
unicri
United Nations Interregional Crime and Justice Research Institute
CENTRE FOR ARTIFICIAL INTELLIGENCE AND ROBOTICS
BI
Norwegian Business School
The Research Council of Norway
Transparency in action
Recommendations to foster public trust in responsible AI innovation in law enforcement

Public trust is the bedrock for legitimate, effective law enforcement – 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 people 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.

These recommendations aim to guide 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. 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. Therefore, these recommendations focus on two practical and interconnected dimensions: **communication** – providing clear, accessible information to the public, and **public engagement** – creating meaningful, two-way dialogue with the communities they serve. Together, these practices form the bridge between transparency and public trust; but only if the organization builds a transparency-first mindset.

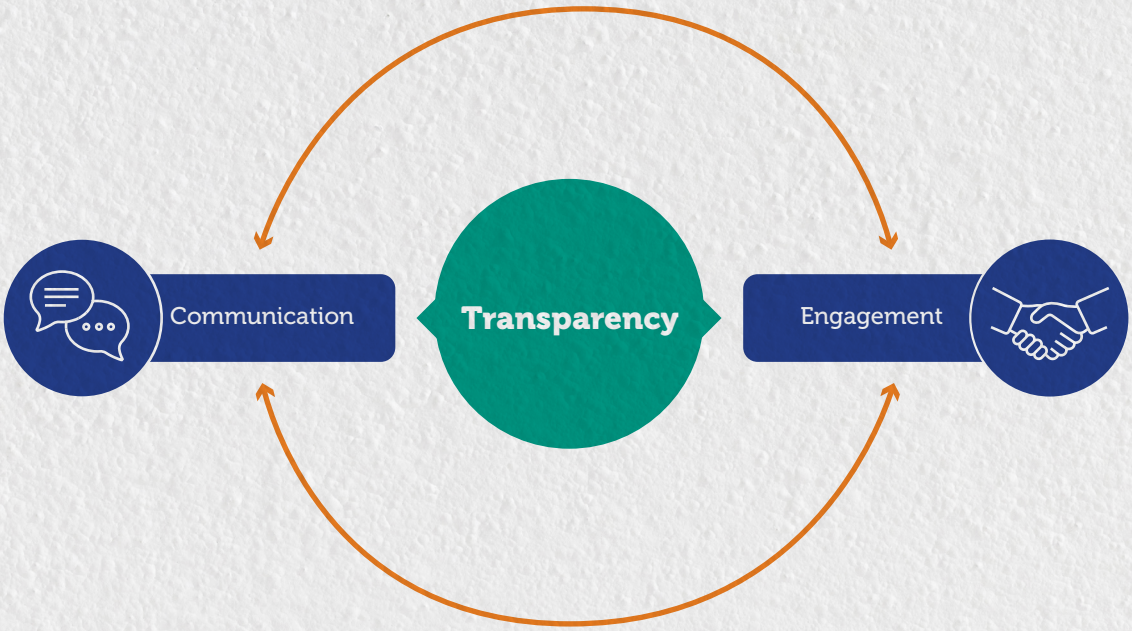

Figure 1 – Transparency as a two-way process

01 Cultivating a transparency-first mindset

Transparency 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. Law enforcement agencies using AI for public safety 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.

Figure 2 – Recommendations to build and maintain a transparency first-mindset

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 freedom of information (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.

02 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 3 – Recommendations for public communication

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 pur-

poses, 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.

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.[1]
- **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.
- **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 simple visuals, audio, translations and easy-to-read layouts.

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

- **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 4 – 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.

03 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.

Figure 5 – Recommendations for public engagement

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.[2]
  - *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.[3]

- **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.

2 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

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

Acknowledgements

This publication is derived from the report "Decoding Transparency: How to Foster Public Trust in Responsible AI Innovation in Law Enforcement", 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.

About

The "Decoding Transparency" report is a product of the AI4Citizens: Legal, Ethical, and Societal Considerations of Implementing AI Systems for Privacy-Preserving Crowd Monitoring to Improve Public Safety initiative by the UNICRI and BI Norwegian Business School, with the generous support of the Research Council of Norway. This publication compiles the actionable components of such report, focusing on its practical recommendations and is intended to facilitate dissemination and use. For the full analysis, methodology, and findings, please refer to the complete report.