PLANK 9:
End high-tech harm and the surveillance state.

Technology can be a force for good and has the power to improve people's lives, yet it continues to play an increasingly pervasive and insidious role in the criminal-legal system. Facial recognition, predictive policing technologies, and algorithm-based decision-making tools can pose threats to Black, Brown, Indigenous, low-income, disabled, and other marginalized communities. The use of these data-driven technologies, many of which rely on racially biased arrest data, can reproduce, exacerbate, and entrench the existing disparities within the criminal-legal system. These technologies are promoted as being "evidence-based" and "objective" when, in reality, they reflect a wide range of underlying flaws and biases. Moreover, these tools are designed, developed, and tested under a shroud of secrecy — often passed off as "trade secrets" — that expand the reach of the criminal-legal system and hamstring impacted individuals when they seek to challenge the basis for restricting their freedom.

The use of these data-driven technologies reproduce, exacerbate, and entrench the existing disparities within the criminal-legal system.

Statements by civil and human rights advocacy organizations have consistently explained how facial recognition, algorithmic risk assessment tools, and predictive policing technologies disproportionately harm communities of color. These statements highlight the lack of transparency, accuracy, fairness, and accountability endemic to these technologies, while underscoring the deep inequities and biases that can occur when technologies are designed and used without the input of the communities that are the most impacted by them.

We must advocate against technology that is used to further a criminalization- and surveillance-focused approach in communities in the United States. Technology must help lift people up, connect them to community-based programs, and give them access to the basic necessities they need to survive and thrive.

WE MUST ENSURE A SYSTEM IN WHICH TECHNOLOGY IS USED TO HELP LIFT PEOPLE UP, CONNECT THEM TO COMMUNITY-BASED PROGRAMS, AND GIVE THEM ACCESS TO THE BASIC NECESSITIES THEY NEED TO SURVIVE AND THRIVE.

State and Local Policy Priorities

Ban systems, software, and platforms that entrench civil rights abuses

- State and local law enforcement jurisdictions must place a moratorium on or outright ban a number of systems, software, and platforms that further entrench civil rights and civil liberties inequities in the criminal-legal system, especially for marginalized communities. Technologies that are based on data from the criminal-legal system are inherently biased and discriminatory; while this list is not exhaustive, here are examples of technologies within the criminal-legal system that should be banned or at the very least have a longstanding moratorium placed on them:
    - Algorithmic or artificial intelligence software or decision-making policing systems — including person-based and place-based systems — that predict, forecast, or anticipate areas designated as “high crime” or for further policing;
    - Facial recognition technologies and all “at distance” recognition surveillance, including emergent technologies such as gait recognition and heartbeat detection;
    - International Mobile Subscriber Identity (IMSI) catchers;
    - Microchip implants;
    - Aerial or drone surveillance of neighborhoods or areas deemed to be “high crime” or for other carceral purposes; and
    - Any other surveillance tools or strategies, including (but not limited to) tools or strategies weaponized against people exercising First Amendment rights through protest.
- Jurisdictions should act expeditiously to phase out the use of the aforementioned tools and ensure that any use is disclosed to the accused’s counsel in a criminal trial.
- Ban the use of the following surveillance tools as a condition of pre- or post-adjudication community supervision:
    - Geo-location monitors, including smartphone applications;
    - Devices that have a microphone, speaker, or other tools that have speech or voice recognition technology;
    - Devices that gather biometric data; and
    - Any other electronic monitoring (including apps on smartphones) software or platforms used to track location.

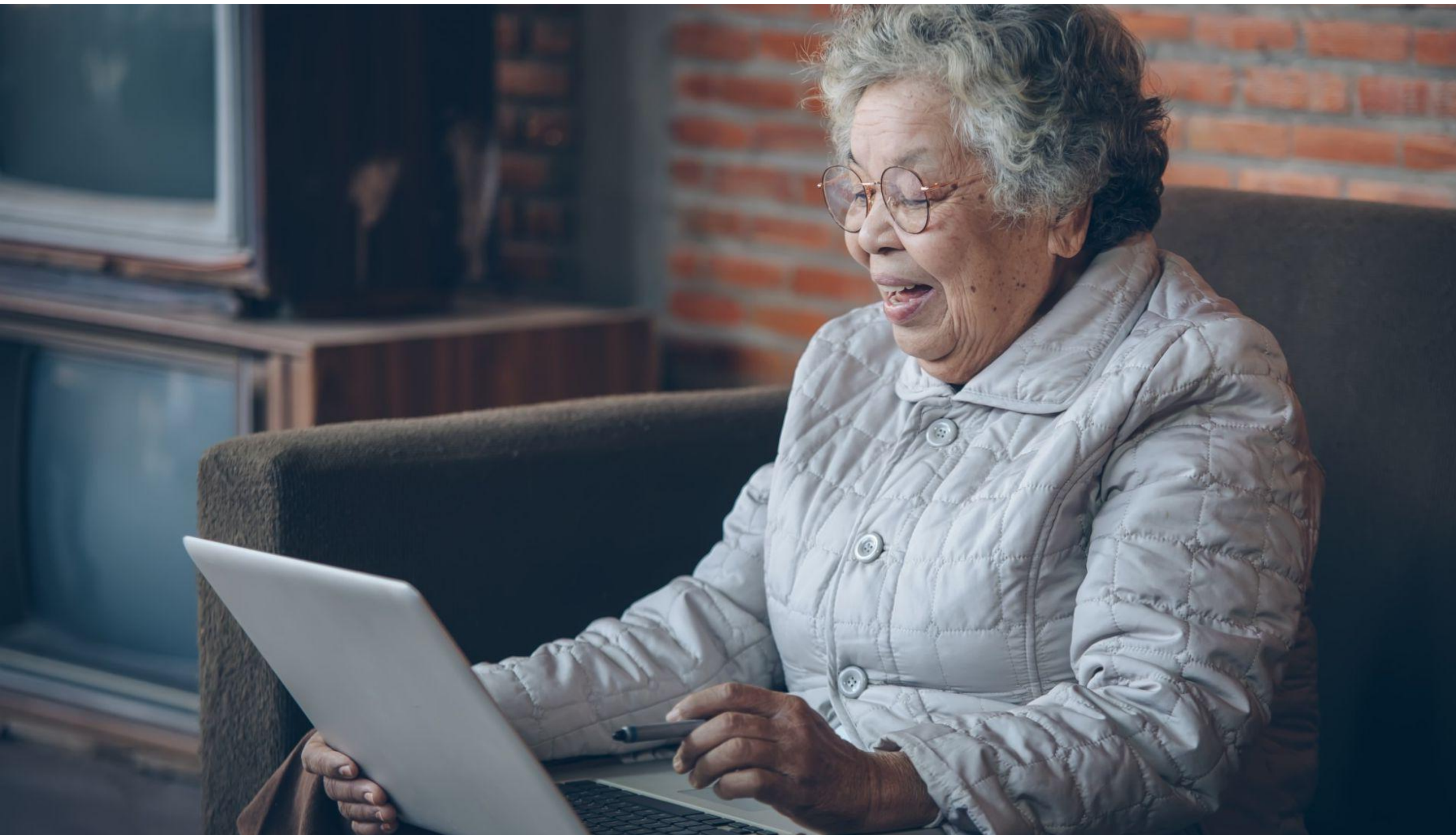
Enhance transparency and accountability

- Any tool that implicates suspects should not be protected by trade secrets when challenged in an adversarial judicial proceeding. In such a proceeding, the software or platform creator should at minimum allow the accused access to: the data that the algorithm, software, or AI is trained on, or the weight of specific data points in the algorithmic system; and whether the system has been tested for disparate impact on marginalized communities.

Federal Policy Priorities

Ban systems, software, and platforms that entrench civil rights abuses

- The federal government must place a moratorium on or outright ban a number of systems, software, and platforms that further entrench civil rights and civil liberties inequities in the criminal-legal system, especially for marginalized communities. Technologies that are based on data from the criminal-legal system are inherently biased and discriminatory; while this list is not exhaustive, here are examples of technologies within the criminal-legal system that should be banned or *at the very least* have a longstanding moratorium placed on them:
    - Algorithmic or artificial intelligence software or decision-making policing systems — including person-based and place-based systems — that predict, forecast, or anticipate areas designated as “high crime” or for further policing;
    - Facial recognition technologies and all “at distance” recognition surveillance, including emergent technologies such as gait recognition and heartbeat detection;
    - International Mobile Subscriber Identity (IMSI) catchers;
    - Any tool or system that collects biometric data that has not been tested by a third party for accuracy, and if tested, the likelihood of false positives, the likelihood of accuracy of that sample, and the accuracy of the biometric data when retested;
    - Microchip implants;



    - Aerial or drone surveillance of neighborhoods or areas deemed to be “high crime” or for other carceral purposes; and
    - Any other surveillance tools or strategies, including (but not limited to) tools or strategies weaponized against people exercising First Amendment rights through protest.
- Jurisdictions should act expeditiously to phase out the use of these tools and ensure that any use is disclosed to the accused’s counsel in a criminal trial.
- The federal government should also be prohibited from expending any funds that go to procuring, deploying, developing, or otherwise using and/or facilitating the state or local use of surveillance technologies and systems. There must also be a review of federal dollars used to aid state and local procurement of surveillance tools, and in particular the role of the FBI in assisting local police departments with digital evidence capacity. Examples of these surveillance technologies include:
    - Predictive policing and predictive policing software;
    - Facial recognition technologies and all “at distance” recognition surveillance, including emergent technologies such as gait recognition and heartbeat detection;
    - International Mobile Subscriber Identity (IMSI) catchers;
    - Any tool that requires access to a source code;
    - Any tool used to collect biometric data;
    - Drones and other aerial surveillance technologies; or
- Severely limit the power of the federal government to use, as part of probation, parole, orders of immigration supervision, or any other community corrections, any tools used to track location. Ensure that the costs of these services are never imposed on the individuals under supervision.

Enhance transparency and accountability

- Any tool that implicates suspects should not be protected by trade secrets when challenged in an adversarial judicial proceeding. In such a proceeding, the software or platform creator should at minimum allow the accused access to: the data that the algorithm, software, or AI is trained on, or the weight of specific data points in the algorithmic system; and whether the system has been tested for disparate impact on marginalized communities.
- Conduct oversight of government surveillance programs. Address government surveillance programs and investigative systems that unjustly securitize or criminalize racial, ethnic, and religious minority communities, including watch listing, predictive policing, gang databases, and the implementation of the National Vetting Enterprise.