COMMUNITY CONTROL OVER POLICE SURVEILLANCE:

TECHNOLOGY 101

ACLU

TECHNOLOGY 101

The proliferation in local police departments' use of surveillance technology, which in most places has occurred without any community input or control, presents significant threats to civil rights and civil liberties that disproportionately impact communities of color and low-income communities. The nationwide "Community Control Over Police Surveillance" effort is looking to change that through legislation mandating that local communities are given a meaningful opportunity to review and participate in all decisions about if and how surveillance technologies are acquired and used locally.

Here is a list of costly and invasive surveillance technologies that might be recording you, your family, and your neighbors right now.

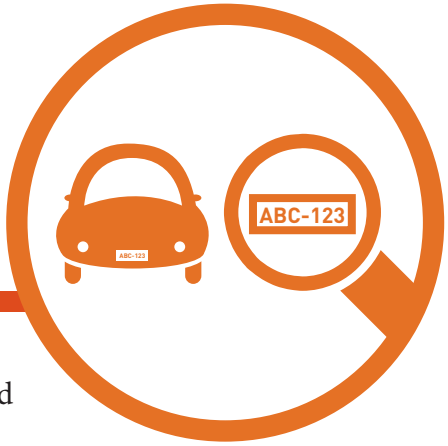
STINGRAYS

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.

The Hailstorm, the latest version of the Stingray, sells for $169,602 per unit. Operational costs are additional and significant.

Whenever a Stingray is used to locate a phone, it also collects information about hundreds or thousands of other phones and their users. The technology is often used without a warrant, and judges are often kept in the dark about its capabilities and limitations. It is very difficult to detect when Stingrays are being used and to ensure they are not being deployed in a discriminatory manner.

AUTOMATIC LICENSE PLATE READERS (ALPR)



Mobile or fixed-location cameras that are used to take photographs of license plates, digitize them, and then store, process, and search captured data in real time or over the course of months or even years.

The data collected by ALPRs is often retained by police departments for considerable periods of time. This allows the government to track where people travel in their cars, including what doctors they go to, what political or religious meetings they attend, and where they sleep at night. Some private companies provide ALPRs to the police free of charge in return for access to the data they collect and the ability to collect fees from private citizens later, such as a vehicle owner they identify as owing outstanding court fees.

ELECTRONIC TOLL READERS OR E-ZPASS PLATE READERS

Electronic toll readers, such as E-ZPass, use radio-frequency identification (RFID) to allow for the collection of tolls using a transponder placed inside a car. They also allow for monitoring of traffic patterns. Although the devices are sold as toll-payment devices, they are frequently used for non-toll purposes without the badge holder's knowledge or permission.

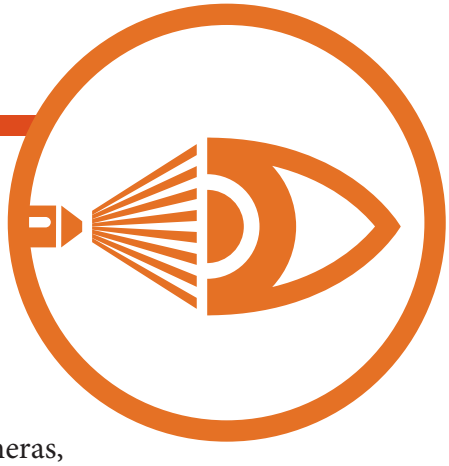
The data captured by electronic toll readers can be stored for an extended period of time and used to create a record of where people travel. The transponders can be read and cars identified in any location there is a RFID receiver, not just at toll booths, which enables the government to develop detailed tracking databases.

CLOSED-CIRCUIT TELEVISION CAMERAS
(CCTV; VIDEO SURVEILLANCE)

CCTV cameras are video cameras that transmit their signal to a limited number of external monitors or computers. They are frequently used by the police to monitor communities remotely. CCTV is also widely used by private entities for security and monitoring purposes.

Despite proof that they are ineffective in reducing crime, CCTV cameras remain over-deployed in areas that are deemed by police to be "high crime," often code for communities of color and low-income communities. CCTV allows the police to monitor residents around the clock in public locations. In communities that are already over-policed, being under the constant, watchful eye of the police greatly increases the risk of having an adverse encounter with the police for every member of the public.

BIOMETRIC SURVEILLANCE TECHNOLOGY



Biometric technologies allow a person to be identified using a physical trait. No longer limited to fingerprints and DNA, publicly known traits such as a person's face or voice can now be run against Department of Motor Vehicle, social network, and other databases to secretly identify and track almost every American. Biometric surveillance technology includes facial, voice, iris, and gait-recognition software and databases.

Used in combination with other surveillance technologies, like CCTV cameras, this tool can completely undermine the ability of person to travel in public or gather with friends anonymously. If video data is stored, this technology can reconstruct anyone's travel history. Technological limitations and biased engineering practices have made facial recognition technology far less accurate in identifying faces of persons of color. This produces more false positives and increases the likelihood that a person of color will unjustifiably draw the attention of law enforcement.

GUNSHOT DETECTION AND LOCATION HARDWARE AND SERVICES (SHOTSPOTTER)

Gunshot detectors, like ShotSpotter, are essentially microphones that are designed to detect the sound of a gunshot. By placing them throughout an area, the microphones are able to triangulate a gunshot and provide police with a limited geographic location from which a gunshot emanated.

While gunshot detectors have a useful law enforcement application, concerns arise from what the devices actually are: microphones that can be used to listen in on a community remotely. If limited solely to detecting and reporting on the locations of gunshots, the devices are not problematic. However, if these secretly operated microphones can be remotely activated and used to listen in on the communities in which they are placed, they can represent another form of general mass surveillance. Only with strict limitations and auditing can we be sure this technology is not abused, and such oversight commonly does not exist.

X-RAY VANS
(Z BACKSCATTER VANS)

The mobile technology uses x-ray radiation to see what no human eye can, such as underneath clothing and car exteriors. An investigative report has shown that these machines may expose people "to ionizing radiation, which can mutate DNA and increase the risk of cancer."

Government purchasers of these vans have not disclosed exactly how they are using them. If they are being used on public streets in non-emergencies and without a warrant, that would be a major constitutional violation and a possible threat to public health. Unless they have probable cause to search a specific vehicle, government agencies should not be roaming U.S. streets conducting backscatter X-ray scans of vehicles and their occupants or bystanders, like pedestrians and cyclists, without their knowledge or consent.

SURVEILLANCE ENABLED LIGHT BULBS
(SURVEILLANCE CAPABLE BULBS OR FIXTURES)

LED surveillance light bulbs, which are presented as energy efficient upgrades to existing incandescent light bulbs, can actually conceal tiny cameras and microphones that can stealthily monitor their surroundings and transmit their feeds back to a central monitoring station.

If these bulbs are installed on municipal streetlamps and put into widespread use, privacy would become as antiquated an idea as the old-fashioned light bulbs the LEDs are replacing. Mass adoption of the technology would throw surveillance nets of almost unprecedented scope over entire communities or cities.

Though marketed as an energy efficient light bulb with built-in monitoring technology, this technology is far more akin to a mass surveillance device being disguised as a light bulb. In truth, the product has a broad surveillance capabilities and far lesser comparative utility as a lighting device.

HACKING SOFTWARE AND HARDWARE

These tools allow law enforcement officials or other government actors to gain access to a person's personal computing equipment (including laptops and cell phones) and password-protected websites or accounts (like cloud storage or social media accounts). They can enable hacking to be performed in person and remotely without the permission of the account holder or service operator.

"Hacking" technology is surveillance because a government that hacks into a private computer or account intends to surveil the private contents of the hacked computer or account without the owner's permission or knowledge. Using hacking software or hardware is like picking a lock to break into someone's house — the act is an integral part of the unlawful entering.

Most hacking tools depend on vulnerabilities in commonly used computer software and services. When our government and police use hacking tools, which exploit these vulnerabilities rather than addressing them, they not only leave the systems open to their own intrusions but also to intrusions by hackers, criminals, and foreign governments.

SOCIAL MEDIA MONITORING SOFTWARE OR SMMS

(DIGITAL STAKEOUT; XI SOCIAL DISCOVERY; GEOFEEDIA; DATAMINR; DUNAMI; SOCIOSPYDER)

This software can be used to covertly monitor, collect, and analyze individuals' social media data from platforms like Twitter, Facebook, and Instagram. It can identify social media posts and users based on specific keywords; geographically track people as they communicate; chart people's relationships, networks, and associations; monitor protests; identify the leaders of political and social movements; and measure a person's influence.

The technology is also promoted as a predictor of future events, including threat assessment.

Instead of relying on criminal activity to prompt investigations, SMMS is used to cast nets so wide it encompasses the entire internet, sweeping in scores of innocent people. Moreover, the technology has been used to disproportionately target persons of color, including Black Lives Matter activists. As the public grows increasingly aware of the government's monitoring of social media, SMMS has the potential to drastically discourage free speech on the internet.

THROUGH-THE-WALL SENSORS/RADAR (TTWS)

This technology uses radar or similar technology to peer through walls of a building. Currently, the technology is precise enough to ascertain how many people are in a particular room within a dwelling unit and, over time, the clarity of the image produced may be able to determine the identities of a building's occupants.

The Xaver 400, the latest version of the TTWS model sold by Camero-Tech, sells for $47,500 per unit. Operational costs are additional and significant.

While this technology may have beneficial uses, no uses are appropriate without a warrant. As the technology advances, this tool may increasingly be deployed as an improper tool for looking into private homes without court oversight.

POLICE BODY CAMERAS

This wearable video and audio recording technology captures police interactions with the public from an angle approximating a police officer's point of view. Device functionality, operations, and reliability can vary significantly based on the manufacturer and operating software.

According to a February 2015 news report, the most popular seller of

police body cameras and related services, Taser, offered the City of San Diego a five-year contract that included the purchase of 1,000 cameras for $267,000 and another $3,600,000 for data storage contracts, software licenses, maintenance, warranties, and related equipment. This figure does not include internal operations cost, which are significant.

While wearable cameras have the potential to promote officer/public safety and provide greater police transparency and accountability, they can also present a significant threat to privacy. The utility of these devices is largely determined by the policies that govern their operations. With the wrong policies in place, body cameras can be turned from a transparency and accountability tool into a police propaganda and mass surveillance tool.

PREDICTIVE POLICING SOFTWARE

Predictive policing software uses mathematical and analytical techniques to attempt to predict future criminal activity, offenders, and victims.

In 2014, predictive policing software manufacturer PredPol offered the Orange County Sheriff's Office a discounted rate of $103,000 for an annual subscription to use their predictive policing software. This rate does not include other, significant personnel, data, and technology-related costs.

The predictive policing model is deceptive and problematic. Inputting historically biased data into a computer and then running it through an algorithm produces biased results that will merely continue the trend of over-policing communities of color and low-income communities. This highly untested technology raises additional questions, such as how accurate the algorithms are that extract information from the data. These tools are often proprietary, with their algorithms, data inputs, and source code being shielded from public review and oversight.

For more information visit ***www.communityCTRL.com***