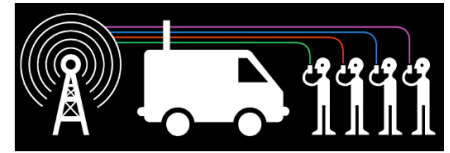


How Are Milwaukee Residents Currently Surveilled?

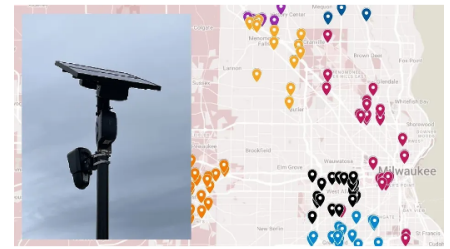
Cell Site Simulators (“Stingrays”)

Also known as cell-site simulators or international mobile subscriber identity (IMSI) catchers, [the device](#) mimics a cell phone communications tower, causing your cell phone to communicate with it. This communications link gives the Stingray the ability to track your location and intercept data from your phone, including voice and typed communications. These devices can disrupt your regular phone service, including making 911 calls.



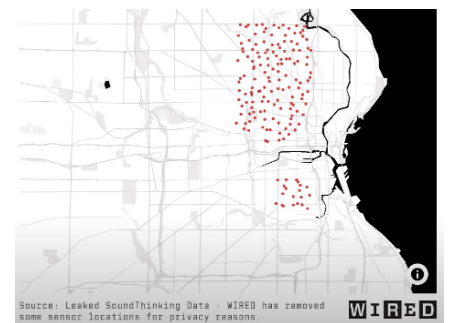
Automated License Plate Readers/Flock Cameras

Automated license plate readers (ALPRs) are high-speed, computer-controlled camera systems typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars. [ALPRs](#) automatically capture all license plate numbers that come into view, along with the location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver/passengers, is uploaded to a central server. [MPD SOP 735](#)



ShotSpotter “Gunshot Detection” Microphones

Milwaukee Police Department uses [ShotSpotter](#) to record audio and send police into areas where the sound of gunshot is detected. Acoustic gunshot detection is a system designed to detect, record, and locate the sound of gunfire and then alert law enforcement. The equipment usually takes the form of sensitive microphones and sensors, some of which must always be listening for the sound of gunshots. They are often accompanied by cameras. They are usually mounted on street lights or other elevated structures, though some are mobile and others operate indoors.



Community Connect Surveillance Camera Network

Through the [Community Connect](#) program, MPD integrates private surveillance cameras for police use. Surveillance cameras are one of the most ubiquitous and recognizable technologies used to watch us as we move about our daily lives. The Milwaukee Police Department, private residences, and local business associations are installing an integrated network of cameras that would give law enforcement 24/7 real time access to surveillance around the city.



Drones

Law enforcement agencies are increasingly collecting our personal information with remote-controlled, and sometimes autonomous, robots and drones. While these devices, especially patrol robots, might look like a fun photo op, they often are equipped with myriad spying technologies, including high definition, live-feed video cameras, thermal infrared video cameras, heat sensors, devices that register wifi pings for cellular devices, and automated license plate readers. Milwaukee Police adopted a “Standard Operating Instruction” on [drones](#), and the Common Council approved their use in March 2025. [MPD SOI: Airborne Assessment Team](#)



Social Media Monitoring/Open Source Intelligence (OSINT)

MPD [acquired an open source intelligence tool](#) ahead of the RNC. “[Open source intelligence](#) (OSINT) involves using freely accessible information to learn about people, places, groups, or events. Information from combing social media platforms, collecting court records, phone numbers, addresses, pictures, videos, geo-location information and more — if gathered from publicly available sources — counts as OSINT.”

Fusion Center

Joint Terrorism Task Forces (JTTFs) and fusion centers are joint federal-state law enforcement intelligence hubs with a long history of investigating, collecting, and disseminating information on protesters and communities of color, but the public has little information about how these entities work and their impact on our rights. [Milwaukee's Southeastern Threat Analysis Center](#) (STAC) was established in 2006 as “a partnership with the FBI Joint Terrorism Task Force, Homeland Security” that disseminates information to other federal, state, and local law enforcement agencies.

Facial Recognition

Facial recognition technology (FRT) is a biometric technology that uses a face or the image of a face to “identify” or verify the identity of an individual in photos, video, or in real-time. FRT systems depend on databases of individuals’ images to train their underlying algorithms. FRT can be prone to failures in its design and in its use, which can implicate people for crimes they haven’t committed. FRT is particularly bad at recognizing Black people and other ethnic minorities, women, young people, and transgender and nonbinary individuals. MPD has proposed [acquiring FRT licenses from the company Biometrica](#) in exchange for “2.5 million jail records,” and currently utilizes FRT from other Wisconsin law enforcement agencies despite no local policy governing its use.