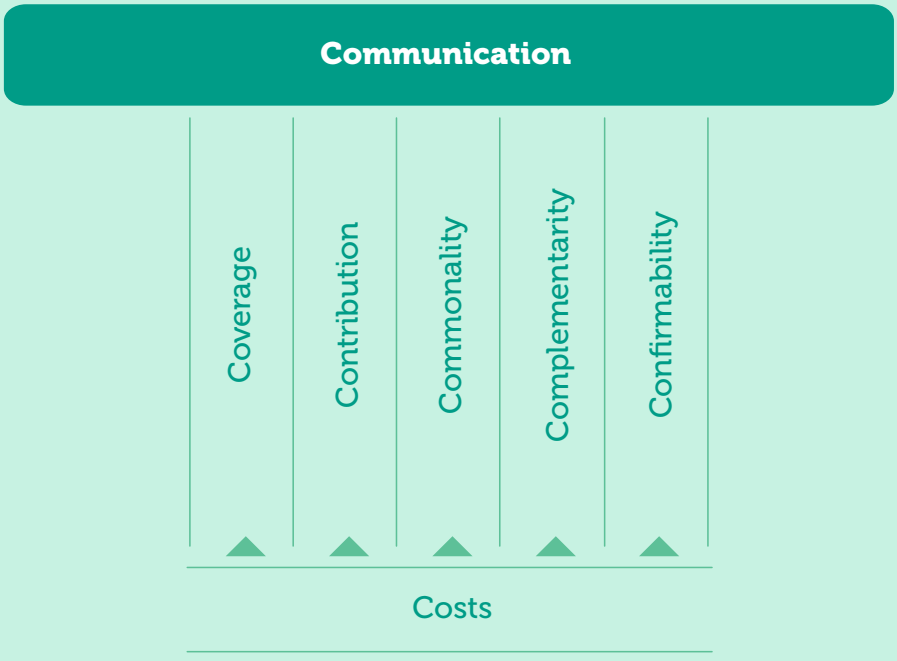


Figure 7 – The six Cs of communication

112 Kevil L. Keller. (2013). *Strategic brand management: Building, measuring, and managing brand equity* (4th ed.). Pearson Education. Accessible at: https://www.scirp.org/reference/referencespapers?referenceid=3044185

Preparing for communication with varied **audiences** is another important part of the communication strategy **(> SEE CHAPTER 2 – SECTION 2.2).** Understanding the audience can empower law enforcement agencies to more adequately select a communication strategy, the platforms for communication, the content and even the spokesperson in any particular instance. Different communication scenarios should be imagined and planned in advance. Similarly, it is good practice to prepare responses to information requests ahead of time. If the agency receives an information request from, journalists, civil society organizations or a member of the public, it can answer quickly and accurately, with a coherent story about its AI systems, without needing to improvise.

The interviewed experts also stressed the importance of the personality, expertise and reputation of the person, entity or group conveying the message. Perceptions of *what* is communicated is inherently shaped by perceptions of *who* communicates it. Law enforcement agencies, especially at a local level, likely lack the expertise or human resources to design meaningful communication about technical issues. Even for larger organizations though, aligning a trustworthy communication strategy with technical knowledge and specific contexts can create internal communication issues.[113] Thus, integrating trusted technical experts as intermediary links may be beneficial. Such communications might showcase that the AI systems was developed not by law enforcement agencies but by reputed scientists, who are available to answer technical questions. A representative from a university, with strong qualifications, might also act as a trusted stakeholder for communication purposes. If any other organizations participate in public safety efforts and also are involved in the AI system deployment or use, such as a private security company or municipality, they should be involved in the communication as well. Experts from different fields, cited in strategic communications, can adjust information to different target audiences. They also can increase the visibility of an AI system implementation.

Organizational capacity must inform such decisions. Depending on its financial and human resources and internal expertise, an agency may be able to leverage its internal communication department or public relations experts, or it may be forced to involve an external communication agency. This recommendation is not to suggest that law enforcement representatives are irrelevant. Experts cannot replace law enforcement agencies deploying the AI system, in communication, because public safety personnel must be present to establish the trustworthiness of the law enforcement agencies. In some jurisdictions, legal rules might also prescribe the types of communication that can be issued by public authorities. Therefore, law enforcement representative should be the first point of (communication) contact, which means they need to be prepared, equipped with both necessary information about the AI systems and relevant skills for understanding, respecting and effectively interacting with diverse audiences.

113 An OECD report covering 200 use cases across 11 government functions found that the main implementation challenges for AI in government and public services include technical skills shortages, outdated legacy systems, difficulties with data sharing and financial constraints. See OECD. (2025). *Governing with artificial intelligence: The state of play and way forward in core government functions*. OECD Publishing. Accessible at: https://doi.org/10.1787/795de142-en.

2.4 Convey essential information about the AI system and expand when necessary

Information about AI innovation in general should be accompanied by explanations of what specific AI systems are used and how their use is being managed responsibly. Not all new technologies are AI systems and members of the public cannot always be expected to make this distinction themselves. Framing a technology as AI can evoke preconceived notions, both positive and negative. Law enforcement agencies should therefore be deliberate in their use of the term, neither overstating nor understating the use of AI systems.

People are more likely to accept or adopt technology they believe they understand.[114] The general public is also likely to demand transparent explanations when an AI system contributes to high-stakes decisions such as those taken in the law enforcement context. **(> SEE USE CASE SNAPSHOT 6).** Alongside any mandatory information, required by each country's legislation **(> SEE LEARN MORE BOX 2),** examples from academic literature and existing digital governance recommendations, aligned with opinions expressed by interviewed experts, suggest that law enforcement agencies should aim to proactively provide the following essential information:[115]

- An AI system is, has been or will be used.
- The purpose of the AI system and its intended benefits.
- The process it uses to obtain outcomes (i.e. the type of AI algorithms and how they work).
- Its performance in terms of evaluation metrics and potential limitations.
- The data it processes and related data security measures.

For AI systems that may create lower risk to individuals and communities, such as those that do not process personal data or inform decisions with direct or indirect effects on the public, this information may suffice. Specifically, including "why" explanations to clarify the reasoning behind AI decisions can foster more positive attitudes than explanations that simply describe the system's actions.[116] Importantly, this information should be clear and intelligible and communicated in an adequate, timely and truthful manner.

114 Massimiliano Ostinelli, Andrea Bonezzi & Monika Lisjak. (2024). Unintended effects of algorithmic transparency: The mere prospect of an explanation can foster the illusion of understanding how an algorithm works. *Journal of Consumer Psychology*, *35*(2), 203-219. Accessible at: https://psycnet.apa.org/doi/10.1002/jcpy.1416. Romain Cadario, Chiara Longoni & Carey K. Morewedge. (2021) Understanding, explaining and utilizing medical artificial intelligence. *Nature Human Behavior, 5*, 1636–1642. Accessible at: https://doi.org/10.1038/s41562-021-01146-0

115 UNICRI and INTERPOL. (2024). Principles. Ibid. Belli, Gaspar & Zingales. (2024).

116 In driving simulations, Koo and colleagues (2015) found that participants responded more positively when a self-driving car explained that it was braking because of an obstacle, rather than simply stating that it was braking. See Jeamin Koo, Dongjun Shin, Martin Steinert & Larry Leifer. (2015). Why did my car just do that? Explaining semi-autonomous driving actions to improve driver understanding, trust, and performance. *International Journal on Interactive Design and Manufacturing*, *9*, 269-275. Accessible at: https://doi.org/10.1504/IJVD.2016.07674. S. Y. Kim Sunnie, Elizabeth Anne Watkins, Olga Russakovsky, Ruth Fong & Andrés Monroy-Hernández. (2023). "Help me help the AI": Understanding how explainability can support human-AI interaction. In *Proceedings of the 2023 CHI conference on human factors in computing systems* (pp. 1-17). Association for Computing Machinery. Accessible at: https://doi.org/10.1145/3544548.3581001

When the potential risks to human rights are greater, more detailed explanations are needed.[117] This allows people to exercise their rights better in the situations where AI systems are more intrusive. In general, in addition to and expanding on the essential information listed above, these situations should prompt communication about additional technical details such as:

- The characteristics of the training data, its sources, accuracy, representativeness and currentness, potential limitations, as well as whether and how these limitations were addressed (e.g. if checks for biases were conducted).
- Performance indicators, including how the performance of the system has been evaluated and the results of its deployment.
- Accountability, oversight and redress mechanisms, beyond what is prescribed by law, to convey the due diligence and transparency of the organization.

While implementation of more intrusive AI systems calls for disclosure of more (detailed) information, operational secrecy requirements in the law enforcement context may lead to exemptions from certain transparency obligations. Such exceptions, however, should be interpreted on a case-by-case basis and do not imply the exemption of law enforcement from transparency as a principle (> SEE CHAPTER 1 – SECTION 2.3.).

Use Case Snapshot 6: Communicating the AI system's functioning

In the use case scenario, the public needs to know about the installation of the AI system into the pre-existing cameras but also how the AI system functions, as it relates to the two algorithms that anonymize the collected data and analyse it to issue alerts.[118] Regarding the processing of data, the provided information should describe data storage, how long the data will be kept, safeguards in the case of data leakages or losses and measures that limit law enforcement agencies' ability to track and trace people who are not engaged in criminal activity. Applied to the use case scenario, the law enforcement agency's communication may look as follows:

User interface and alert management

- When an anomaly is detected, users receive an alert indicating unusual behaviour. This alert includes anonymized footage, geolocation data, timestamp, duration, and confidence detection (on the scale of 0–100%), thus allowing law enforcement personnel to quickly assess the context.
- Anomalies are not labelled as specific crimes but as potential safety incidents that need further investigation.

117 When an AI system is defined as high risk, some jurisdictions even impose specific regulatory and legal standards for communication. See EU AI Act, Articles 26(11) and 50.

118 Asres, Jiao & Omlin. (2025). Ibid.

Anonymization algorithm

- **Function:** Automatically anonymizes video footage upon capture. Human figures are fully masked to obscure personal attributes (face, body, clothing, phone screens) with a solid silhouette. Other objects (e.g., weapons, bags) are not anonymized.
- **Training data sources:** The data for training the algorithm come from publicly available datasets. The datasets were not specifically related to the context where the AI system is deployed, which might limit their accuracy. Bias checks were conducted.
- **Objective:** Prevent unauthorized access to personally identifiable information, ensuring that law enforcement personnel cannot recognize individuals.
- **Limitations:** Despite high accuracy, there is a margin of error resulting from (i) certain human figures not being detected and therefore not being masked; (ii) some characteristics being susceptible of being inferred from the anonymized footage, such as mobility aids, certain gender features, clothing styles or other objects.

Anomaly detection algorithm

- **Function:** Processes anonymized footage to identify abnormal events that could signal public security risks, such as shooting, explosion, road accidents, vandalism, assault or arson. Anomalies are defined as deviations from normal behaviour that may constitute threats to public safety.
- **Training data sources:** Trained on an anonymized version of publicly available datasets, using a weakly supervised learning method. The datasets were not specifically related to the context where the AI system is deployed, which might limit their accuracy. Bias checks were conducted.
- **Objective:** Prompt alerts for law enforcement to check and, if necessary, intervene in or investigate potentially dangerous situations.
- **Limitations:** Accuracy in detecting specific anomalies may vary across different types. A system set to minimize missed incidents (false negatives) might become too sensitive and frequently alert irrelevant events (false positives). Minimizing false alerts may lead to missed events that require intervention. Improved models are optimized to minimize errors while managing the trade-off between false positives and false negatives.

Data processing

- Only authorized personnel can access the anonymized footage (both in real time and post-event). However, because masking is not 100% effective in eliminating all personal identifiers, some personal data might still be processed and reviewed by users.
- The interface allows users to view the masked footage, evaluate the anomaly context and take action based on their assessment.
- Personnel only have access to raw (non-anonymized) footage when specifically authorized by a court warrant (for example, in the context of a criminal court case).

- The raw footage is stored in the CCTV cameras, which ensures higher data security. The camera executes the anonymization algorithm and sends the anonymized footage to the server system, where the anomaly detection is processed.
- Both the raw and anonymized footage are stored only for two weeks and automatically deleted afterwards.

Even if few people dedicate the time needed to engage with all this information, it should be easily accessible and searchable, such as on a public platform that is not access restricted.

Although these general considerations promise to be relevant to many forms of communication about the use of AI systems by law enforcement, no one-size-fits-all approach exists. Regional, cultural, historical and other nuances should inform what law enforcement agencies choose to highlight in their messages. Audiences across different contexts rely on different signals of the trustworthiness of AI systems.[119] For example, some audiences prefer information about policies and their outcomes rather than detailed descriptions of decision-making processes;[120] others seek moral and ethical rationales instead of technical justifications;[121] some audiences seemingly care only about accurate AI predictions;[122] and in still other cases, people prioritize social impacts, public benefits and public safety over protection of human rights.[123]

When it comes to adjusting information about the AI system to match the audience, it is not sufficient to solicit feedback from fellow law enforcement personnel; nor can the message solely represent developers' intuition about what constitutes a meaningful explanation.[124] Information that is important to internal agency processes or development considerations is not necessarily important to other audiences. To tailor the message to a specific audience, the communication strategy can take the platform and case into account and detail both recognition of the community's concerns (**> SEE USE CASE SNAPSHOT 7**) and measures that already have been taken.

119 Edwards Lilian & Michael Veale. (2017). Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18. Accessible at: https://scholarship.law.duke.edu/dltr/vol16/iss1/2/

120 Ostinelli, Bonezzi & Lisjak. (2024). Cadario, Longoni, & Morewedge. (2021).

121 Dorotic, Do & Bigman. (2025).

122 Anne-Marie Nussberger, Lan Luo, L. Elisa Celis & M. J. Crockett. (2022). Public attitudes value interpretability but prioritize accuracy in artificial intelligence. *Nature Communication, 13*, 5821. Accessible at: https://pubmed.ncbi.nlm.nih.gov/36192416/

123 Belli et al. (2024).

124 Tim Miller. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial intelligence, 267*, 1-38 Accessible at: https://doi.org/10.48550/arXiv.1706.07269. Retno Larasati, Anna De Liddo & Enrico Motta. (2020). The effect of explanation styles on user's trust. In Smith-Renner, A. et al. (Eds.), *ExSS-ATEC 2020: Explainable smart systems for algorithmic transparency in emerging technologies*. CEUR-WS. Accessible at: https://ceur-ws.org/Vol-2582/paper6.pdf.

Use Case Snapshot 7: Highlighting impacts on safety and public funds

When presenting a project for public consultation, the focus should be on how it will benefit the public, not the implementing organization. In the use case scenario, two key benefits should be highlighted:

- **Faster identification of potentially dangerous situations**. The AI system can assist personnel in identifying anomalies and emerging risks in real-time, which promises faster police responses to incidents and improved opportunities to avoid dangerous escalation of problems, contributing to safer public spaces. The system therefore should be framed not as an internal efficiency gain, but as a tool that enhances public safety through improved prevention.
- **More efficient use of public resources.** By improving operational efficiency and enabling more targeted deployment of personnel, the system can reduce unnecessary expenditures over time. This more efficient use of public funds may help ease financial burdens on taxpayers in the long run.

It may be equally important to remind the public that the system cannot be abused by law enforcement to track or trace people who are not engaged in criminal activity.

When handled properly and in good faith, communication with experts can also attract their support in delivering the message. Because AI today spans a vast, multidisciplinary domain, it cannot be explained fully by any single person, organization or discipline. Communication with and through experts can address this gap. If experts who understand how AI systems work publicly express confidence in the AI system adopted by a law enforcement agency, its wider acceptance may occur.

2.5 Adequately inform about AI risks and limitations

When disclosing the deployment and use of technology, AI in particular, it is not sufficient to concentrate on explaining the benefits and capabilities of AI systems. Specific features of AI (lack of explainability of the algorithm, black box problem, etc.) increase the potential of this technology to inflict harm. The power imbalance that is inherent in law enforcement relations with the communities further exacerbates such risks. Thus, responsible AI innovation calls for disclosure of potential risks of this technology, of its limitations and of measures undertaken to reduce them.

The interviewed experts expressed similar views, stressing that the disclosure of information about the use of AI systems appear to reinforce a specific narrative. This narrative is often abstract and opaque, marked by exaggerated techno-optimism that mimics the claims of private-sector suppliers, and by questionable promises of greater safety, efficiency and financial and human resource savings. For the general public, however, law enforcement agencies should share transparent information about the risks and potential harms associated with their uses of AI systems. This is especially relevant to audiences made up of the members of society who are most vulnerable to and at risk of

being discriminated against or disadvantaged by the use of specific AI systems, and who experience substantial discomfort with the idea that law enforcement agencies are deploying AI systems.[125] Open communications should include information about assessments of the human rights impacts of AI systems used in law enforcement. Presenting communications that highlight the benefits and improvements associated with the system while openly acknowledging its potential risks and safeguards applied to mitigate them represents a promising, balanced approach to introducing an AI system. Adding detailed explanations of how the system is likely to affect people's daily lives would make the information more meaningful and relevant.

In parallel, the agency should plan ahead for recovery communications, after potential errors. This plan should include insights into events or developments that are likely to lead to errors, along with descriptions of how those errors might manifest **(> SEE CHAPTER 2 – SECTION 2.5).** These insights help protect the public from the detrimental effects and consequences of errors, but they also help the law enforcement agency understand what information is useful and what is misleading, which factors may lead to errors, what needs attention and what can be discounted.

In order to be in a position to adequately communicate the risks and limitations of the AI systems they use, law enforcement agencies should require the system developer or manufacturer to inform them about them.

As these recommendations consistently indicate, a substantial degree of candour is required. Being honest when reporting on AI system performance, whether using metrics or narratives, signals the law enforcement agency's authenticity and determination to be trustworthy and to find innovative ways to protect the public safety.

125 See, for example, Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, UN Doc. A/HRC/55/60, par.33, https://docs.un.org/en/A/HRC/55/60.

2.6 Foster continuous communication: results and refinement

Finally, communication cannot stop at the moment the AI system is deployed. This continuous activity must keep informing people of intermediate effects and results. Any assessment of the effectiveness of an AI system seemingly should prompt communications conveying the information to interested audiences.

Success stories can shape and strengthen perceptions of AI innovation. They should feature evidence more than claims; they should also emphasize how the decision to implement AI systems has delivered real results. When law enforcement personnel lead or engage in such communication, assuming they are not public relations experts, they need training and insights into the importance of communicating success stories. As was the case for communicating about the purpose of AI systems, stories of successful AI implementation should reflect the particular context (**> SEE LEARN MORE BOX 7** for an example of how to build this communication).

Learn More Box 7: Contrastive explanations

To increase people's understanding of the rationale for AI-related decisions or events, the use of contrastive explanations proves as a particularly effective approach. Contrastive explanations inform why a specific decision was made as well as which alternative outcomes were ruled out, and why.[126]

This approach provides deeper insights into the decision-making process and the reliability and fairness of the system,[127] which can boost public confidence in the system's recommendations. People often do not seek information about why event "X" happened, but rather why event "X" happened instead of some event "Y". For example, when law enforcement are communicating to the public about a crime detected with the help of an AI system, instead of just stating that an anomaly was detected by an algorithm, a contrastive explanation would also explain that the system classified the event as an anomaly and ignored all of the activity classified as benign.

Crisis communications are equally important. If the technology goes wrong, imposing negative effects on some individuals or communities, law enforcement agencies risk losing public trust altogether. Regaining it demands even more effort and resources. Future communication campaigns

126 Cadario et al. (2021) experimentally tested how explanations influence engagement with an AI-based skin cancer detection app. Participants were shown one of two advertisements: a functional ad stating, *"Our algorithm checks if skin moles are cancerous,"* or an explanation ad stating, *"Our algorithm checks how similar skin moles are in shape, size, and color to cancerous moles."* The results showed significantly higher engagement with the explanation ad, indicating that understanding the mechanisms being AI outcomes enhances user trust and willingness to adopt the tool. Cadario et al. (2021).

127 Larasati et al. (2020). Miller. (2019).

become particularly difficult, because their starting point is farther from a successful result. Negative perceptions of the AI system, spanning different stakeholders, could also jeopardize the wider application of an otherwise good product. Still, ignoring the failure is not an option. In the event of revealed failures or public backlash, a key recommendation is to be ready to act immediately. Such readiness requires preplanning the response and putting recovery strategies in place. Rather than pretending as if nothing has happened, law enforcement agencies must acknowledge the errors and then outline the lessons they have learned to avoid similar issues in the future.

Along with the recommendation to be ready to act immediately, another consideration is the need to balance urgency with the need to take enough time to conduct a proper internal investigation and release only thoroughly verified information. An improper, misconstrued or inaccurate message can amplify negative narratives, especially if picked up by media outlets. Law enforcement agencies must obtain substantial and accurate information and then share it as soon as possible. Over time, consistent, truthful communication builds a strong track record. Reinforcing perceptions of transparency, legitimacy and reliability in turn makes future AI initiatives easier to promote and, ultimately, contributes to the trustworthiness of AI systems used in law enforcement.

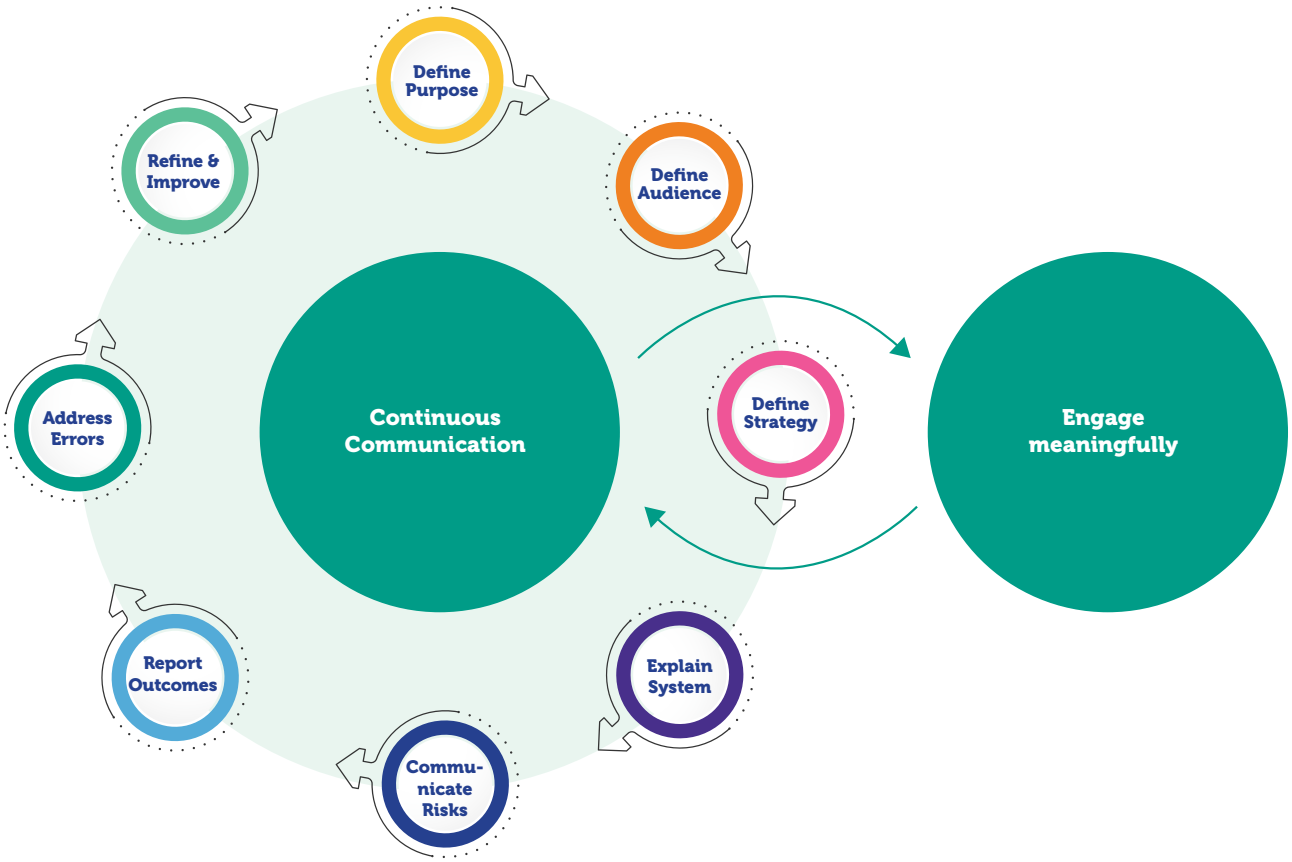


Figure 8 – Foster continuous communication.

3. Approaches and strategies to avoid

Several approaches to communication should be carefully avoided. The following list is not exhaustive: historical, political and cultural specificities can reveal other detrimental approaches that are likely to lead to undesirable consequences.

1. **Deploying an AI system "in secret" such that people must learn about it on their own, usually with negative consequences.** When an AI system is introduced covertly and only later discovered by the public, the potential for negative interpretations is vast. It seems destined to fuel misinformation and conspiracy theories. In that case, law enforcement agencies start communicating from a defensive position. Reversing an already formed public opinion, based on mistrust, is extremely challenging.
2. **Starting communication too late or not having any communication strategy at all**. Launching a late information campaign gives people time to form preconceived notions of the AI innovation policy or specific AI systems. The more challenging communication efforts in this case would need to focus on overcoming those preexisting impressions rather than shaping them.
3. **Misunderstanding the audience.** When defining audiences of communication efforts, it is unproductive to ignore nuances, such as personal and community experiences, their history of interactions with law enforcement and AI systems, media consumption or other influences. Identifying groups that feel threatened by technology and determining the source of their fear and distrust are challenging, but also essential steps for understanding audiences.
4. **Communicating without achieving sufficient public trust.** When law enforcement agencies communicate with audiences that already distrust them, the messages often have limited impacts or even unintended consequences, because the audience is sceptical about the intent behind the communication. If law enforcement agencies represent unreliable sources in their view, the information being conveyed is irrelevant. Even the most carefully designed communication strategy is unlikely to change that viewpoint. Rebuilding trust takes time, effort and attention. It might also require mediators who can bridge the trust gap. Yet communication efforts cannot be limited to easy targets, like existing supporters. Careful consideration is needed to find ways to communicate effectively with audiences who exhibit low levels of trust.
5. **Ignoring ethical considerations, conducing simple check-box exercises or only barely meeting legal requirements.** Responsible AI innovation demands meaningful adoption of AI systems, but the surge of AI may create an expectation that every organization and agency should embrace it. Instead, law enforcement agencies must avoid just following trends and conduct careful assessments and plans for integrating AI systems into their existing processes. Those assessments need to identify the problem to be solved, determine whether an AI system is necessary and offers value beyond that provided by less expensive or intrusive instruments, while performing ethical and human rights due

diligence analyses. The results of those analyses and assessments in turn should be communicated in detail, not just presented as a list of checked-off demands.

6. **Providing too much or too little information.** Overly complex, highly technical information can create misunderstanding and amplify concerns about the AI system's limitations and risks. Laypeople might reject complex communication and revert to a simple heuristic: the system feels "bad" because it is too difficult to understand. Too much information can also discourage people from engaging. Furthermore, being overwhelmed with information might prompt suspicions of covertness or trying to "trick" audiences. People already are overwhelmed by information overload. To read all the policies and terms of use they encounter on a daily basis, they would need to invest hundreds of hours of effort.[128] After information fatigue has set in, people avoid extensive explanations. But framing the information too simplistically can be problematic too, because people who are constantly bombarded with advertising, subscription notifications, cookie banners and other such messaging in their daily lives have developed metaphorical blinders that enable them to ignore additional signs and stickers.

7. **Conveying only the benefits of AI systems while ignoring the disclosure of risks.** Concerns about the risks of AI have increased significantly in recent years.[129] When used to support decision-making, AI makes procedural risks – particularly those related to fairness, accountability and lack of human oversight – more salient.[130] Communication efforts should not ignore such concerns by downplaying the drawbacks and substituting them by a techno-optimistic narrative, often by citing numbers and statistics about the capabilities of AI systems. When messages do not address public scepticism or fears of adverse outcomes, rather than conveying information authentically or in good faith, such communication efforts ignore the needs and preferences of their audience.[131] Law enforcement agencies should reinforce consistency in terms of conveying AI uses and policies, instead of reacting only to questions or pressure from media and civil society organizations.

128 Aleecia M. McDonald & Lorrie Faith Cranor. (2007). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society, 4*(3). Accessible at: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf. I Wagner. (2022). Study shows privacy policies are longer and harder to understand in 2021, De Montfort University Leicester. Accessible at: https://www.dmu.ac.uk/about-dmu/news/2022/february/study-shows-privacy-policies-are-longer-and-harder-to-understand-in-2021.aspx

129 Ada Lovelace Institute. (2025).

130 Hobson et al. (2023).

131 A. M. van der Bles, S. van der Linden, A. L. Freeman & D. J. Spiegelhalter. (2020). The effects of communicating uncertainty on public trust in facts and numbers. *Proceedings of the National Academy of Sciences, 117*(14), 7672–7683. Accessible at: https://doi.org/10.1073/pnas.1913678117

4. Recommendations: Communicating with clarity

Earning public trust requires acting in good faith and then showing that you have done so. It is up to law enforcement agencies to demonstrate that their AI systems align with the public interest. Clear, understandable information about AI initiatives, shared according to strong, strategic communication practices, can go a long way towards building confidence and trust. Poorly designed and insufficient communication instead can cause perceptions of uncertainty and a lack of safety.

This section offers practical recommendations for **what** you should communicate, to **whom**, **when** and **where** such communication might be more effective, and thus **how** you should go about it. The applicability of these recommendations varies with different contexts, because not all measures will be relevant for all AI systems or across unique societal and institutional conditions. It is up to you to consider these factors in deciding which measures will be most appropriate.

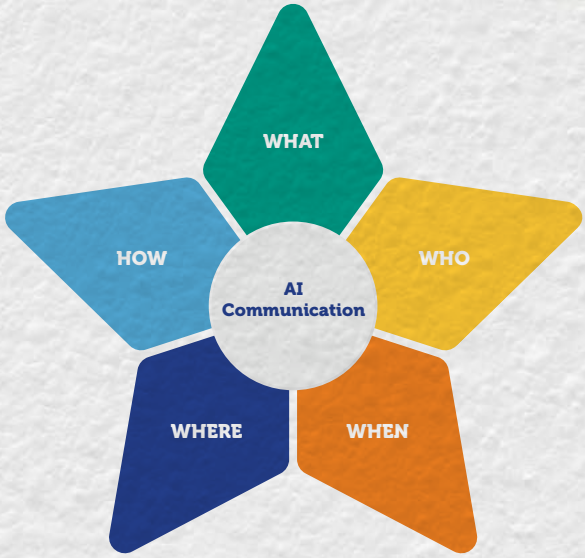


Figure 9 – Communicating with clarity

What to communicate

Effective communication provides as much information as possible, without undermining the confidentiality necessary for operational secrecy, while avoiding overwhelming the public with unclear or excessive detail.

- **Communicate clearly.** Explain the purpose and goals of your communication efforts to demonstrate your responsible and trustworthy conduct. Share plans and demonstrate that processes are transparent, inputs are well-founded and outcomes are clearly defined. Help the public understand the process, inputs and results throughout the system's life cycle.
- **Disclose the use of AI systems.** Tell the public when AI systems are being used, explain what the systems do and detail how you are using them responsibly. Always tell people ahead of time when they are interacting with an AI system.

- **Explain how AI serves the public interest.** Provide context and details to establish that your approach to innovation aligns with the public interest. Such details should include insights into:
- Organizational strategies, such as an AI innovation strategy, and initiatives to increase AI literacy and training of personnel.
    - Governance frameworks, such as oversight mechanisms, risk assessments and third-party evaluations.
    - Other information that might be of public interest, including information about public tenders, procurement processes and partnerships with academia or the private sector.
- **Explain accountability measures.** Describe both existing and planned accountability measures, such as audits and risk assessments, to demonstrate structured oversight. Make reporting and complaint mechanisms readily accessible and recognize them as meaningful sources of reviews that can also signal your good faith and strengthen public trust.
- **Go beyond minimum disclosure requirements.** All legally required information obviously must be disclosed, but do not stop there. Move beyond such legal minimums and engage in proactive transparency to build your credibility and foster long-term public trust.
- **Balance transparency with operational integrity.** You might not be able to disclose every detail or identify each AI system in use, but share as much information as possible. You might describe built-in safeguards and security measures in general terms to reassure the public while still preserving operational integrity.

Decisions about what to communicate also depend on the AI system adopted and the audiences you target, as the following points specify.

Communicating about specific AI systems

The level of information you disclose about each AI system should be proportionate to the impact on human rights.

- **Offer simple disclosures when the risk is low. Offer more detail when the risk is greater.** If an AI system poses minimal risk to human rights, basic information about the AI system and its purpose may be sufficient. If an AI system could have significant implications for human rights, provide more detailed disclosures. In particular, describing risk assessment and mitigation measures can help the public, and more detailed technical information should benefit expert audiences.
- **Clearly establish individual rights.** You need to make individuals aware of their rights when you use an AI system, including their right to be informed that AI contributed to a decision, to request meaningful explanations, to challenge or appeal outcomes, and to access information about procedural safeguards that promise to uphold fairness and equality.
- **Increase disclosure when individuals are directly affected.** Individuals who are directly subject to the outputs of an AI system, such as those accused or convicted of a crime following investigations that relied on the system, must be granted substantial transparency.

Tailor communication to the audience's needs

Communication initiatives need to reflect the characteristics and needs of different target audiences. You should attempt to identify each audience's level of AI literacy and interest in technical details to determine how much detail to share.

- **Pursue a two-tiered approach.** Introductory but essential information can go to general audiences; more detailed and technical explanations should be ready for stakeholders with advanced knowledge or specific interests.
- **Share only what is needed, not everything.** Achieving a sufficient level of transparency for all implementations of AI systems does not demand disclosing every detail. The public does not need to know everything to have enough knowledge.

For a general audience

- **Provide a general description of the AI system.** Explain its purpose, what it does, the type of algorithm(s) it uses and how they work.
- **Communicate the rationale.** Share, in plain language, why the AI system was introduced and how you expect it to benefit users or the public.
- **Explain benefits, risks and impacts.** Describe the benefits of the AI system relative to previous practices or other approaches. In these descriptions, emphasize the expected benefits but also recognize potential risks, so that the public understands the trade-offs involved.
- **Specify data processing practices.** Reveal which data, and especially personal or identifiable information, the AI system will collect and process, how long those data will be stored and why, whether the data will be reused and for what purposes, and what security measures exist to ensure their confidentiality, integrity and availability.
- **Also specify which data are *not* collected.** Whenever applicable and relevant, confirm that some data are not collected, such as personal and sensitive data, or reassure the audience that cross-border transfers will not take place. Indicate when long-term storage is not part of the data processing practices too.
- **Provide a contact for concerns.** Indicate whom the audience members should contact if they believe their rights have been adversely affected, together with instructions for how to submit complaints or request redress.
- **Specify the actors involved.** Explain who is involved in the deployment of the AI system and their exact roles, including:
    - Who operates the system, including law enforcement agencies, municipal councils, city councils, transport authorities or private-sector entities. Also indicate whether and which information or data may be shared across these entities.
    - Who might operate or access the AI system in the future, considering potential projects and relationships between public agencies and the private sector.

- Who developed the system, who acquired it, who is maintaining it and the roles of any third parties, beyond operating the system.
- Who has decision-making power over when the system will no longer be used.
- Who has access to the AI system and its data.
- Who is in charge of the collected data.
- Who is accountable if something goes wrong.

For expert audiences

Stakeholders with advanced knowledge or specific interests should receive detailed technical information so that they can assess the AI system's performance and overall efficiency.

- **Explain system capabilities.** Describe how the AI system works, what it can do, and how it was developed (e.g. which learning methods were used, - supervised, unsupervised or reinforcement).
- **Specify human control and oversight mechanisms.** Provide contextual details about the extent to which the AI system is monitored and how it supports human decision-making. Explain the uses of its outputs to assist human decisions. Make the system's operating parameters available if appropriate.
- **Communicate rationales for adoption.** Emphasize why a particular AI system was chosen over human-only processes. Present the system's performance metrics and list the priorities, criteria and evidence behind the choice to adopt the AI system, such as unsolved public needs. Then grant audiences the system's performance metrics.
- **Share costs.** Calculate and share the costs associated with the AI system, then compare them with any evidence used to justify its adoption, such as cost-effectiveness analyses.
- **Disclose training, testing and validation data.** Detail which data were used to train, test and validate the AI system. Indicate its sources, accuracy, representativeness and currentness and describe which data attributes contribute to the system's performance.
- **Disclose the technology developer.** Indicate the entity or team that developed and supplied the system, whether internal or external to your organization.
- **Provide relevant documentation.** Consider detailing regulations, policies, terms of use, training materials, standard operation procedures and other documentation available to operators of the AI system.
- **Reveal the results of built-in safeguards.** When appropriate, publicize impact assessments, results of quality certifications and results of tendering systems to reflect the fairness and security of the AI system.
- **Showcase accountability.** Describe which institutional mechanisms ensure that the AI system deployment follows the original plan and avoids misuse. The detailed description could highlight oversight mechanisms, audit results and activities taken in response to public feedback.
- **Specify safeguards and consequences for failure.** Commit to specific actions when required conditions cannot be met or the AI system is abused, including procedures for addressing failures, corrective actions and accountability measures.

Who to involve in the communication

Law enforcement agencies should lead and own their communication efforts, as a way to demonstrate trustworthiness and accountability. However, because AI is a multidisciplinary domain, communicating about its deployment demands the involvement of multiple actors, internal and external to law enforcement agencies, including:

- **Multidisciplinary experts.** Involve experts from different fields in your communication strategies. They can help you tailor your message to the needs and level of understanding that characterize your target audiences. Continuously work to expand your network of experts. Working with the same selected partners limits the reach and effectiveness of your messages.
- **High-level representatives.** Ask high-level members of law enforcement agencies, municipalities and other public authorities to function as spokespersons in your communication efforts.
- **Field officers.** Give law enforcement officers in the field enough information about the AI system's deployment that they can share while directly engaging with the public.
- **Communication experts.** Involve public relations and communication specialists who can tailor your message to different audiences, according to geographic, cultural and societal differences. For larger law enforcement agencies, an in-house communication team might be essential.
- **Legal and ethics experts.** Ask individuals or teams with legal and ethics expertise – both internal and/or external – to support your communication initiatives with insights about AI risks and harms, mitigation measures, and legal and regulatory frameworks that govern the system's use. External experts' independence signals accountability for the AI system's use and impacts.
- **Academics.** Cooperate with universities, researchers and other trusted technical experts, who offer both expertise and credibility.
- **The technology provider.** If possible, showcase a trustworthy relationship with the technology provider or vendor. Ask it for support in delivering messages on the AI system's technical specifications and replying to specific technical questions.
- **Civil society organizations.** Talk to civil society and community leaders, who are key intermediaries who can effectively convey your message to the public, particularly vulnerable individuals and communities **(see Chapter 3)**.

When to communicate

Effective communication should begin as early as possible and continue throughout the entire AI innovation process. To maintain such extended efforts, strive to do the following:

- **Establish a clear communication strategy from the start.** If you do not establish a communication strategy at the start, you cannot apply it in every stage. Defining it early on enables its application throughout all AI innovation stages. The strategy should outline when and how to share information, about the overall innovation efforts and the specific AI systems involved.

- **Constantly provide and seek information and feedback.** Information about AI system implementation should appear at every stage, together with details about feedback mechanisms.
- **Think long-term.** Long-term communication strategies move beyond implementation, citing clear actions for each stage (pre-, during, post-introduction) that align with the overall purpose and vision of the communication strategy.

Where to communicate

An integrated communication strategy spans diverse channels, so it requires a holistic approach to align and coordinate all these communication platforms and the messages that appear on them. Such consistency requires that you:

- **Maintain a presence across communication channels.** Actively participate in digital media, physical spaces and broadcast platforms (e.g., television, radio) to achieve broad coverage, reinforce messaging and attain complementarity across channels.
- **Communicate in different formats.** Host presentations. Give interviews. Publish press releases. Visit podcasts. You can prioritize more suitable formats for the different audiences you target.
- **Take care to avoid excluding audiences with limited access.** Not everyone has Internet access. Different communities and societal groups (e.g., youth, expats, refugees, day labourers) receive information and engage through different channels.
- **Select channels according to audience engagement.** After you determine how different target audiences access and engage with information, use the appropriate formats accordingly, such as radio messages broadcast at various times, different TV channels, regional and national newspapers, diverse social media platforms, and posters in public locations such as transport hubs or supermarkets located in different communities.
- **Maintain a website.** Information about your AI system deployment should be constantly available on a dedicated website, which should also host links to other pertinent resources.[132]
- **Provide clear, recognizable identifiers.** Use visible signage and recognizable logos on hardware components, like cameras and drones, so the public can easily identify the AI system being uses in public spaces.

How to communicate

The methods that law enforcement agencies use to communicate with the public, expert audiences and other stakeholders should reflect relevant considerations, such as the risk level of the AI system and the target audiences. In general, to communicate effectively, you should:

- **Demonstrate lawful, good-faith conduct.** Show that your activities comply not only with legal requirements but also with the underlying intent and principles of the law.

132 See the recommendation to use clear, large fonts on visible signs or stickers under "The power of visually appealing messages."

- **Use different formats to reach diverse target groups.** Adapt communications to reach youth, people with low literacy or limited resources, and community members with disabilities by offering accessible and inclusive options, such as simple visuals, audio, translations and easy-to-read layouts.
- **Ensure information accessibility for people with disabilities.** Ensure people with disability can access communications on an equal basis. Follow principles of universal design. Provide information in accessible formats, appropriate to different types of disability.

Some more specific recommendations emerge for powerful verbal and visual communications, as detailed below.

The power of appropriate language

- **Use clear, accessible language.** Simple, plain terms are effective for everyone but especially for people with limited AI literacy. Then adapt messages to local contexts, to ensure it is relevant and easy to understand.
- **Avoid information overload.** Too much detail, especially in settings already marked by information overload, will undermine rather than support transparency.
- **Avoid overly technical information.** Using highly technical language can make information difficult to process and understand, even for experts but especially for general audiences.
- **Create layered information designs and provide clear follow-up options.** Preparing materials with varying levels of complexity can address the needs of stakeholders with different backgrounds, interests and levels of expertise. Concise, essential details can be supplemented by links, QR codes or contact information that makes it easy for people to obtain more information and exercise their rights, if necessary. For example, the following steps can be productive in shaping layered information designs:
    - Provide basic information in simple language that is interactive, engaging and appealing, in places where people are most likely to interact with the AI system.
    - Add links leading to more detailed information on your institutional website.
        - Provide files with key specifications, links to legal resources or academic research on the topic (if available).
        - Complement it with the links to explanations by experts with different backgrounds, adjusted to distinct audiences
- **Communicate in relevant languages.** Make information available in multiple languages, particularly if more than one official language or different languages are commonly spoken in your country or region.

- **Recognize and address people's concerns.** You are communicating with people whose perceptions have been shaped by their backgrounds and experiences. Acknowledge those influences in a meaningful and respectful way, mindful that a lack of transparency can reinforce existing fears and mistrust, particularly among communities that already feel vulnerable or scrutinized.
- **Make it fun if possible.** Amusing and entertaining examples can lighten the tone. Humour also can make you feel more approachable and build human connections with audiences.

Figure 10 – Appropriate language

The power of visually appealing messages

- **Use clear, large fonts on visible signs or stickers.** Information in an easy-to-read format, without small print, avoids burdening people who already might be fatigued by having to read too much text in their daily lives.
- **Use visuals and other media formats to reinforce messaging.** Consider graphics, images and animations to convey short, effective and appealing messages and help people understand the information quickly and clearly.
- **Cite real-world examples.** Choose scenarios that are relevant to your audiences, so the message feels practical, familiar and easy to understand.
- **Strike a balance between too technical and not technical enough.** A clear general message ("what does the system do and why") can be presented together with a "learn more" option that leads audiences to additional resources (e.g., FAQs, articles, videos, external links) that they can explore at their own pace.
- **Use tactile, interactive or engaging formats.** Touch screens, maps and physical displays (e.g., depictions of showing camera coverage) encourage people to interact more directly. Physical engagement creates intimacy, builds trust and makes the system feel more accessible.

Chapter 3

Public engagement with AI innovation

1. What is the point of public engagement?

For law enforcement contexts, public engagement refers to a structured, two-way process of dialogue and collaboration between law enforcement agencies and the public that aims to foster trust, mutual understanding and knowledge exchanges. The public includes a broad range of stakeholders, such as individuals and communities, civil society organizations, academia, and the private sector. Such public engagement is essential for obtaining support, ensuring accountability and implementing AI systems in ways that respect human rights and rule of law principles. Beyond a mere public relations exercise or consultation that may get ignored in later decision-making stages, public engagement must create space for meaningful dialogue and allow law enforcement agencies and other authorities to hear community concerns, especially from civil society organizations, religious groups and underrepresented voices. Done well, public engagement supports the successful co-creation of safety strategies.

This collaborative, two-way exchange cannot just include attempts to convince the public that existing practices are "good." Rather, to foster trust and meaningful co-creation, public engagement needs to be organized to include deliberative, consensus-oriented processes that foreground reason-giving, public justification and accountability to encourage openness and shared responsibility in joint decision-making. Without a foundation of dialogue and inclusion, even well-intentioned technological innovation attempts might backfire. Such concerns are especially relevant for AI systems that can threaten human rights. The perceived intent for an AI introduction and the risks it creates powerfully drive people's acceptance and support for AI implementation in public settings.[133] When surveillance systems are introduced without genuine conversations with the public and other key stakeholders though, such AI implementations can prompt perceptions that the technology is more intrusive than it actually is or that it has been introduced for nefarious reasons.

Public engagement depends on multiple factors, such as a country's democratization level, historical tensions between law enforcement and specific communities and broader socioeconomic contexts, to name just a few. To gauge the opinions and needs of diverse segments of the population, public engagement efforts thus must span a range of formats: focus groups and interviews, public surveys, deliberative polls, town halls, discussions with vulnerable individuals in their communities and so on. Informal communication channels (e.g., social media, community meetings led by religious leaders or civil society organizations) can be key to reaching traditionally underserved members of the community. Depending on the circumstances, law enforcement agencies must adopt different approaches to gain access to multifaceted perspectives and voices, as is required to be able to align their strategic communication about deploying AI systems in public safety with their public engagement efforts.

133 Dorotic, Stagno & Warlop. (2024). Ibid.

2. Effective engagement strategies

Designing public engagement strategies requires answering four central questions. These questions aim to shift the notion of engagement away from opinion gathering and towards a process that can credibly inform decisions, such as about the use of AI systems in law enforcement, as exemplified in > USE CASE SNAPSHOT 8.[134]

- **How inclusive is participation?** Inclusiveness requires that participation is not limited to the most vocal stakeholders but also gathers members of the broader public, and especially the groups more likely to be affected by the use of the AI systems.
- **How thoughtful is the process?** Thoughtful processes ensure that these participants become informed, have access to balanced information, consider competing arguments and can deliberate on trade-offs rather than simply gaining affirmation of their initial views.
- **What effect does the public engagement aim to achieve?** To determine the intended effect, law enforcement agencies should imagine what changes are likely, in terms of knowledge, priorities or judgments, and try to anticipate what decisions people would support if they were well informed. If law enforcement agencies' decisions match what people would support once they understand the use of AI systems, it may reduce backlash later and build credibility.
- **In what conditions can it work?** Relevant conditions include social, political and institutional elements that may make high-quality participation more or less feasible, including safeguards against repression, dominant groupthink and institutional commitments, to ensure the process has a genuine impact on the relationships between law enforcement agencies and the public.

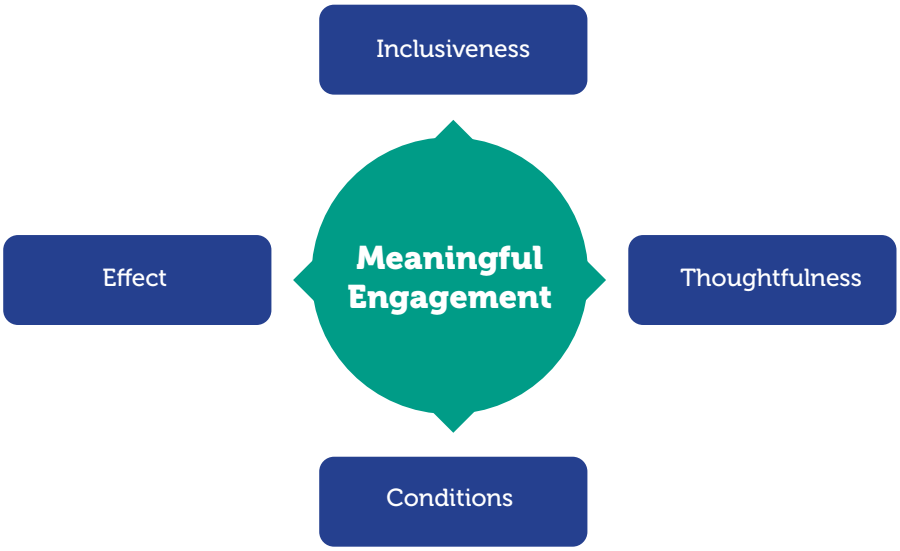


Figure 11 – Key elements of meaningful engagement

134 James S. Fishkin. (2009). When the people speak: Deliberative democracy and public consultation. *Oxford University Press.*

Use Case Snapshot 8:
Engaging the public, regularly and transparently

In the use case scenario, the law enforcement agency needs to engage with the public regularly and transparently to foster mutual understanding and encourage public trust in the use of the new technology. Based on the guiding questions outlined above, the agency could build an effective public engagement strategy, aimed at building and upholding trust around the new system, by asking themselves:

- Which different individuals and community groups are **involved** in shaping and approving the use of the AI monitoring system?
- **How carefully** is the AI system designed, deployed and evaluated to protect rights and build trust?
- Which specific public safety **effects** does the system intend to deliver, and how are they measured?
- **What conditions** must be in place for the AI system to operate effectively and responsibly?

In addition to, and in parallel with, these broad questions that should guide any public engagement efforts, the interviewed experts suggested common considerations and principles for engaging the public, as specified below.

2.1 Start early and be consistent

Engaging at an early stage, then constantly including people in the AI innovation journey, is critical for ensuring that the AI systems adopted by law enforcement agencies offer real value once they are implemented. The public should participate at every step of the AI innovation process, from inception to internal development or external procurement of the AI system, through to its deployment and eventual decommissioning. It is particularly important to gather public input before the actual deployment of AI systems, including their sense of the nature of the problem and efforts to co-design a solution for it.[135] To ensure that public engagement remains timely and relevant, law enforcement agencies also need to actively maintain their efforts over time, while updating their best practices and operating procedures to reflect shifting priorities. Early engagement strategies must prioritize public needs and benefits, rather than technical solutions (> SEE CHAPTER 2 – SECTION 2.1). For example, before deploying body-worn cameras in 2021, Scottish law enforcement agencies entered into dialogues that described different scenarios in which their use could help individuals and explained their own interest in using all technologies available to keep communities safe. Furthermore, transparent conversations about standard operating procedures, implementation policies and training materials for police personnel helped foster the development of trustworthy relationships.[136]

135 UNICRI and INTERPOL. (2024). Principles. Ibid.

136 Scottish Police Authority. (2024). Body Worn Video – Public Briefing. Accessible at:https://www.spa.police.uk/publication-library/body-worn-video-public-briefing/public-surveys/.

2.2 Understand the underlying dynamics

Public engagement strategies should reflect the emotions and perceptions of the public towards law enforcement agencies. More broadly, understanding and acknowledging all parties' feelings, concerns and perceptions regarding the use of AI systems provides meaningful information that can shape responsible uses of AI by law enforcement agencies and thereby influence whether the public accepts or rejects them. Further considerations of the importance of AI perceptions are presented in **CHAPTER 1 - SECTION 1.2.**

Such perceptions also are dynamic, so tracing the relationship between law enforcement agencies and the public is crucial for developing and implementing effective public engagement. If the public perceives law enforcement agencies as mainly devoted to state control, individuals and communities will tend to be more resistant to the arguments these agencies put forth, so they must devote more effort to building meaningful communication.[137] Intermediaries, such as trusted community groups or civil society organizations, can be particularly helpful in establishing such meaningful connections.

With regard to how law enforcement agencies perceive the public they serve, a critical consideration is the recognition that law enforcement personnel are not neutral actors. They carry their own perceptions that shape their interactions with the public. Behind their uniforms, they are humans with emotions, lived experiences and unique perspectives. If law enforcement personnel perceive communities as hostile or uncooperative, more interested in finding errors than sharing constructive feedback, their engagement efforts may become more performative than genuine. Recognizing this human dimension helps counter the tendency to limit personnel's roles to functioning solely as institutional actors and creates space for empathetic dialogue and opportunities to build trust.

2.3 Thoughtfully engage with vulnerable groups

The experts strongly emphasized the importance of dedicating particular attention to engaging with vulnerable groups, including over-policed and underserved individuals and communities. However, their composition, needs and grievances differ across contexts. Therefore, true engagement with diverse, vulnerable groups requires trust-building approaches that are carefully tailored, culturally sensitive and responsive to their unique lived experiences. Trust can be fostered only if law enforcement personnel demonstrate transparency in their operations and deliberately avoid covert practices or tactics that deepen existing mistrust.

Determining the existing level of distrust provides a foundation for effectively engaging both vulnerable and highly polarized groups. Beyond gauging the level, efforts should be directed towards understanding the causes of such distrust, by listening to participants' perspectives and the causes of their distrust. Here again, meaningful engagement might benefit from the involvement of trusted intermediaries, especially if the goal is to reach strongly opposed individuals, groups or those who have historically experienced harm at the hands of authorities. Addressing fears surrounding AI systems is essential as well, which can be achieved by offering information sessions, training and demonstrations of how AI systems support personal and professional development. Such efforts

137 Vatamanu & Tofan. (2025). Ibid.

help demystify the technology and reduce anxiety around its use.

A relevant risk arises from this recommendation though – namely, the risk of tokenizing vulnerable groups or unintentionally reinforcing stereotypes, which can further alienate the communities that engagement efforts aim to include. Such practices often discourage participation completely, underscoring the need for thoughtful, respectful, and genuinely inclusive strategies.

2.4 Plan for effective public engagement

For many places, public engagement in policing remains a novel approach. To introduce and normalize this idea, it should be included as a regular goal, such as among the priorities set and outlined in annual police plans. In some jurisdictions, such a plan is a statutory document.[138] Such a statutory approach, involving a legally mandated framework that requires public bodies, including law enforcement, to engage with communities and report how this engagement has shaped their decisions, offers a clear demonstration that communities' participation is influential and also holds agencies accountable for the outcomes.

An effective public engagement plan should account for time, people and monetary resource requirements. It takes time to build trust, understand community perspectives and engage in meaningful dialogue. Well-qualified human resources, including not just from law enforcement personnel across hierarchical rankings but also religious leaders and intermediaries, increase the chances that engagement is inclusive, representative and grounded in real needs. Finally, adequate funding supports practical engagement needs: outreach activities, fees to rent venue and catering services, accommodation and travel for participants and so forth.

2.5 Collect public input and establish feedback mechanisms

Collecting public input and feedback can spark a constant information loop between the public and law enforcement agencies throughout the life cycle of AI systems. Feedback mechanisms might include public surveys and annual assessment reports that are designed specifically to give people sufficient time to engage. They bring incident reports and complaints to the attention of law enforcement agencies and relevant external authorities. At the same time, they provide the public with channels for accessing justice and effective remedies.

After AI systems are established, law enforcement agencies should also assume a critical view of their systems, based on careful acknowledgement of the public's concerns. They should solicit additional input from other stakeholders, like academia and civil society organizations, that can check and confirm that they have integrated all the public feedback they receive into their decision-making processes. Furthermore, law enforcement agencies need to remember that negative feedback can be constructive. Even refusals to answer a survey could indicate a general lack of trust and highlight the need for more sustained efforts to encourage public engagement.

138 In Scotland, for example, the Annual Police Plans (APP), required by Section 35 of the Police and Fire Reform (Scotland) Act 2012, must describe how policing objectives align with community needs, which include "engagement and public contact". Scottish Police Authority & Police Scotland. (2025). Annual Police Plan 2025/2026 (pp. 21). Accessible at: https://www.scotland.police.uk/spa-media/z51avgov/annual-police-plan-2025-26.pdf.

2.6 Make engagement work by including diverse external stakeholders

Law enforcement agencies often have limited time to engage with external stakeholders, and it can be temptingly easy to collaborate only with supporters within a community, but a multistakeholder approach is the most effective way to achieve successful deployment of AI systems. When founded in the conscious application of standards of inclusivity, objectivity and reliability; explicit goals to bridge the knowledge gap between technical and non-technical communities; and clear recognition of power imbalances among actors, diverse stakeholder engagement creates complementary, balanced insights. For example, academics might not fully grasp the operational and stakeholder dynamics in the private sector; public institutions may lack the technical knowledge needed to properly evaluate or question private-sector solutions. Collaborations involving both academia and civil society organizations bridge such gaps. In this sense, considering the different roles of various categories of stakeholders in public engagement and communication efforts may be helpful:

- **Academia** offers empirical evidence and rigorous research approaches. Viable evidence is a cornerstone for building trust, so including academic research can increase trustworthiness, along with the effectiveness of new solutions and policies.
- **Journalists** can consult with law enforcement agencies, then verify and disseminate relevant information.
- **Civil society organizations** often have insights into the needs and beliefs of certain communities, and they can function as trusted messengers that can contribute to constructing an effective narrative. Increasingly, these organizations also have experience with the deployment of AI systems for law enforcement. For instance, some civil society organizations raise awareness about inequalities in AI development and access across the Global South compared with the Global North. To combat such inequalities, civil society organizations often advocate for continuous information exchanges, as a way to avoid exacerbating existing issues and replicating mistakes, as well as to share best practices and lessons learned.
- **Policymakers and government representatives** encountering complex technologies might lack initial knowledge of them; their expertise lies in other areas. However, they need to understand the technology to be able to regulate its use and engage in redress or oversight.
- **Local governments, institutions and public offices** need to be involved in conversations and decisions about AI systems in law enforcement, because they know the key stakeholders within the community and also can guide the process by asking the right questions to the most appropriate actors.
- **External oversight bodies** provide independent, objective and expert evaluations to build public trust and ensure accountability in AI systems' implementation.
- **Developers and providers of AI systems or digital infrastructure** are responsible for providing all the related information and documentation to law enforcement agencies.

For instance, they need to disclose risk assessments, the limitations of their algorithms, and their data sources and collection methods, to enable users to understand the potential impacts, evaluate data reliability and make informed decisions. Particular attention is required when private sector developers are involved. Engaging private companies requires a clearly established legal basis that specifies which data they may lawfully access, process or repurpose in designing and developing their AI systems. They should also be required to obtain explicit consent from affected individuals where applicable. Failing to hold private companies to such standards can undermine public trust, weaken accountability and create opaque data ecosystems, such that neither communities nor oversight bodies can fully understand how information is being used, or misused.

- **AI experts** can raise technical questions about system ownership and data location, as well as flag risks prior to the deployment of the AI systems. Given their expertise, they serve as credible sources and important collaborators, including for advocacy purposes. Independent AI experts can provide objective evaluations of potential risks and harms; experts who are funded or employed by technology companies should clearly disclose their affiliations and any potential conflicts of interest to safeguard transparency and trust.
- **Privacy experts** similarly can share feedback on the overall implementation process and its ability to preserve privacy, as well as offer advice on where to install the AI system (e.g., where to put cameras), based on clear criteria.
- **Content creators and influencers** who collaborate via social media platforms can share non-technical narratives to reach diverse audiences.
- **Other categories of professionals** likely have relevant insights too, in their roles as informational hubs with the potential ability to navigate difficult conversations. Faith leaders, healthcare workers and other professionals (e.g., hairdressers, baristas) often develop trust in a community and receive nuanced information about people's concerns, such as the impacts of wearing turbans or hair braids on privacy-preservation matters related to the use of AI systems. Such professionals also might foster grassroots discourses between law enforcement agencies and distrustful communities.

Reflecting the distinct needs of these multiple stakeholder groups, the content and approach must be adjusted: while more straightforward engagement and communication efforts can be offered for the general public, other stakeholders, such as developers and providers of AI, privacy and AI experts, and oversight audiences, require deeper technical explanations and risk assessment results.

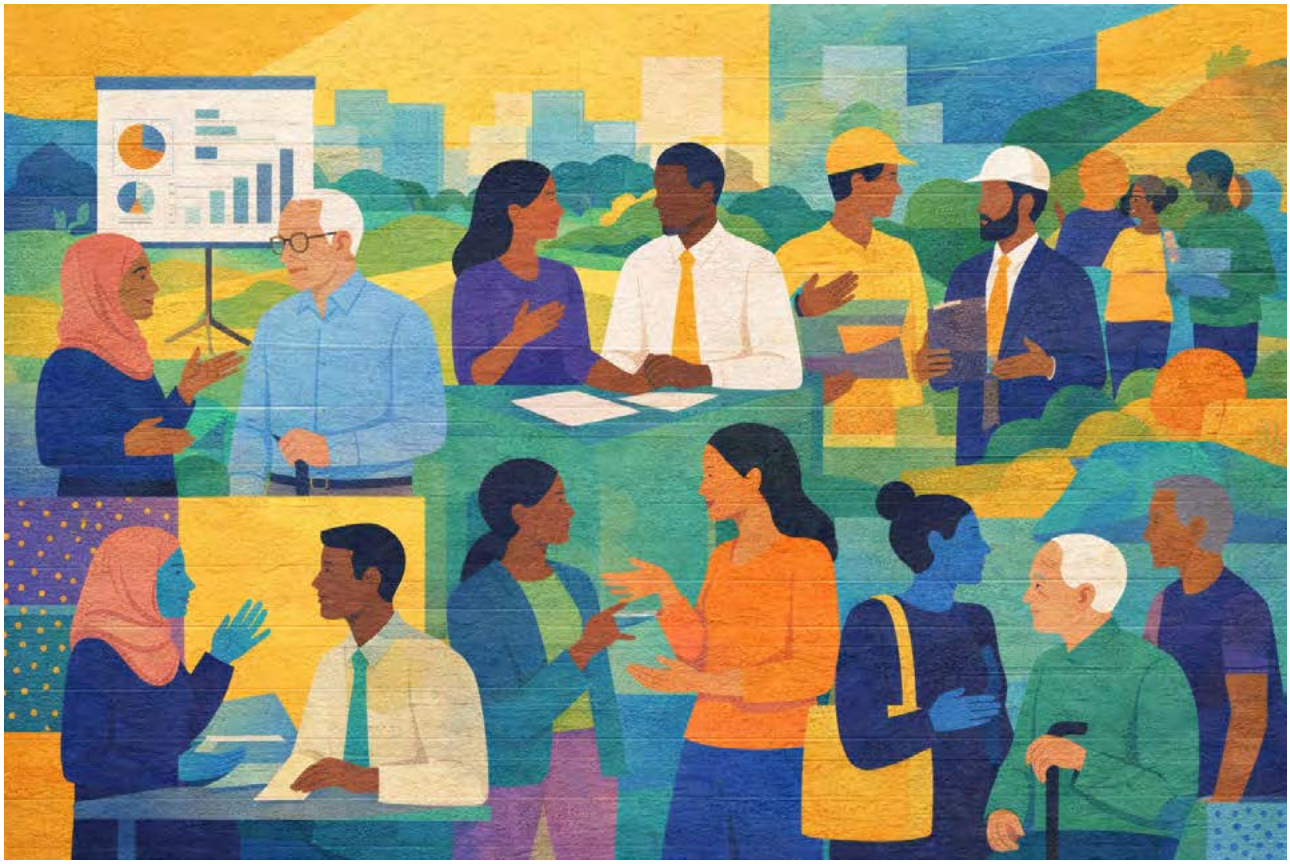


Figure 12 – A must: experts and community engagement

3. Approaches and strategies to avoid

Ineffective approaches to public engagement can worsen the delicate relationship between law enforcement agencies and the public, particularly when the reasons for deploying AI systems are unclear or incomprehensible. The following list is not exhaustive, and historical, political and cultural specificities can make other approaches problematic as well, but it offers a starting point.

1. **Lack of institutional capacity for meaningful engagement.** The challenges that the interviews revealed often reflect human factors, exacerbated by the limited capabilities and time that law enforcement personnel have to dedicate to public engagement. Agencies often lack trained professionals who know how to convene and guide meaningful public engagement. Accordingly, rather than being carefully coordinated and providing a consistent message, public engagement initiatives often appear as separate efforts in practice. Starting up public engagement activities without a coherent communication strategy is likely to lead to backlash and resistance, even to the best-intended and most potentially beneficial plans. This risk also increases when public consultations fail to influence how the agency performs its law enforcement duties. In this case, the law enforcement agency might regard the public consultations as a hurdle or add-on, such that it never gets prioritized or developed.

2. **Deprioritizing engagement when times are tough.** When budgets shrink, public engagement is often one of the first activities to be scaled back or postponed. Law enforcement agencies might regard it as a discretionary expense – one that requires staff time, facilitation expertise and logistical resources that all could be redirected towards seemingly more immediate, operational needs. Yet deprioritizing engagement in these moments can create a risky situation. Without sustained dialogue, law enforcement agencies risk making decisions based on internal assumptions rather than community priorities. The result is likely misaligned initiatives and diminished public trust, which in turn lead to higher long-term costs. Public engagement should always be pursued; it becomes particularly necessary and beneficial when finances are strained. Public concerns and perspectives can help law enforcement agencies strategically prioritize their efforts, allocate their limited resources where they will have the greatest impact and thereby save financial resources overall.

3. **Treating public engagement as information dissemination rather than dialogue.** As noted, gaining the trust of the public, and particularly vulnerable individuals and communities, takes time. Building meaningful public engagement thus demands patience, as well as actual dialogue and conversations with the public. An outward, one-directional lecture that presents the AI system as the only solution, without acknowledging or allowing for any alternative views, will not be effective. During honest, sincere conversations, law enforcement representatives must explicitly acknowledge people's concerns and frame the discussion around the problem that law enforcement agencies and the public both hope to solve, and whether it is worth deploying an AI system as a solution. Hosting a presentation that does not allow for responses or livestreaming a press release represents examples of ineffective approaches.

4. **Consulting the public after the fact.** Such tactics often coincide with a fourth ineffective practice, which arises if law enforcement agencies make the decision to implement a chosen AI system to solve a problem and then tell the public later. Such an approach is counterproductive and likely to antagonize the public. It makes it seem as if any requested feedback or consultation is symbolic rather than meaningful, a signal that vastly undermines trust and legitimacy. In contrast, the early and inclusive engagement recommended in SECTION 2.1 of this chapter would allow the law enforcement agency to identify and address key concerns well before the AI system implementation, by improving the quality and acceptability of the decision-making process.

5. **Engaging just a few or non-representative stakeholders.** Law enforcement agencies might enjoy hearing from supporters, and their contributions are relevant and important, too. But prioritizing such voices, without seeking diverse representation and broad engagement, is exclusionary by nature. As public service agencies, law enforcement agencies have a mandate to listen to all voices and serve the entire population, with policies that account for their diverse needs. Even relying too much on influential local leaders to repair or enhance the image of the local law enforcement agency can be counterproductive, because it undermines their status as trusted community members. Civil society and grassroots organizations representing disadvantaged groups might try to avoid engaging directly with law enforcement agencies to avoid allegations of selling out or betrayal of the communities they serve. Here again, it is the responsibility of law enforcement agencies to find ways to resolve such reasonable concerns, and encourage these organizations to engage with them, rather than writing them off as inaccessible.

Recommendations: Fostering effective public engagement

Trust is a two-way street. Simply conveying information to the public, without creating opportunities for them to share their feedback, is neither productive nor conducive to establishing and maintaining trust. Trust needs to be informed and earned through meaningful public engagement.

The section outlines practical recommendations regarding **what** meaningful engagement actually entails, **who** should be involved and **with whom** you should engage, and **how** you can achieve it. Some recommendations reflect general good practices; others offer inspiration for future approaches. Their applicability depends on the context, including the purpose of the AI system deployment, the risks it creates, existing levels of trust in law enforcement agencies and broader societal and institutional conditions.

What does meaningful engagement entail?

To be meaningful, effective public engagement should be grounded in a good-faith commitment to true consultations, such that it is substantive rather than performative in nature. Therefore, you should:

- **Genuinely listen.** Seek feedback on AI-related activities from all stakeholders and then apply it when appropriate. Trusting stakeholders is essential if you expect them to trust you.
- **Respond.** Even, or perhaps especially, if the feedback cannot be implemented in practice, clearly explain why. Which legal, technical or other constraints prevent you from addressing these concerns? Be sure to acknowledge, rather than minimize, the concerns that people raised.
- **Remain open to changing course.** When you receive well-grounded, relevant information, be brave enough to recognize that it requires a genuine change to your approach and practices or even the discontinuation of your use of an AI system.
- **Question your own perspective.** If you can assume a critical approach towards your work and systems, you are more likely to understand other perspectives. After you have done so, communicate your needs and potential challenges. Openness in this respect demonstrates accountability and willingness to co-create with stakeholders.

Contributions and feedback

Building on this commitment to meaningful engagement, it is equally important to create opportunities for contributions and feedback that are inclusive, actionable, and widely accessible. You should consider:

- **Using feedback constructively.** Granular, immediate feedback forms a strong basis for producing valuable data and insights.
- **Facilitating a grassroots approach.** Involve the entire community. Encourage contributions in any format convenient for individuals and communities with specific needs and customs.
- **Gathering inclusively.** Offer the public multiple ways to provide feedback, such as in writing or orally, or in analogue or digital forms, taking into consideration potential language or cultural barriers.
- **Asking for feedback widely.** Post requests for feedback where your audience is most likely to encounter them, such as on social media platforms, on TV and radio, in newspapers, and in physical locations such as bus stops or supermarkets.

Who should be involved?

Public engagement requires the commitment of the entire law enforcement agency, from leaders and law enforcement personnel to diverse internal actors, according to their expertise and availability. Your goals thus should be to:

- **Involve everyone.** Communication with the public cannot be limited to spokespeople and media teams if the goal is to prompt engagement.
- **Train personnel well.** Training for law enforcement personnel in the field is essential because they are the ones who engage most with the public in their day-to-day activities. But this training should be available to all members of the agency, to help them build their skilled dialogue methods and avoid allowing their biases to influence their interactions with the public.
- **Assign leadership.** Designating a person or team to lead the public engagement effort can help keep the agency on track. If you have the resources, a dedicated research and insight team can track national and local law enforcement developments and then redefine public engagement efforts to align with shifting strategic and community service priorities.

With whom should you engage?

Public engagement must be rooted in inclusivity, diversity and a multistakeholder approach. Therefore, you should:

- **Engage at every level of government,** national, state, regional and local. If an AI system is deployed to address a problem targeting a specific community at the local level, engage with that community first, to design potential solutions that match their perspectives and needs, and then integrate other levels.
- **Map external stakeholder groups.** You might identify external stakeholders who actively develop, sell or interact with the AI system (e.g., technology providers, external auditors). You can also identify those who are likely to be directly or indirectly affected by the AI system (e.g., interest groups, individuals, communities). A comprehensive stakeholder overview helps clarify whom to include in public engagement efforts.
- **Involve intermediaries.** Some groups cannot access law enforcement agencies easily, for a range of practical, social, cultural, linguistic or structural reasons. Ask trusted intermediaries or representatives to help you ensure that these communities are being heard and included in the process.
- **Consider mediators.** Mediators can mitigate disagreements with the public; you should have them in place to facilitate your interactions with deeply opposed groups.
- **Address distrust.** If you engage early on with the most opposed and distrustful groups, you might prevent distrust from spreading, as well as shift their views, at least to a neutral sentiment and at best to a positive one.
- **Engage widely.** Find and involve expert stakeholders who might have a stake in implementing the AI system and involve them as appropriate, ensuring diversity in representation.

- **Map external groups and experts.** Keep track of external groups and experts whom you might consult: innovation teams that support other law enforcement agencies, private-sector AI system developers, legal and ethics consultants who might conduct impact assessments, other civic and essential service agencies that also use AI systems (e.g., healthcare, city hall), civil society groups dedicated to community needs, and academics and independent researchers who study AI systems, to name a few.

Because of the particular need to include members of vulnerable populations, you should devote purposeful effort to the following targeted approaches:

- **Include underrepresented and excluded voices.** Consider frequently ignored groups, such as the elderly, children, minorities and people with disabilities. Children may need their parents or guardians to represent their interests.
- **Seek cultural insights.** Members of minority groups can offer advice about the sensitivity required to handle communication and engagement with specific communities, seeking a balance with what is legally and technically possible in specific circumstances.
- **Maintain open dialogue.** Listen to the public's opinions and concerns. Especially if they believe they have been treated unfairly in the past, regular conversations may be useful to prevent and address any type of tension.
- **Demonstrate your desire for feedback.** Establishing dedicated feedback mechanisms provides the public with a visible signal that you want their input and that you will offer them a secure, trusted space to share concerns.
- **Prevent discrimination.** Establish specific safeguards to monitor for and prohibit racial profiling, mass surveillance of minority groups and other AI system uses that reinforce systemic discrimination; then describe those efforts in detail to the public.

How should you engage with the public?

Law enforcement agencies can adopt several formats and modalities to support their efforts to engage openly and effectively with the public. You should adopt them according to existing conditions and relationships and consider:

- **Building from the bottom.** If you start with community-level engagement, you are more likely to develop a durable and responsible AI system, gain acceptance among the public and reduce the risk of profiling-driven biases.
- **Demonstrating relatability.** If you want people to open up and start trusting you, you have to show them that you relate to them in some way. Participate in their local networks, visit their religious or social centres, patronize local businesses and encourage the actions of civil society organizations.
- **Making leadership visible.** When high-level institutional representatives make their participation evident, it increases the credibility of the law enforcement agency and signals transparency, openness and accountability as genuine organizational priorities.

Some practical suggested approaches for fostering public engagement through diverse modalities are as follows:

- **Build small groups.** Engage a few experts or local governmental authorities, if applicable to the context, and then build small, diverse groups (e.g., 20 people) to start the initial dialogue.
- **Hold public information sessions.** Your goal in these sessions might be to educate the general public about AI systems, address fears or misconceptions and explain how law enforcement agencies' use of AI is designed to support, protect and benefit communities rather than harm them.
- **Engage informally**. Interact with the public in informal settings, such as over coffee or during local community meetings, to build rapport.
- **Create safe and neutral spaces for dialogue.** Engagement formats should enable participants to speak freely and candidly. While public sessions are often appropriate, in some cases off-the-record conversations, private meetings, closed-door discussions, or settings operating under Chatham House rules or non-disclosure agreements may be more suitable, particularly for sensitive topics where a more constructive and conciliatory exchange is needed.
- **Frame engagement as dialogue.** Describe public engagement as a scenario-based conversation that illustrates how AI systems can support the public and explains how law enforcement agencies intend to use these tools.
- **Offer hands-on exposure.** Groups can visit law enforcement agencies to receive demonstrations of how AI systems are being deployed for public safety, through simulations or practical examples. Ask law enforcement personnel to participate in such visits, to encourage meaningful engagement.
- **Hold regular community forums.** Bi-weekly or monthly community forums can bring together community members and relevant organizations. They require credible, visible and meaningful participation by your organization.
    - *Community forums* are structured, open meetings designed to share information, discuss issues and exchange feedback on topics of shared interests, such that they can promote transparency, encourage public engagement and build trust through regular dialogue.
- **Organize community engagement days.** Law enforcement personnel can plan to meet with individuals in their neighbourhoods, in relaxed, open settings. These casual gatherings help build familiarity, reduce apprehension and encourage positive word-of-mouth throughout the community.
- **Support peer-to-peer community networks.** Rely on community networks to get advice on culturally sensitive concerns, tailor interactions to specific communities and strengthen trust through respectful engagement. Examples are:
    - *Community Safety Partnerships (CSPs):* Statutory bodies, typically at the district or local authority level, in which various agencies collaborate to reduce crime and improve community safety. Local representatives of the public also join CSPs to

contribute to ensuring police engagement in the area.

- *Civilian Review Boards:* External bodies, established to review complaints of police misconduct and provide oversight of law enforcement activities.

- **Establish inquiry or statutory public safety bodies.** National and local public administrations can create dedicated bodies to address public safety concerns, including those raised by vulnerable groups, to safeguard their rights and ensure that policies and practices reflect community needs and priorities.

  - *Statutory bodies,* set up by legislation, perform specific, ongoing and likely permanent functions. Their purpose is to regulate, supervise or deliver public services.[139]
  - *Inquiry bodies* instead are set up to respond to major public concerns, establish facts, identify what went wrong and offer recommendations to prevent recurrence. They tend to be temporary and *ad hoc*.[140]

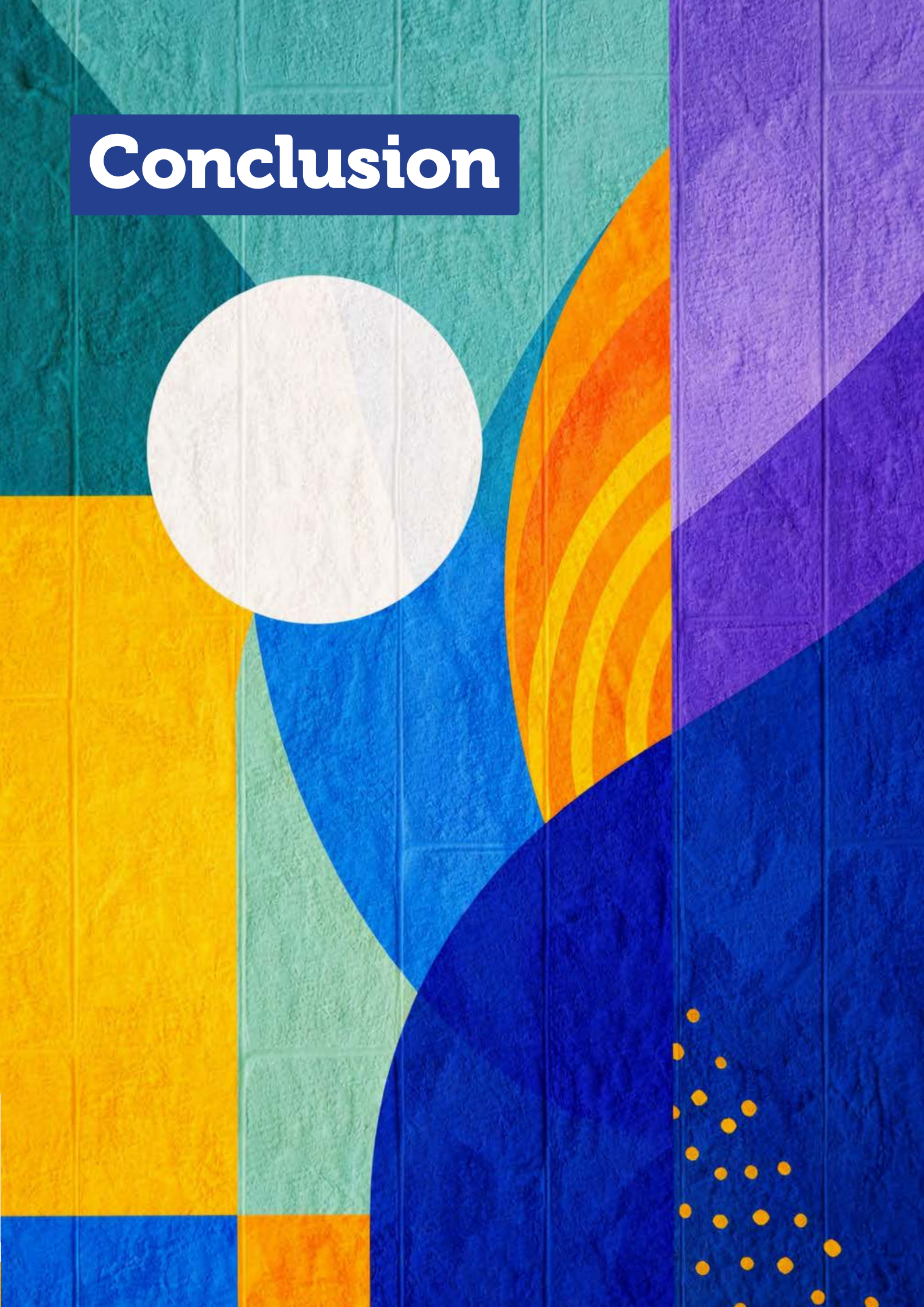
- **Engage online.** A presence in digital spaces is essential for enabling broad and inclusive dialogue. In particular, online engagement hubs can support ongoing dialogue and remote participation, by allowing people to join from wherever they feel psychologically safe and in accordance with their personal or professional needs. Effective online engagement hubs:

  - Ensure participants have what they need to contribute to their best ability, by breaking down barriers to inclusion (for instance, providing access to computers and mobile data to digitally excluded residents to help them take part in consultative processes).
  - Assign an experienced moderator to facilitate online conversations to ensure fruitful public engagement online.
  - Exploit the capabilities of digital technologies, such as allowing for anonymous feedback by people who feel unsafe providing their opinions in person or worry about being targeted.

139 Ian Thynne. (2006). Statutory bodies: How distinctive and in what ways? *Public Organization Review, 6*, (pp. 171–184). Accessible at: https://doi.org/10.1007/s11115-006-0011-2.

140 An example is the Nottingham Inquiry website, accessible at: https://nottingham.independent-inquiry.uk/frequently-asked-questions/.

Conclusion



The general public's attitudes towards the use of AI systems for law enforcement purposes tend to be cautious or negative, largely because of a lack of trust in law enforcement agencies, limited AI literacy and the influence of historical and cultural contexts. The public appears especially wary when it comes to the use of AI systems to make moral judgements and potentially replace law enforcement personnel in decision-making processes. A careful analysis of these elements indicates that law enforcement agencies should regard these concerns as foundational issues to address and resolve, before deploying any AI systems, while also building and maintaining the trust the public grants them.

For AI innovation, trust is fundamental to legitimacy; without it, the decision-making and operational effectiveness of AI systems become significantly undermined. However, building public trust in uses of AI by law enforcement agencies represents a complex, lengthy journey, and it must be rooted in transparency – defined in this report as openness by law enforcement agencies regarding their AI innovation efforts. To move beyond a one-directional information disclosure process, this report also frames transparency as a reciprocal, evolving interaction between law enforcement agencies and relevant stakeholders, including the general public, vulnerable populations, academia, civil society organizations and the private sector. Each actor is instrumental in promoting transparency through clear communication and effective engagement, which in turn emerge as key transparency practices.

To drive trust, transparency must reflect a continuous commitment to fairness, inclusivity and accountability. Transparency implies clear, meaningful communication of relevant information, through the life cycle of the AI systems, as well as effective engagement with the general public and various stakeholders to account for their diverse concerns, needs and perspectives throughout the AI innovation process. None of these efforts can be tick-box exercises. Missteps and failures in implementing AI systems, communication or public engagement efforts can provoke backlash, diminish public trust, trigger security threats concerns, engender societal tensions and result in financial losses.

In light of these considerations, this report provides law enforcement agencies with suggestions on how to adopt a structured approach to transparency, communication and public engagement in their AI innovation processes. These recommendations can guide law enforcement agencies and other actors concerned with public safety in navigating the multidisciplinary demands of responsible AI innovation, such as how to embed and communicate about transparency and how to engage effectively with the public and various stakeholders. No single methodology is definitive, and no process is infallible. AI systems, already deeply embedded in society and law enforcement, are no exception. The most appropriate response thus is to adopt a deliberate and proactive approach.

Annex

Methodology

The semi-structured interviews targeted multidisciplinary experts with backgrounds in the following areas:

- Criminology, policing and security
- Human rights and law
- Marketing, public relations and media
- Sociology, political science, ethics
- IT, science and technology

Figure 13 – Background of experts

The experts' affiliations accordingly represented several organizational categories:

- Law enforcement and public safety entities
- Academia
- Civil society
- Policymakers and government
- Business, consultancy, law firms

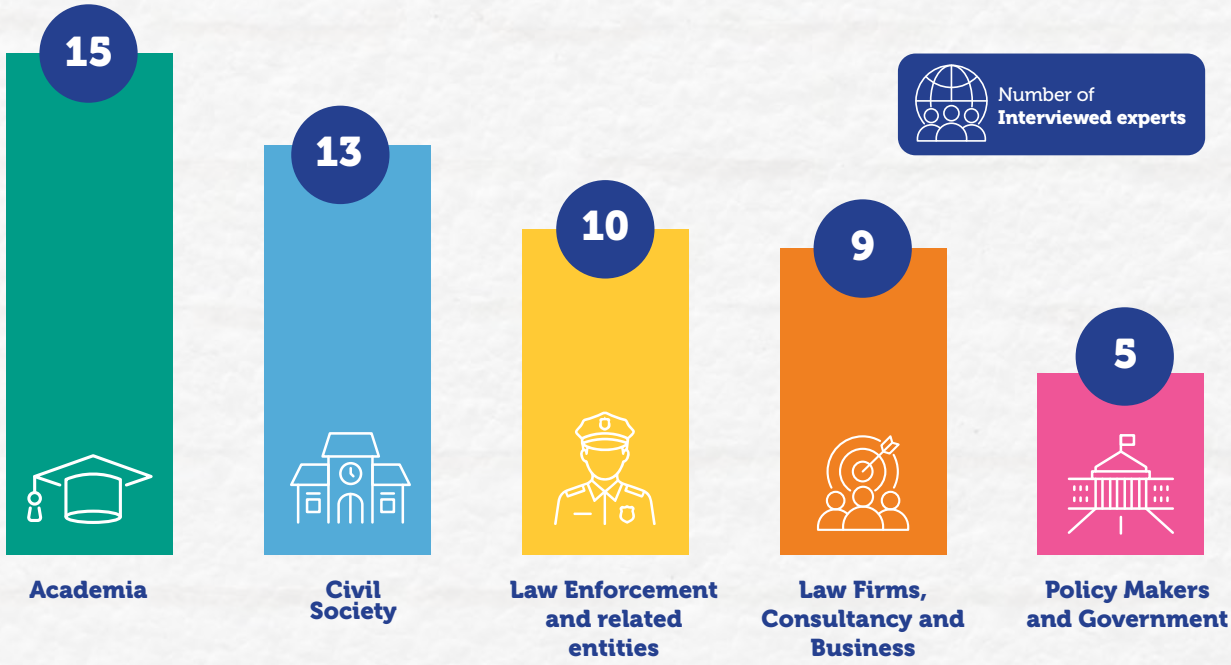


Figure 14 – Affiliation of experts

Many experts have multidisciplinary backgrounds. The attributions reflect their affiliation or occupation at the time of the interviews.

The interviewees represented all five geographic regions: Europe, Americas, Africa, Asia, and Australia and Oceania.

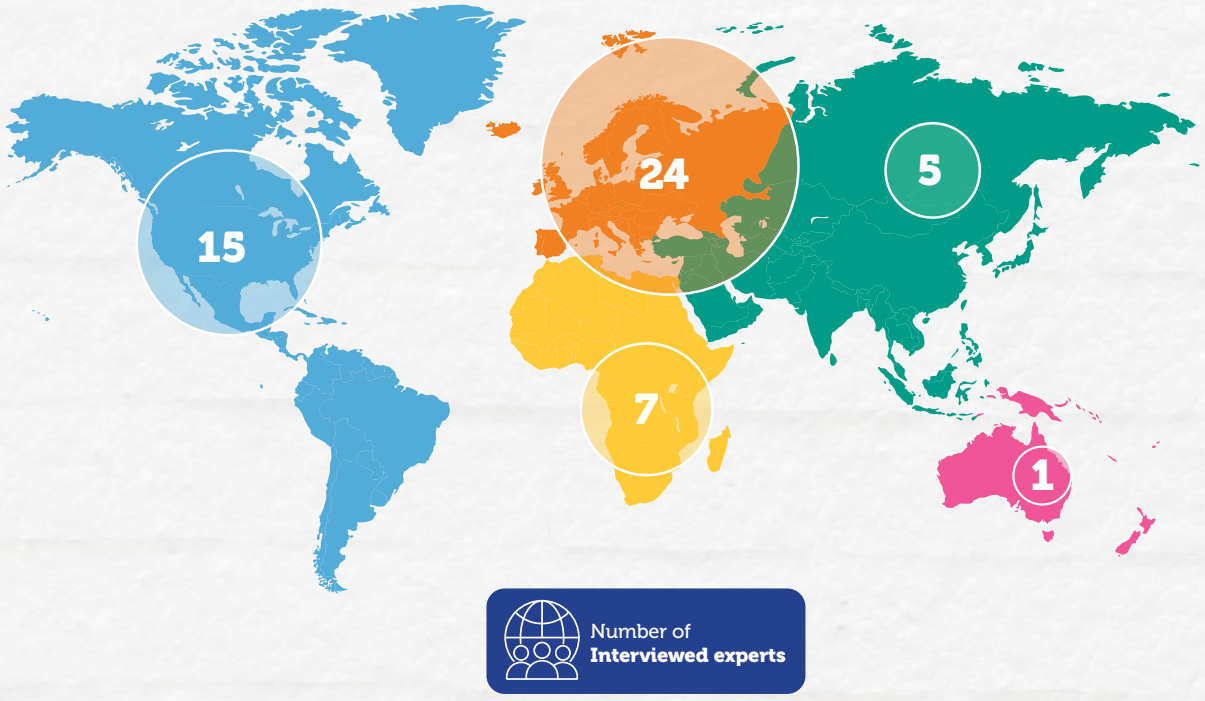


Figure 15 – Geographical representation

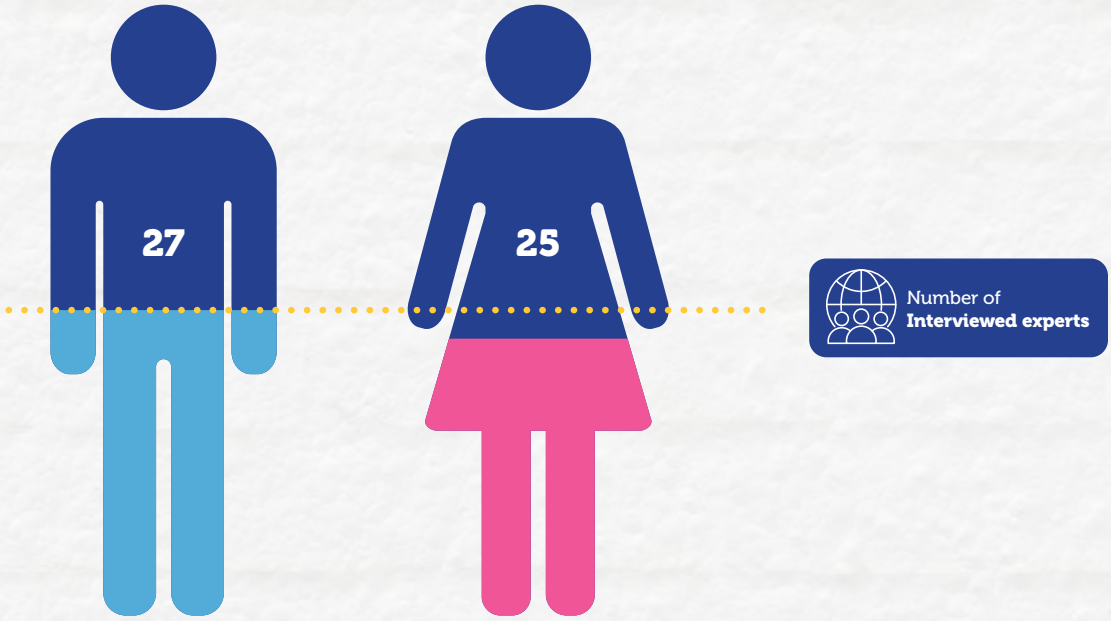


Figure 16 – Gender representation

Several sets of questions, developed for each area of expertise, encompass the experts' feedback on the use case scenario, based on their professional experience with AI systems, public safety and communication.

Law enforcement agencies and related entities:

- Your or your organization's experience with AI systems for crowd monitoring and anomaly detection.
- Your or your organization's experience with citizen engagement and public communication about AI systems.
- Your understanding of transparency and public trust.
- Opportunities and challenges in enhancing transparency in law enforcement use of AI.
- Specific considerations regarding the hypothetical use case scenario such as the type of information to be disclosed, communication channels, and entities responsible for the dissemination of information.

Experts in communications/marketing:

- Effective strategies to communicate to the public the deployment and use of responsible AI systems.
- Potential impacts on public trust from increased transparency by law enforcement in their use of AI.
- Suggested approaches, procedures and strategies to engage with citizens regarding the law enforcement use of AI systems.
- Specific approaches to engage with individuals and groups most vulnerable to discrimination/social inequalities.
- The role of external expert groups (practitioners, academics, civil society groups, and community leaders) in addressing societal concerns regarding the use of AI in law enforcement and fostering public trust.

Human rights/policy/ethics experts:

- Current practices in how (local) law enforcement communicates with the public and promotes transparency and their effectiveness.
- Key challenges and opportunities in fostering public trust regarding AI applications in law enforcement.
- The role of regulation, oversight and accountability mechanisms regarding transparency and trust in AI implementation in law enforcement.
- The role of external expert groups (academics, civil society organizations, and community leaders, etc.) in engaging the public and addressing concerns related to AI systems.
- Strategies for engaging individuals and communities most affected by discrimination or social inequalities in discussions about anonymized AI systems for crowd monitoring.
- Specific considerations regarding the AI system we are researching, such as the type of information to be disclosed, communication channels, and entities responsible for the dissemination of information.

Technical experts:

- Your or your organization's experience with AI systems for crowd monitoring and anomaly detection.
- What kind of built-in safeguards to make AI systems reliable and more appealing, which law enforcement agencies can also easily communicate.

- Any particular recommendations for law enforcement on communication with the public regarding the specific AI system from the hypothetical use case scenario.
- Your understanding of transparency and public trust.
- How to communicate/break down technical terms for a non-technical audience.

Cross-cutting questions about the hypothetical use case scenario:

- What kind of information should be disclosed to the public for this type of AI system, considering its implementation is aimed at increasing public safety and public trust?
- What kind of general explanation about the AI system should be disclosed?
- Where should the information about the use of AI systems be located?
- When/at which stages of the use of the AI system should the information be disclosed?
- Why should the information be disclosed and why not?
- How should the information be presented?
- What kinds of negative consequences for the work of law enforcement should be kept in mind/could be anticipated that can result from the disclosure of information on the use of anonymised AI system for crowd monitoring to public, or hinder law enforcement operations?
- Who should disclose and/or provide the information to the public?

Disclaimer

The opinions, findings, conclusions and recommendations expressed herein do not necessarily reflect the views of the United Nations Interregional Crime and Justice Research Institute (UNICRI), BI Norwegian Business School or contributory organizations, and do not imply any endorsement. The responsibility for opinions expressed in signed articles, websites, studies and other contributions rests solely with their authors, and publication does not constitute an endorsement by UNICRI of the views expressed in them. UNICRI does not endorse or recommend any use case, case study, product, process, or service. Any such references in this publication are provided solely for illustrative and analytical purposes and should not be interpreted as an endorsement or recommendation by UNICRI.

The designation employed and presentation of the material in this document do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations or UNICRI concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

Acknowledgements

This publication is a product of the initiative AI4Citizens: Legal, Ethical, and Societal Considerations of Implementing AI Systems for Privacy-Preserving Crowd Monitoring to Improve Public Safety by UNICRI and BI Norwegian Business School, with the generous support of the Research Council of Norway. It was written by Inês Gonçalves Ferreira (UNICRI), Ottavia Galuzzi (UNICRI), Volha Pashkevich (UNICRI) and Matilda Dorotic (BI Norwegian Business School), with notable contributions by Maria Eira (UNICRI), Michael O'Connell (UNICRI), Emma Kristina Persson (UNICRI), Bente Skattør (Oslo District Police), Emanuela Stagno (University of Sussex) and Mulugeta Weldezgina Asres (University of Agder). Design was by Marianna Fassio (UNICRI) and editing by Elisabeth Nevins (Editor and Director, Effectual Editorial Services). Hamed Arjmand assisted with qualitative data coding.

UNICRI wishes to extend its sincere gratitude to all individuals and entities who generously contributed to this report by participating in interviews, sharing expert insights and sources, and providing peer review. The following contributors have kindly consented to be acknowledged:

Alexandru Lazar (CyberPeace Institute), Atul Rai (Staqu Technologies), Ayca Ariyoruk (Center for AI and Digital Policy), Ayodele Sogunro (Osgoode Hall Law School, York University), Dr. Bas Testerink (National Police Lab AI, Netherlands National Police), BIGDATPOL team (Ghent University), Dr. Christopher Lee Bush (Allen County Community College), Captain (R) Cyril Piotrowicz (French Gendarmerie), Cynthia Picolo (Laboratory of Public Policy and Internet – LAPIN), Dasha Borysov, Deshni Govender (FAIR Forward – AI for All, GIZ), Doreen Nkatha Muthaura (Distinguished Legal Professional, Law Reformer, Legislative Drafter and Governance Expert in Kenya), Dr. Whitney Phillips (University of Oregon), Evaldas Visockas (Police Department under the Ministry of Interior of Lithuania), Even Hallås (HH Kommunikasjon), Fabien Leimgruber (CyberPeace Institute), Felipe Rocha da Silva (Laboratory of Public Policy and Internet – LAPIN), Franco Giandana (Access Now), Frederic Baervoets (NIDO Innovation Lab), Graham Drake (Tony Blair Institute for Global Change), Irene Poetranto (The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto), Isabela Maria Rosal (Centre for IT & IP Law, KU Leuven), Jake Okechukwu Effoduh (Lincoln Alexander School of Law, Toronto Metropolitan University), Dr. Jennifer Matthews (Dr. Jennifer Matthews Consulting), Jingjie He, Dr. Joshua Hughes (Trilateral Research), Kaylyn Jackson Schiff (Purdue University), Kevin Ditcham (Police Scotland), Kris D'Hoore (Federal Police, Belgium), Laureline Lemoine (AWO), Lloyd McKeag (Northern Ireland Police), Marjolijn Bruggeling (Policing Lab), Morana Fuduric (University of Zagreb), Nazareen Ebrahim (Naz Consulting International), Osman Mohammad Ibrahim (Agency for Emergency Planning, Oslo Kommune), Patricia Gestoso-Souto (Gestoso Consulting), Paula Lopes (OLIVER), Pedro Diogo Carvalho Monteiro (Laboratory of Public Policy and Internet – LAPIN), Dr. Pete Fussey (University of Southampton), Rafael Zanatta (Data Privacy Brasil Research Association), Richard Stirling (Oxford Insights), Dr. Rita Matulionyte (Macquarie Law School, Macquarie University), Severina Kelley (Northern Ireland Police), Sonya Merkova (Adviser to UN Special Rapporteur on the Rights to Freedom of Assembly and Association), Stefano Puntoni (The Wharton School, University of Pennsylvania).


www.unicri.org