MEMORANDUM

To: Katerina Canyon, Purushottam Bhandere
From: Rashell Khan
Date: 18 December 2025
Subject: Surveillance and Domestic Militarization

Just as the drug war fuelled increased military participation and militarization in domestic policing, the war on terrorism has driven the militarization of domestic intelligence operations.[1] Unlike the purchases of physical equipment, domestic intelligence activities take place mostly in the dark. Neither the public nor policymakers really know what is happening. Military intelligence officials are trained for war against hostile enemies. Their tools, tactics, and attitudes reflect that mission, and are completely inappropriate to a domestic application. Domestic intelligence programs have become militarized in three ways:

1. Data Collection: Military agencies are conducting domestic intelligence collection against Americans, and providing that information to law enforcement officials. The National Security Agency scoops up domestic telephone calling data, as well as the content of U.S. international communications, "inadvertently" grabbing tens of thousands of purely domestic calls each year in the process. The FBI has direct access to this material, and can use it for general criminal purposes through so-called "back door searches." Military officials also collect domestic intelligence for "force protection." A military unit that was caught spying on anti-war protesters under this authority was disbanded in 2008, but the Defense Intelligence Agency picked up its "offensive counterintelligence" duties and re-established an intelligence database in 2010. National Guard units and civilians working at military agencies have been caught illegally spying on domestic protesters, and more recently, engaging in undercover law enforcement activities in violation of the Posse Comitatus Act, prohibiting military personnel from enforcing criminal laws.
2. Information Sharing: Military agencies and personnel participate in formal and informal information sharing programs on the federal and state level, including between FBI Joint Terrorism Task Forces, state and local law enforcement intelligence fusion centers, and information sharing networks like the Navy's Law Enforcement Information Exchange (LInX), and the FBI's eGuardian program. Though there are legal limits to the type of work military officials can do within these programs and the information they can share, there is little to no oversight conducted to ensure they follow the law.
3. Blurred Boundaries: Military intelligence tactics and attitudes rub off on law enforcement personnel assigned to intelligence matters. Most nations outlaw espionage, so foreign intelligence activities have to be carried out through stealth and deception. Avoidance of the law and contempt for the truth can become habitual among intelligence officials, but they simply have no place in a democratic government's interactions with its own citizens. Yet, throughout the history of domestic intelligence operations in the U.S., law enforcement officials have gone to the military intelligence toolbox in selecting their methods. The federal government has loosened or ignored law enforcement guidelines restricting intelligence gathering in the years since 9/11, removing or weakening the criminal predicates necessary to ensure a proper focus on illegal activity. The results were predictable: increased police spying on minorities and political dissidents and increased efforts to escape judicial and public oversight. Federal law enforcement agencies have adopted policies of "parallel construction" to mask the surveillance methods they use to gather evidence, misleading courts and depriving defendants of their right to challenge

[1] https://www.brennancenter.org/our-work/analysis-opinion/militarization-domestic-surveillance-everyones-problem

their constitutionality. Where evidence of improper FBI surveillance has leaked to the public, the Justice Department invoked “state secrets” to shut down litigation.

A number of technologies have aided the mass surveillance attendant upon domestic militarization:

1. Face Recognition: A dragnet surveillance technology whose expansion within law enforcement over the last 20 years has been marred by systematic invasions of privacy, inaccuracies, unreliable results, and racial disparities.[2] Over 20 jurisdictions have banned their local police from using it. However, ICE and CBP are adopting face recognition as a tool for their “Trump Terror” deportation drive, most notable through the development of the “Mobile Fortify” app. This app was only made public through leaked emails and documents obtained by 404Media, and allows agents to point a phone at anyone in public, compare their faces against a variety of government databases (of over 200 million images), and obtain instant access to their name, date of birth, and intimate data. It also allows the contactless collection of fingerprints. In addition to the inherent unreliability of facial recognition, the databases upon which the app relies are full of errors. In 2019, a federal judge ruled ICE’s own database “so unreliable[,] that they could not serve as the basis for probable cause warrants against detention targets.”
2. Drones: The proliferation of unarmed aerial systems (UAS, or drones) presents both opportunities and significant threats to policing and communities, particularly those with significant minority demographics. The ostensible democratization of drone technology has led to increased threats to civilian populations. Domestic law enforcement has dramatically increased its reliance on surveillance drones.[3] Equipped with facial recognition software, infrared technology, and speakers capable of monitoring personal conversations, they pose unprecedented threats to our privacy rights. Interconnected drones could enable mass tracking of vehicles and people in wide areas. Tiny drones could go completely unnoticed while peering into the window of a home or place of worship. These newly emerging technologies are bringing us closer to the reality of a surveillance state, in which our every move is monitored, tracked, recorded and scrutinized by the government.
3. Predictive Policing: Use of advanced statistics, algorithms, and machine learning to predict where crimes may happen, in order that law enforcement officers might find suspects and intervene before 911 calls are placed.[4] Law enforcement relies on a system of crime prediction, crime pattern recognition, and crime analysis to derive crime patterns and to forge advanced systems to guide police departments. It carries multiple inherent risks, including service inequality, lack of public trust (especially in minority communities), and potential privacy violations. *Place-based prediction* predicts the time and location of future criminal activity. *Person-based prediction* identifies individuals who are likely to commit future crimes or become crime victims. The principal techniques involve *statistical crime mapping*, *machine learning algorithms*, *risk terrain modeling (RTM)*, and *social network analysis (SNA)*. Algorithmic bias and privacy concerns persist. Furthermore, there is tremendous risk of further alienating marginalized populations. The practice also raises Fourth Amendment concerns pertaining to unreasonable search and seizure and probably cause.
4. CCTV: mass data collection via AI-powered cameras and license plate readers create detailed movement records, building comprehensive profiles of citizens’ lives without warrants. Pervasive monitoring through smart city sensors, drones, and ubiquitous cameras creates an environment where constant surveillance is normalized. This unchecked surveillance threatens the Fourth Amendment, as well as the First Amendment rights to free speech and assembly (notably in the monitoring of protests). Critics have also argued that constant monitoring has a chilling effect on dissent and normal behavior and fosters censorship.[5]

[2] https://www.aclu.org/news/privacy-technology/ice-face-recognition
[3] https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones
[4] https://www.amu.apus.edu/area-of-study/criminal-justice/resources/what-is-predictive-policing/
[5] https://www.eff.org/deeplinks/2021/09/stop-military-surveillance-drones-coming-home