POLICING PROJECT
NYU SCHOOL OF LAW

NYU School of Law
40 Washington Square South
New York, NY 10012

E: info@policingproject.org
W: policingproject.org

Frequently Asked Questions about Disclosures of Police Use of AI in Criminal Investigations

The Policing Project's model statute "Police Use of AI - Inventory and Disclosure" requires law enforcement agencies to disclose information about AI tools authorized for use in criminal investigations to the public (via an AI Inventory) and those used in specific cases to prosecutors and defendants. This FAQ addresses questions relating to why these disclosures are essential and how these policies work.

1. What do we mean when we talk about AI in criminal investigations?

Broadly speaking, police use AI in criminal investigations to help generate leads, gather evidence, and draft reports. Early in an investigation this might mean using facial recognition technology to help identify a suspect or a vehicle surveillance system to provide images and locations of a suspicious vehicle. Later on, officers might turn to a publicly available tool like ChatGPT or a program designed for police use such as Axon's Draft One to help write police reports for the investigation. A broad overview of police AI use is provided in our explainer "How Policing Agencies Use AI."

2. Are there any problems with police use of AI in criminal investigations?

Unfortunately, yes. AI is still a very new and developing field, and AI tools may be unreliable or error prone. For example, there are already real-world instances of vehicle surveillance systems misreading license plates, leading officers to pursue and detain the wrong person. Similarly, generative AI has a well-known "hallucination" problem in which it confidently asserts things with no basis in fact—a problem with potentially devastating consequences in an official police report.

In addition, even AI that works in theory can fail in real world applications, errors that officers may be more likely to overlook due to our natural bias toward trusting advanced technology like AI. Likewise, AI tools may implicate someone for a crime without ever fully explaining why or how they reached this conclusion, a black box of decision-making that undermines our Due Process rights. There also are serious privacy concerns and constitutional issues that come with systems that are massively more powerful than traditional police methods and that lack practical human limits—such as the need to sleep or the ability to only be in one place at a time—that guard against unnecessary police actions.

3. How do we know which AI tools an agency uses in criminal investigations?

Frequently, we don't know. There are few state laws requiring transparency for police use of AI, and many law enforcement agencies don't have publicly-available policies on their use of AI. This lack of transparency makes it much more difficult to ensure that police are using AI reliably, fairly, and in line with community priorities. Instead, law enforcement agencies grapple with difficult questions over if, how, and when to use various AI products, without the benefit of public input or oversight by policymakers.

4. Do police disclose AI use in individual criminal cases?

Often they don't. Laws or policies requiring officers to inform criminal defendants about their use of AI are rare. In most cases, the sole obligation to disclose AI use comes from constitutional guarantees that the government provide criminal defendants with information that it intends to use at trial or that suggests the defendant might be innocent. However, officers may believe that these requirements do not cover their use of AI, such as when they only use it for lead generation or report drafting. In these instances, it's entirely possible that neither the prosecutor nor the defendant ever find out that an AI tool was used in a case.

5. Why is it a problem for the police not to tell prosecutors or defendants that they're using AI?

The failure to disclose AI use in a given case means that the accuracy and legality of that use will remain unchallenged. This can undermine a person's right to a fair trial, possibly resulting in a wrongful conviction (which may also mean the actual perpetrator of a crime remains free). Further, without the ability to review the use of AI in court, unreliable tools or inappropriate uses of AI could slip under the radar and continue to undermine public safety over a longer period of time. Fortunately, prosecutorial oversight and the adversarial criminal justice system serve as quality controls to find exactly these sorts of issues — a goal that can only be achieved through transparency.

6. What information should be disclosed?

Law enforcement agencies should publicly release, and regularly update, an "AI Inventory" that provides basic information about each AI system used in connection with criminal investigations. This should include details such as the name of the AI system, a brief description of its capabilities and limitations, the types of data it uses and produces, and all authorized and unauthorized uses.

In criminal cases, an initial disclosure should be enough for prosecutors or defense attorneys to determine whether they need more information to adequately assess if an agency's AI use was lawful and error-free. This will look a bit different depending on the specific tool. For facial recognition, for example, this might mean indicating that the system helped identify a suspect, whereas for an AI-assisted police report, the disclosure should indicate which portions of the report AI helped draft. Then, if prosecutors or the defense need more information, such as internal evaluations on the AI's accuracy or officer training on the AI, they can request it, with courts resolving any further issues during discovery.

7. Will these disclosures burden police?

No. By requiring only the release of basic information, such as the type of AI used and its general purpose, at the outset of each criminal case, the initial burden on officers is minimal. These disclosure obligations could even potentially be fulfilled by checking boxes on a form or indicating information through a drop-down menu, something that officers already regularly do for other information. Requests for additional, more detailed information can be subjected to standard criminal discovery processes. This will help ensure requests are tailored to the case at hand and no more burdensome than the other discovery motions routinely handled in criminal cases.

8. Will disclosures interfere with police operations?

No. Disclosure rules only require transparency. Law enforcement will continue to decide which AI tools to use and how, and discovery rules can take into account the need to protect sensitive operations. Further, in the long run, discovery and motion practice examining the use of AI will help identify inaccuracies and other problems, which can improve police operations. Communities also should consider rules on how police use AI, but that is a distinct issue from basic AI disclosure.

9. How can we ensure appropriate disclosures are made?

The most effective solution is state law. Although law enforcement agencies and prosecutor offices can and should adopt internal policies requiring adequate disclosures relating to police use of AI, these policies lack the power of law and are subject to change without any public input or even notice. In addition, state law standardizes practices across local jurisdictions, ensuring a uniform set of rights and processes for criminal defendants throughout the state.