Policing Project
NYU School of Law

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

info@policingproject.org
@policingproject
212.992.6950

RESPONSIBLE USE OF POLICING TECH: EVALUATIVE FRAMEWORK

New technologies promise to make policing safer and more effective. But there is widespread concern about these technologies, including invasions of privacy, inaccuracy, and perpetuation of racial bias. Too often, adoption of new policing technology is debated as a matter of being "for" or "against" it. We believe the better approach is to figure out if society can benefit from a particular technology. Then, if there are benefits to be had, the question becomes whether it is possible to minimize or eliminate any harm. (Some harms, like constitutional violations, are impermissible in any degree.) We also believe it is essential that any decision to use technology has democratic legitimacy.

We evaluate policing technologies using this framework:

Potential Benefits. Any analysis necessarily begins by asking about the assumed benefits of the technology. Particularly when use of a technology has attendant social (and hard) costs, it is important to identify the specific problem the technology is designed to address or solve, or social improvement it is intended to bring. We do so in the following stages:

1. **Specify the Problem & the Benefit:**
   - What is the specific problem(s) the tech is intended to solve?[1]
   - How important/what is the magnitude of the problem the tech expect to solve?

2. **Evaluate Certainty of the Benefit:**
   - How certain is it that the technology will address the problem?
   - Have there been evaluations (either internal or external)?
   - Are there product performance concerns that might limit effectiveness?
   - If the tech succeeds in addressing the problem, will benefits be evenly distributed, or do they favor one segment of society over another?
   - What countermeasures might individuals take in response to the adoption of this tool, and how much would such countermeasures reduce the expected benefits?

3. **Evaluate Unintended or Secondary Benefits:**
   - Minimize criminalization of low-level offenses?
   - Additional control and protection of personal data?
   - Mitigation of racial and/or identity bias?
   - Improved transparency or public trust?
   - Better compliance with U.S. constitutional requirements?
   - Other societal benefits?

[1] "Problem," here, might be a law enforcement problem (e.g., improving law enforcement methods), it might be a social problem, or it might be a problem relating to the internal operations of a police department. It is important, when framing the problem as a "law enforcement" problem, to be able to articulate the public safety goal that would be addressed through the use of technology, rather than considering "law enforcement needs" as an end in itself.

Potential Costs. Only if a technology has identifiable, concrete benefits should one turn to considering potential costs, including attendant social costs.[2] To facilitate this technology-specific evaluation, we evaluate a number of criteria that often arise in the case of new policing technologies.

4. **Transparency.**
   - **With the Public –** Do members of the public know about and/or consent to this information capture? Does the company itself make the public aware of where and how its product operates? How does the company's public description of its capabilities compare to actual capabilities? How does the company's public description of benefits compare with to actual benefits? How open is the company in dealing with the public and media?

   a. **Public Clients of Technology Companies –** How and to what extent are customers prevented, permitted, encouraged, or required to inform or engage with the public about the customer's decision to acquire or use the technology? To share information about the nature of the product or data it generates?

5. **Personal Information Privacy.**
   - **Data capture –** What information can or does the tech capture, measure, collect, or use? Is all of this data relevant and necessary to accomplish the purpose of the technology? From whom is this data collected?
   - **Data aggregation and mining –** Does the tech aggregate data and if so, how? Is the data stored in an anonymized fashion? Does the system analyze data to identify previously unknown facts or patterns (aka data mining)?
   - **Data retention –** Is data retained by the company or the customer? What are the guidelines/limits for doing so? How long is data retained? Can individuals request access to or deletion of their personal data?
   - **Data ownership and sharing –** Who owns the data collected? Who has access to that data? Does the company use any third-party data processors and for what purpose? Can customers share data with a third party? Does the company or the customer sell or otherwise monetize data?
   - **Data control and security –** How/where is data stored? Is personally identifiable information separately stored and or encrypted? What are the physical, technical, and administrative protocols for data storage and access? Are there built-in audit trails to determine what type of data is collected and/or accessed by an end user? What are the protocols in place for a data breach? Will those whose data is acquired by notified? Is there risk of physical harm to individuals or locales in the event of a security breach?
   - **Compliance** – How does the vendor monitor compliance with data policies?

[2] Any true benefit-cost analysis must take into account hard costs, including but not limited to long-term retention and data storage costs. Although these types of costs are an important consideration both to police departments and their communities, we focus here on ethical considerations, not financial ones.

6. **Racial or Other Identity Disparities.**
   - Disparities in design (*e.g.*, whether the technology itself has any inherent bias, including algorithmic bias relating to personal identity, for example, by employing unrepresentative training data or exhibiting algorithmic bias)?
   - Disparities in operation (*e.g.*, whether the technology might be deployed or used in ways that create or exacerbate identity bias and/or disparities)?

7. **Increased Criminalization.** Will use of the tech lead to more people being stopped, ticketed, arrested, or incarcerated? If so, for what type of crimes? Is enforcement of these crimes a net contribution to society or a net harm (*i.e.* are you contributing to low-level criminalization)?

8. **Evidentiary Risk.** Does the tech produce evidence to be used at trial? Under what circumstances? Does it meet chain-of-evidence, *Daubert*, and other rules of evidence? Are their protocols in place to ensure all necessary information is turned over to prosecutors and the defense?

9. **Constitutional Risks.** To the extent not already discussed, does use of the technology risk directly or indirectly violating constitutional rights, including but not limited to:
   - 1st Amendment (speech, press, religion, assembly, association, petition)
   - 2nd Amendment (right to bear arms)
   - 4th Amendment (searches, seizures, excessive force)
   - 5th Amendment (self-incrimination, *Brady* & impeachment evidence, due process)
   - 6th Amendment (right to counsel, speedy/public trial, cross-examine witnesses)
   - 8th Amendment (cruel & unusual punishment, excessive bail, excessive fines/fees)
   - 14th Amendment (equal protection)

10. **Other Potential Social Costs.** Are there other potential social costs that have not yet been considered, including but not limited to:
    - Whether there might be a unique impact on any specific subgroup (*e.g.*, youth, LGBTQ communities, particular religious groups, socioeconomically disadvantaged communities)?
    - Whether there are historic considerations that may make particular communities distrustful of this technology?
    - The potential for mission creep (either over time or in response to critical events)?
    - The impact of how others in the industry will respond?
    - Global/international human rights impact?

11. **Less costly technologies?** Once the social and other costs are identified, unless it is all benefit and no cost, there is one important last question: Are there alternative means of addressing the problem or providing the social benefit that are less costly, less-invasive, or avoid the costs identified here?

Operational Concerns. In additional to considering potential costs and benefits, there are several categories of operational concerns that one must always keep in mind thinking through the potential impact of new policing technologies:

12. **Tactical Impact -** How will the product impact the performance of police officers? Will these changes create additional risks for officer or for the public?

13. **Integration Risks.** Can the tech freely integrate with other tech, and how might such integrations impact the risks discussed above? Can it be augmented with outside software (e.g., adding face recognition to CCTV or body-worn camera)

14. **Intended use vs. Actual use.** Can the product be used differently than originally intended? Does this different downstream use present additional risks to consider? What are the vendor's terms-of-use and do they adequately limit how the tech can be used? Other than terms of use, what policies, procedures, or design features exist to limit, monitor, or audit downstream use or misuse?

15. **Internal Policies & Procedures.** Has the agency implemented a use policy? What internal policies and protocols are in place to ensure the product is used in the manner described above?

16. **Training.** What type of training do analysts, officers, and supervisors receive? Does the vendor provide on-going training and/or support?