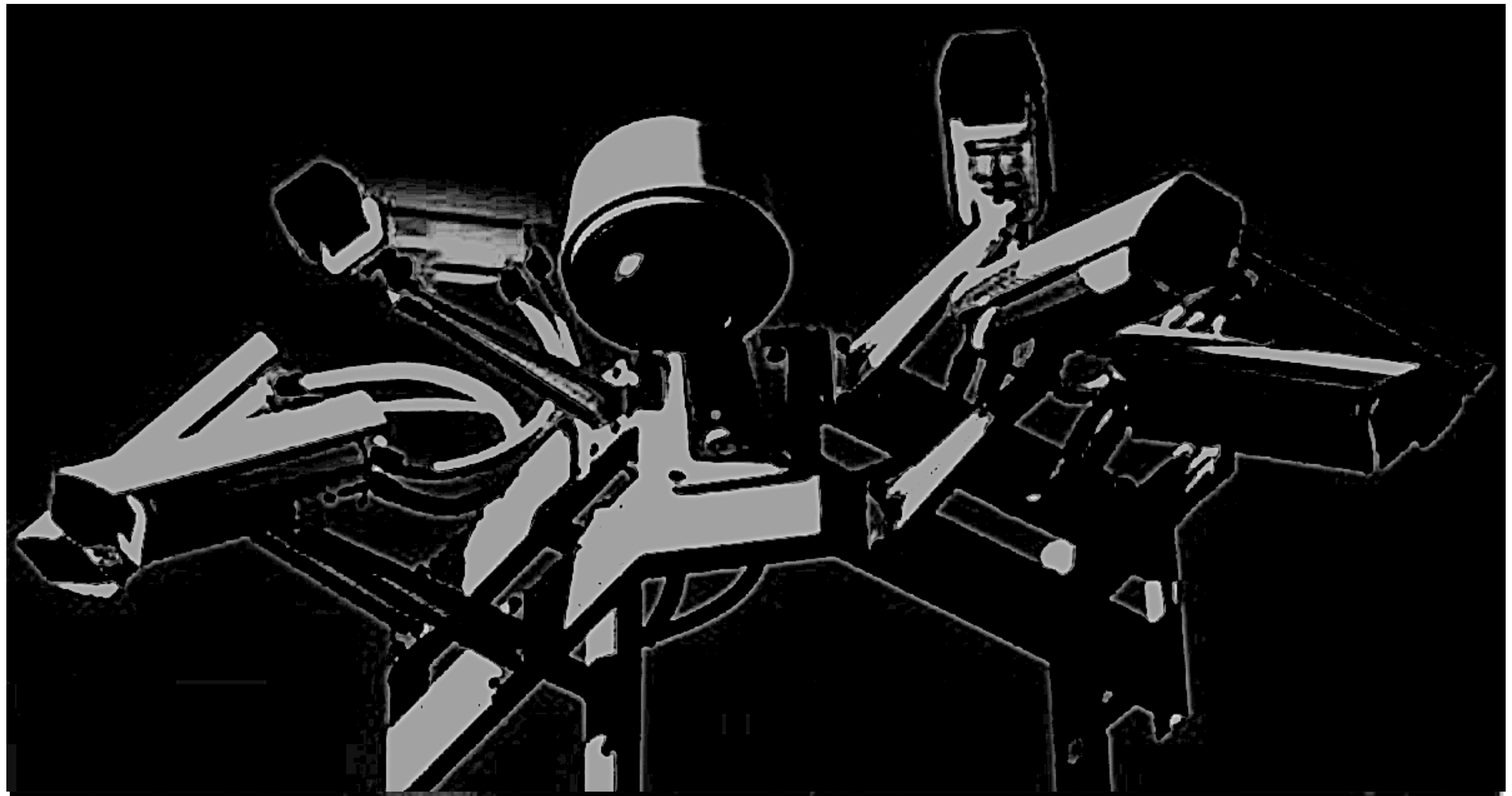
Please feel free to distribute this zine to yr friends by scanning & printing a physical copy—we don't need to put everything we're thinking about on the internet. Ⓐ

*Tin Foil is the New **Black***

a brief reminder to double layer yo tinfoil



BEWARE OF VEHICLES
小心車輛

A **Tire Pressure Monitoring System (TPMS)** is a 315MHz transmitter located at the valve stem on your rim (not the tire). This device has its own battery, a unique ID, and also conveniently enough, your VIN number.

The only real solution here is to create/ buy a 315 Hz Jammer. If you were to google this you would be able to find ways of doing it.

Further reading:

https://www.defcon.org/images/defcon-21/dc-21-presentations/Pukingmonkey/DEFCON-21-Pukingmonkey-The-Road-Less-Surreptitiously-Traveled-Updated.pdf

Black bloc tactics have been around for a few generations, although they didn't really start spreading in the US until the late 1990s during the anti-WTO mobilizations. Bloc tactics have kept many a rebel out of prison and will continue to do so, but times are changing. "No face, no case" isn't necessarily true anymore, and so black bloc & other insurgent tactics must be reevaluated and updated accordingly.

The systems of control employed by the state to halt any form of insurrection are getting more advanced by the day. But they still can't fucking stop us. No matter how small or far away, each insurrection builds a larger culture of resistance, support, and strength. Tactics developed in Hong Kong just a few months ago are already generalizing across revolts from Chile to France.

However, the state understands our potential and will do anything to make sure we don't get our momentum going, that our tactics don't spread. Surveillance technology is advancing rapidly, and we need to understand what we're up against so we can develop more militant, organized, and informed strategies—not to mention stay the fuck outta prison.

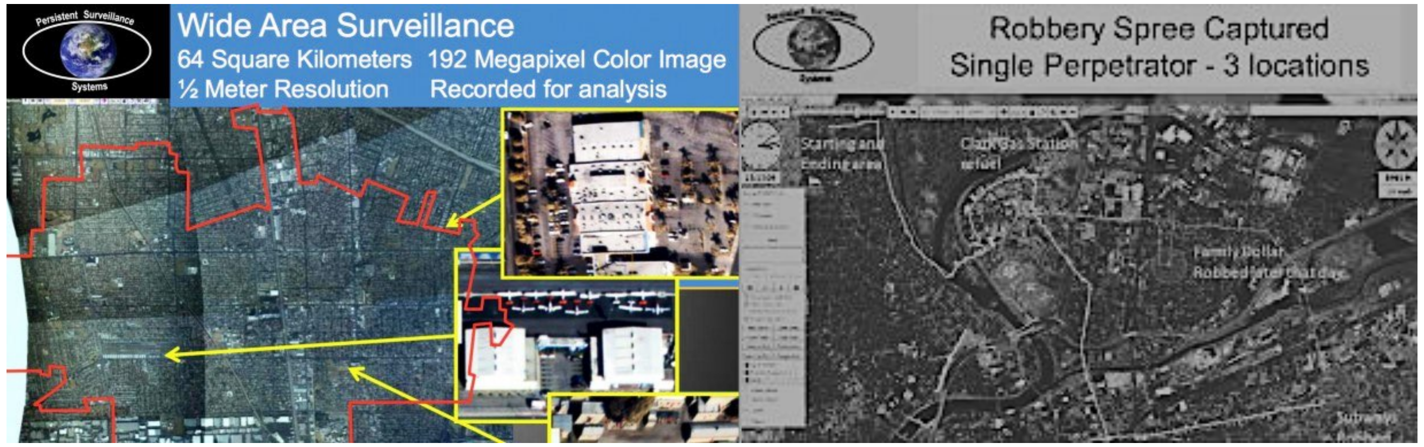
So here is a brief outline of some of the newer & lesser-known surveillance technologies that are currently being deployed by the United States.

This zine is not meant to scare anyone off from bloc tactics, sabotage, or guerrilla attacks. This is simply a brief reminder to double layer yo tinfoil. By the time this zine reaches your hands, even more new tech has probably already been used against the movement.

Aerial Surveillance

Widespread persistent surveillance technologies are a relatively new threat to radicals which must be taken into account for future actions.

Starting in around 2005, the United States military began developing surveillance systems which could be mounted on a plane to provide surveillance over an entire region. At first, the cameras were unable to distinguish between fine details. However, 12 years later, the cameras being mounted onto aircrafts can distinguish between models of cars, individual wardrobe, and possibly even use facial recognition.

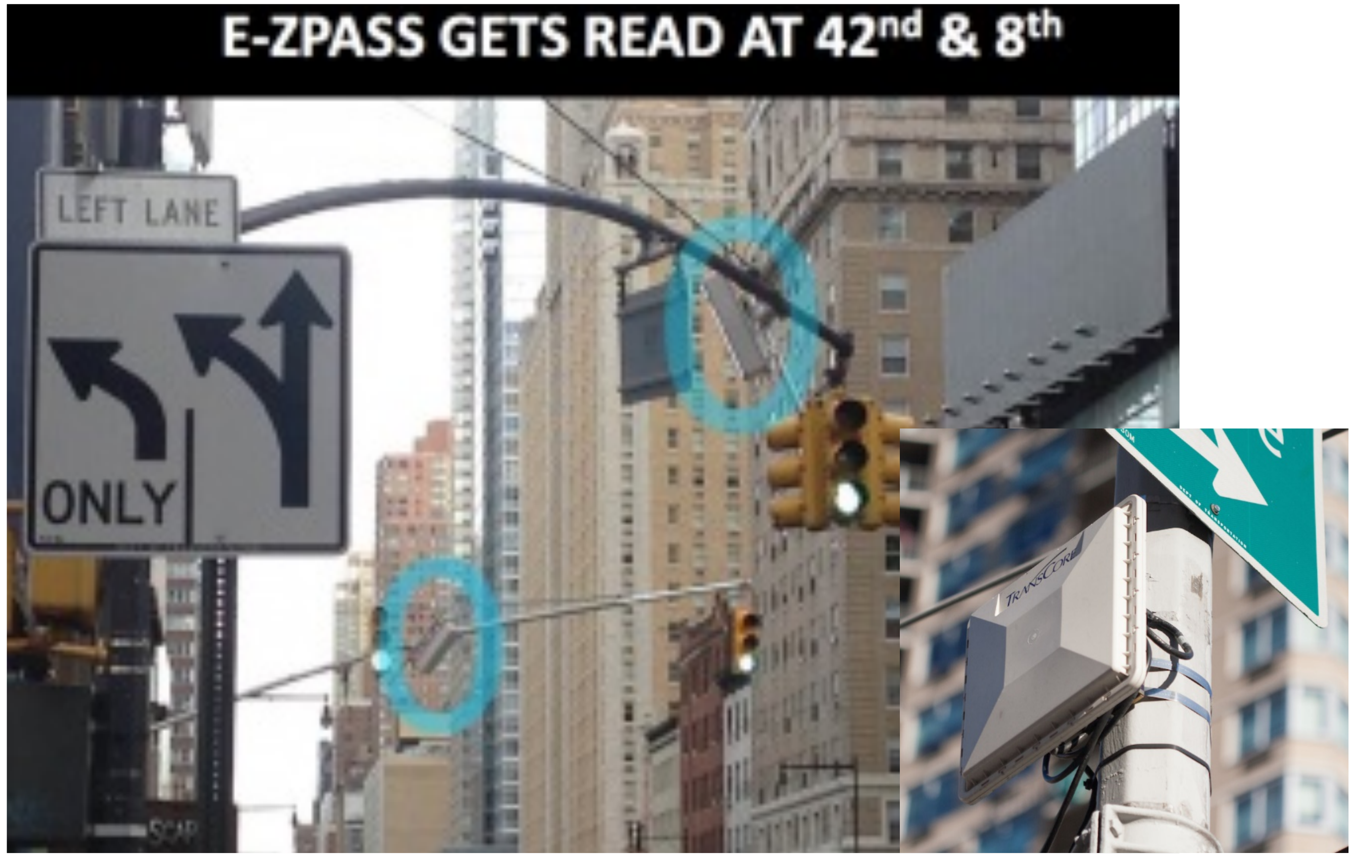


For example. Kestrel is a surveillance system was developed by the military in 2010. By 2012, the Science and Technology Directorate for the Department of Homeland Security conducted a seven-day demonstration of the system in Nogales, Arizona. The purpose of the tests was to tests the systems capability to detect and track activity across the Mexican border.

Kestrel apparently led to the development of the Simera wide-area persistent surveillance system. Simera's website claims the system can "monitor an entire city-sized area at once, detecting vehicles and moving dismounts in near real-time. In addition, Simera provides operators with a readily accessible digital video recording of the entire field of view for later analysis."

These systems are exceptionally expensive and as a result many law enforcement agencies have to rent these out for events from private companies so you can really just look all this shit up. The Baltimore police own a small plane which is fitted with a camera developed by a company named Persistent Surveillance Technologies which regularly patrol Baltimore, providing real time information to law enforcement officers on the ground nearly everyday.

Electronic Toll Collection Tags are RFID readers which work with transmitters used to pay tolls (E-Zpass, Allegro, eGo). While I'm uncomfortable with my location being tracked every time I pay a toll, tollbooths aren't really the issue here.



Transcore is an ITS and Tolling company which collects car location data. Transcore has developed readers which can pick up on all transportation formats (E-Zpass vs. eGo). This company, along with others, have put up readers at nearly every intersection in every major city.

The justification for it is these readers can be used by emergency response services to turn all traffic signals red at an intersection an emergency response vehicle is approaching. Another justification used is that they help the Department of Transportation estimate travel times as these devices can accurately calculate how many cars per minute are moving past the fixed point.

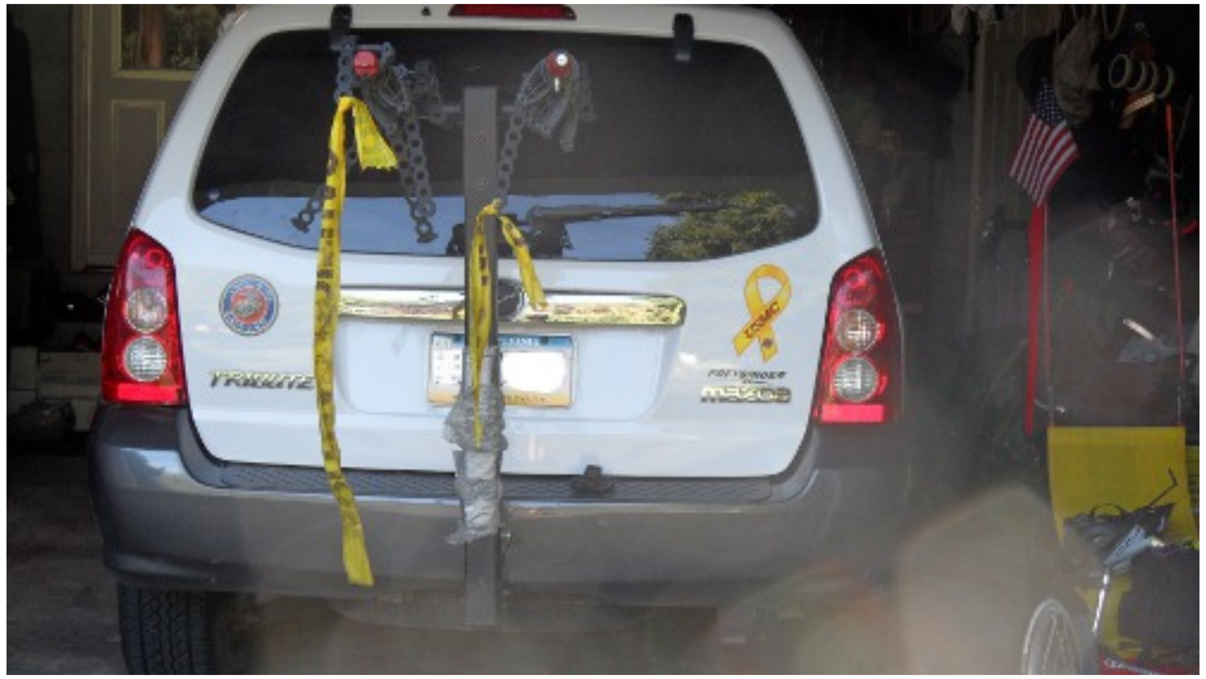
However, conveniently enough, these readers which have been installed at most traffic intersections also have the capability to record every E-Zpass-like device which travels past it. I could only guess who is interested in buying that data.

So get the fuck rid of your fancypants toll device.

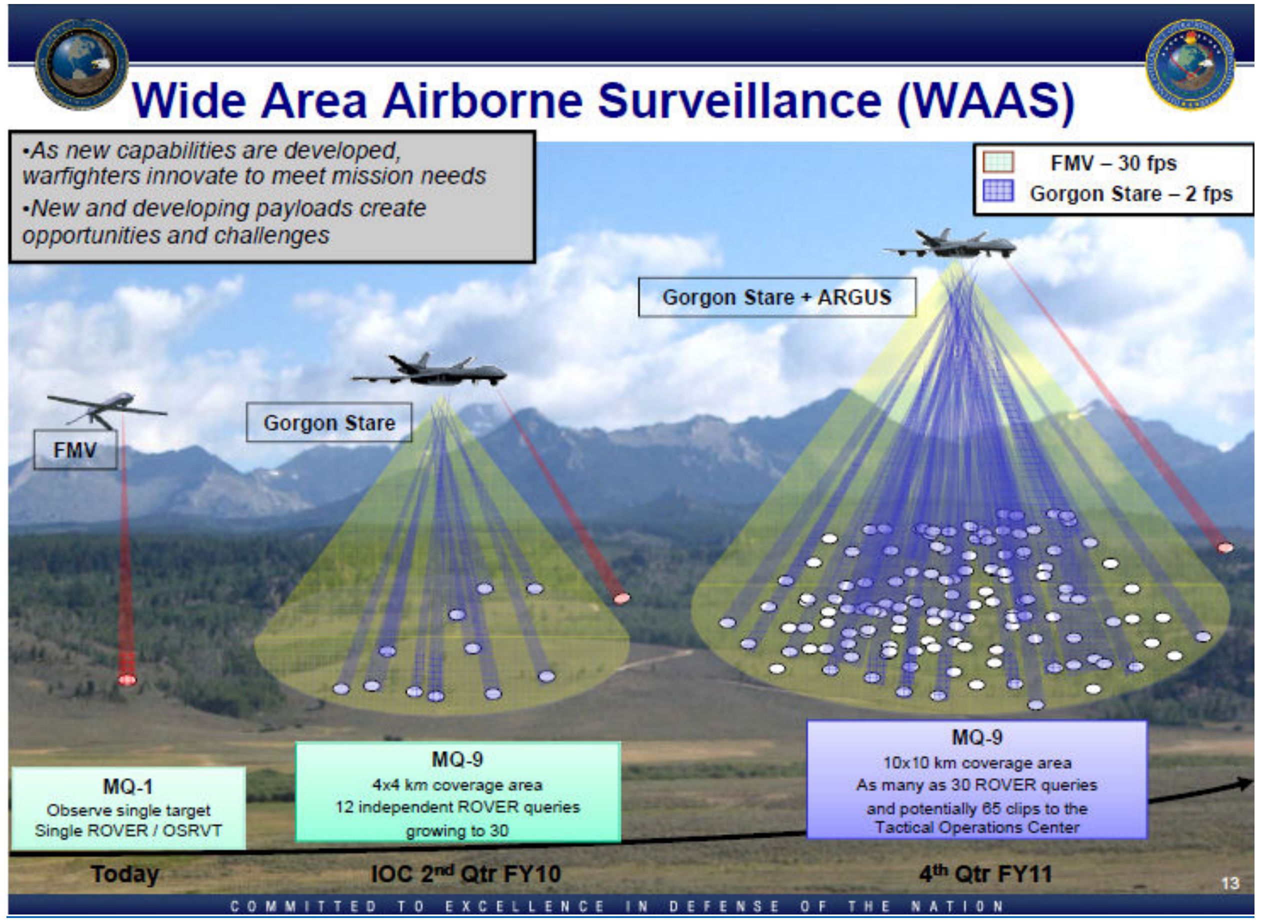
Additionally, you can get pretty creative obscuring the rear plates. Maybe your trunk was packed just a little too full and you had to get a rope to tie it down, obscuring two of the characters? Maybe you got a trailer hitch for the back of your car that is positioned in a way to obscure a couple characters? Going out for a nice bike ride but can't fit your bike in your trunk? A bike rack could also help you out.

You get what I mean. If you really want to, you can find a way which isn't terribly sketchy to cover your plates.

Tactics like this are not necessarily meant for everyday use. Treat them more like an extra layer of security while you on you way to the pinewood derby with your scout mates.



Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS) was created by BAE Systems in a government funded project. This system claims to be able to monitor every movement of every person in a 36 mile square area by attaching one of their cameras to an unmanned aircraft.



Wide Area Airborne Surveillance (WAAS)

•As new capabilities are developed, warfighters innovate to meet mission needs
•New and developing payloads create opportunities and challenges

FMV – 30 fps
Gorgon Stare – 2 fps

MQ-1
Observe single target
Single ROVER / OSRVT

MQ-9
4x4 km coverage area
12 independent ROVER queries growing to 30

MQ-9
10x10 km coverage area
As many as 30 ROVER queries and potentially 65 clips to the Tactical Operations Center

Today
IOC 2nd Qtr FY10
4th Qtr FY11

13

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

ARGUS-IS utilizes an automatic object-tracking software called Persistics which claims to "stabilize video, eliminate parallax, compress background, and provide unprecedented subpixel resolution of moving objects of interest. The technique permits "seamless stitching," a process that optically combines images from multiple cameras to create a virtual large-format camera, as well as the ability to compare images of the same area at different times and identify what has changed over that period."

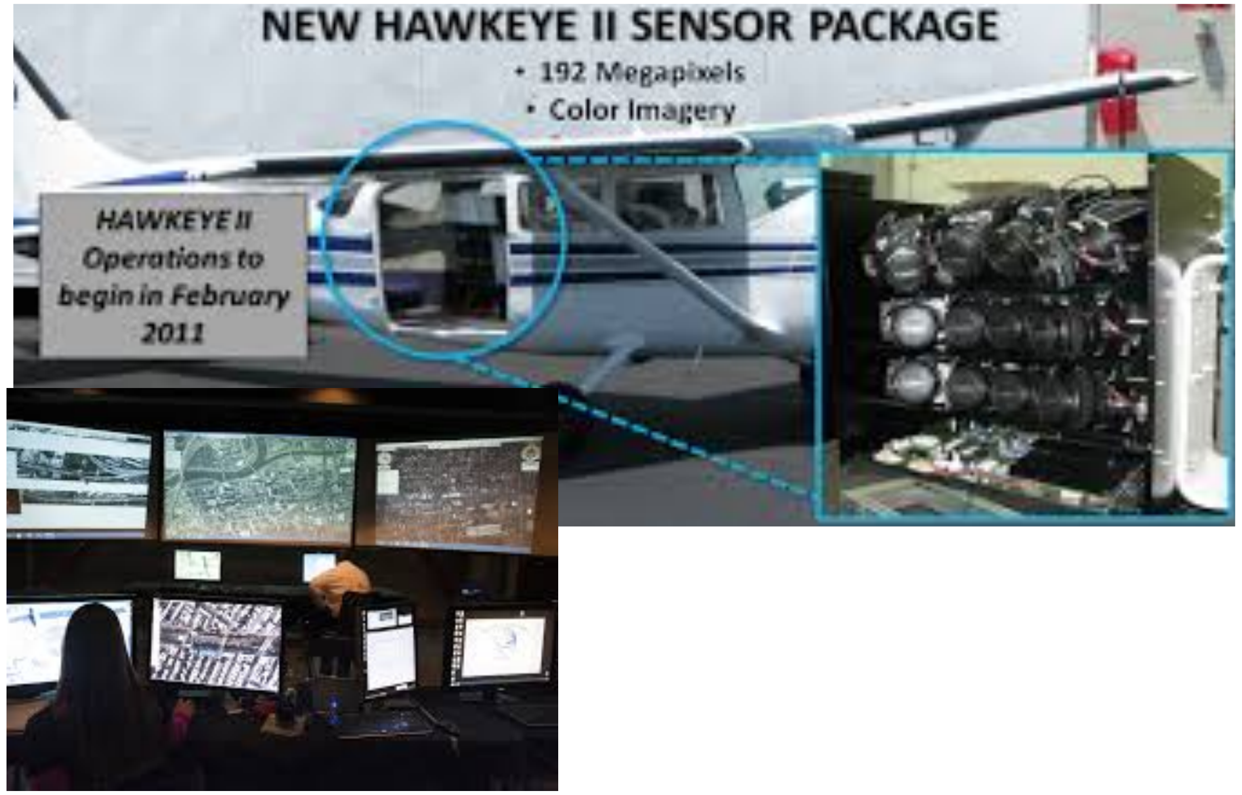
The combination of aerial surveillance in addition to a unified grid of cctv cameras populating most cities seems to be incredibly advantageous to law enforcement. There are traffic cameras on nearly every city intersection at this point.

We know that locations have been and will be tracked from wide-area aerial surveillance systems attached to drones or planes and helicopters. The Baltimore and Ferguson riots had FBI planes flying in circles for the duration of them both. We know the feds have on-demand access to cameras on nearly every street. What might not be an unfair assumption to make at this point would be that the paths of instigators can be tracked through aerial footage and then their path can be compared to accessible cameras so continuous footage can be compiled to getting high resolution footage of the beautiful soul in question.

Relatively cheap improvisations can render billion dollar projects ineffective. One idea is to develop a strategy of large clusters using umbrellas. If there are 10 or 15 people walking in the middle of the bloc with umbrellas all connected to one another, an individual could get mixed up relatively easily. Easily enough it would be very hard to track the specific paths of instigators or have any surveillance really hold up in court.

It may prove advantageous in future actions to have individuals run in and out of the umbrellas in random paths while others are taking part in the Lord's work, providing enough confusion that tracking software from above would be unable to decide any of the paths of the instigators and thus the threat of matching aerial footage with cctv footage in court is diminished.

Additionally, as was seen in the 2017 Portland Mayday shenanigans, some folks had the great idea of running in circles around the bloc holding up smoke bombs in each hand. This seemed like it was pretty effective in making the cameras unable to discern who is doing what.


NEW HAWKEYE II SENSOR PACKAGE
• 192 Megapixels
• Color Imagery
HAWKEYE II Operations to begin in February 2011

vision, which is retained in a database for 21 days to 5 years depending on the jurisdiction. In 2009, in new York city, there were 108 fixed APLRs and 130 mobile. With this many data points, it is not difficult for the state to set up an automated program which has a location history for each car.

A company called Vigilant Solutions (whose only customers are law enforcement) has a presence in 28 metro areas reading about 35 million plate a month. Additionally, many tow truck operators use these cameras looking for repo hits, but then sell the data to law enforcement.

So, what do we do from here? There is a robust private market centered on tracking our cars' locations, then selling the data to the pigs who will certainly use it against us. In many states, a front license plate is not required. In some places/ times/ circumstances, it may be worth the risk to remove your front license plate.

Now if you have a pick up truck, if you close the back bed of the truck, the license plate *should* be unreadable from most angles. This is probably something that can get you pulled over if the wrong pig sees you, but that risk may be better than having yourself be tied to an event.

There are also some ways of playing with your license plate. You can scratch off the reflective gloss on your plates. This is illegal in CA and MA but legal elsewhere and makes it harder for the APLR to read the plate. Some states allow you to have stacked characters rather than linearly aligned, this makes it a little harder to pick up on as well.

Some folks have taken to buying old iPod touches in cash off craigslist, using a burner number to set up Signal, and only using the wifi in public places with no cameras.

The ability of law enforcement agencies to track cell phone GPS data is also concerning in that they also have the ability to turn on the microphone of the cellphone. For example, it would be relatively easy to set up a program which waits until people of interest are meters apart from one another, and then turns on the microphones of the cell phones. Now, this is not admissible in court, however, it can be used in Grand Jury Trials to intimidate you or your friends into being informants or by Feds trying to fuck with your mind and scare you into snitching.

License Plate Readers

So pretty much all of this is taken from a presentation that I will link at the end but I thought it was important enough to include.   With so many folks driving across state lines to go to actions, it's important that we limit the amount in which our vehicle locations are monitored, collected, and analyzed. Even if one were to not bring a phone to an action and cover ones face, their car being tracked in the vicinity of an alleged action can hurt their case.

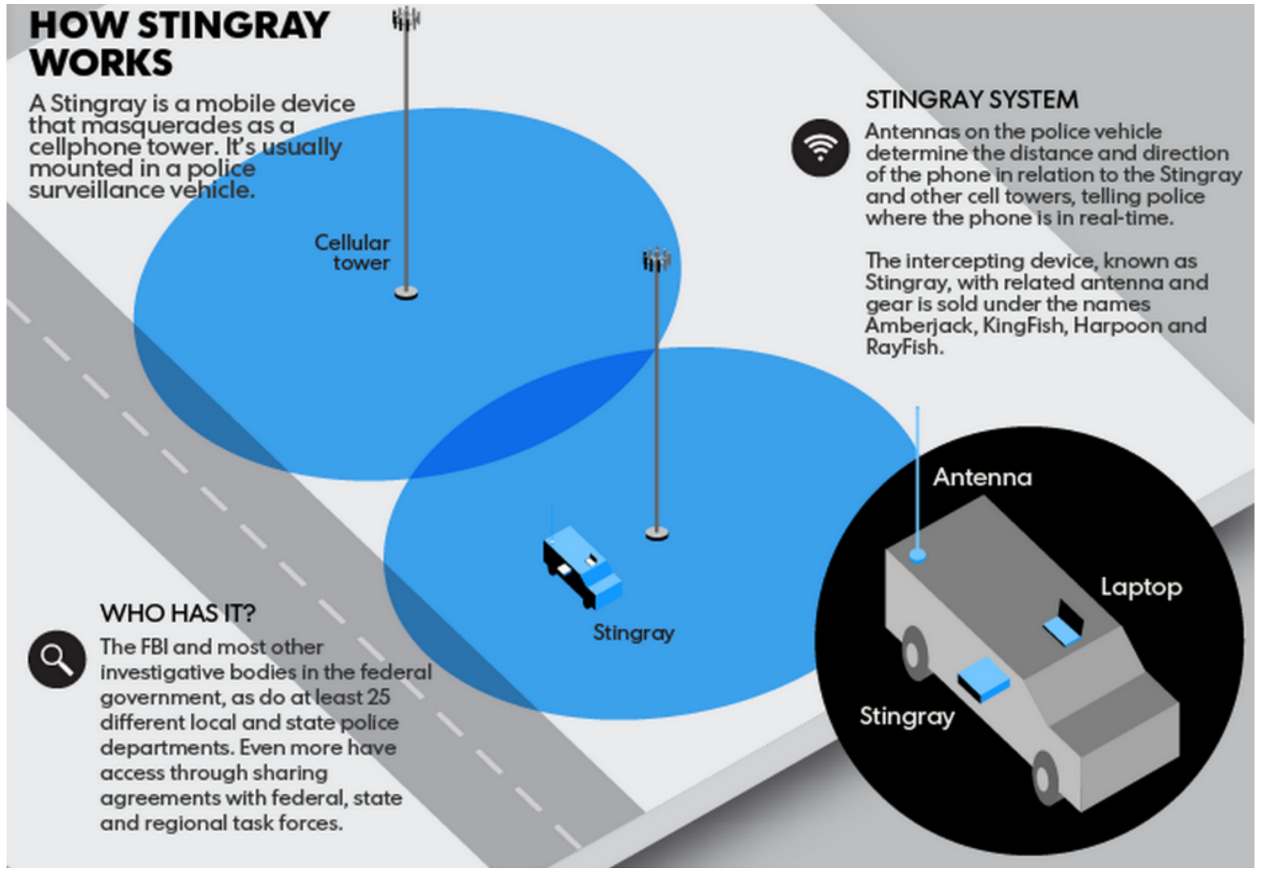
There are three main ways in which car locations are tracked: Automatic License Plate Readers (ALPRs), Transponder based Electronic Toll Collection (ETC), and automatic tire pressure monitors.

Automatic License Plate Readers are a system of cameras, computers, and GPS that can read license plates and notes the coordinates and time of passage. These systems can be in fixed locations or can be used mobile.   They have the ability to read 3,000 plates/hour and all the data is saved to a central repository.   They are commonly seen on the back of police cars but may also be located on the top of the police car, next to the sirens.

These cameras can also be put next to traffic signals on telephone poles at busy, urban intersections.   They can be hard to distinguish from red light cameras and may be located right next to a bundle of red light cameras.   These automatic license plate readers can capture all plates in their field of

ISMI (stingrays)

I would hope at this point most radicals have heard of "stingray" devices which local, state, and federal law enforcement agencies regularly use. The concept behind a stingray is that the device is either stationary or placed in a moving car or plane, when in operation, the device acts as a cell phone tower. It tricks all of the cellphones in the area to first connecting to the stingray, before later connecting to the cell tower.



HOW STINGRAY WORKS

A Stingray is a mobile device that masquerades as a cellphone tower. It's usually mounted in a police surveillance vehicle.

STINGRAY SYSTEM

Antennas on the police vehicle determine the distance and direction of the phone in relation to the Stingray and other cell towers, telling police where the phone is in real-time.

The intercepting device, known as Stingray, with related antenna and gear is sold under the names Amberjack, KingFish, Harpoon and RayFish.

WHO HAS IT?

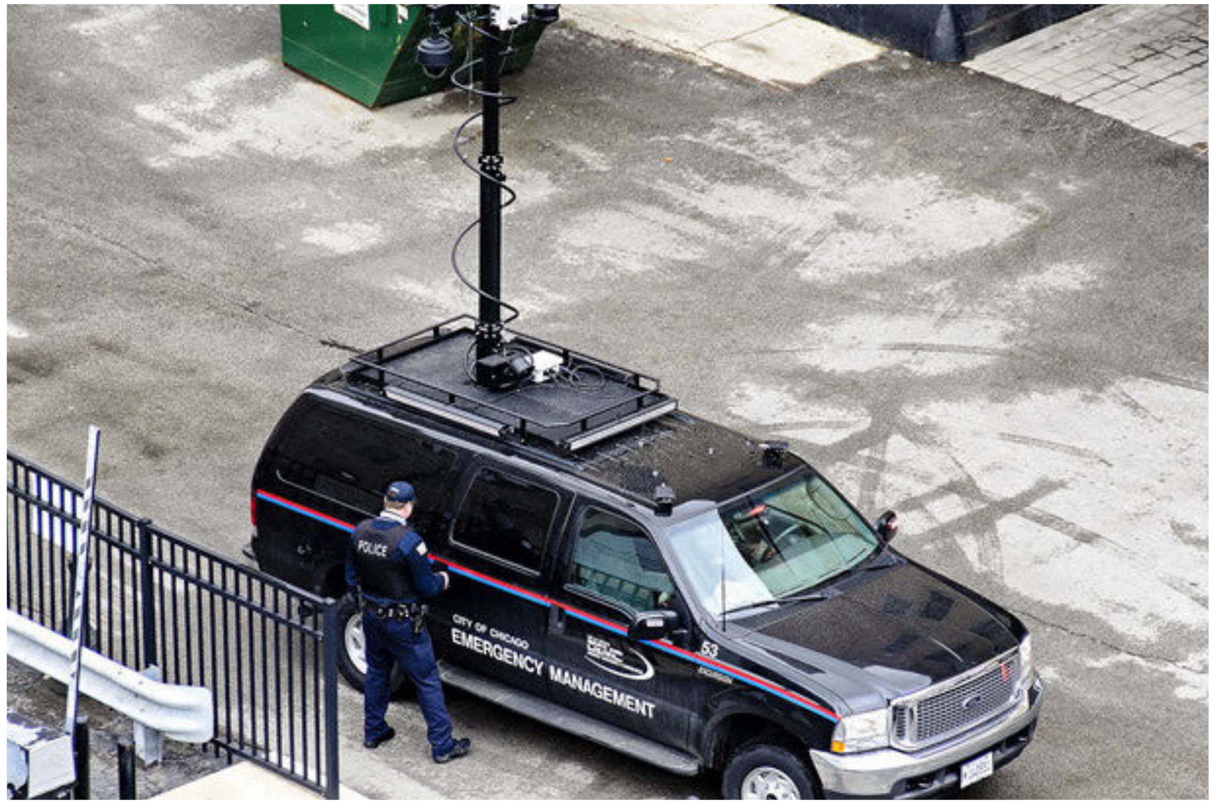
The FBI and most other investigative bodies in the federal government, as do at least 25 different local and state police departments. Even more have access through sharing agreements with federal, state and regional task forces.

Stingrays relay text messages, phone calls, and GPS locations to law enforcement before sending them to the cell tower of the cellular provider. Different stingrays have different effective lengths, some have discrete antennas which are usually fitted on top of police vans which boost their strength. It has also been reported some stingrays have the ability to act as a cellular jammer, making phone communication impossible if law enforcement so wishes.

The use of stingrays was contested by civil liberties groups until finally, the FBI placed a gag order on the use of stingrays by local and state law enforcement agencies. This means the police may be tracking you and arrested you because of your messages, however, unable to reveal such information in court.

This often takes the form of law enforcement waiting for larger drug deals to be mentioned, then the police will pull over the car with the money/ drugs for speeding (even if it wasn't speeding) then say the car smells like weed (even if it doesn't), and bam! The police department just made a lot of money through asset seizure.

The best defense against a stingray? Never send a text that you wouldn't want read back to you by a federal prosecutor that's trying to lock you up. Other than that, using encrypted apps like Signal or burner phones isn't a bad idea. But remember, stingrays will still intercept your messages, calls, and GPS location with a burner phone. There will be no name legally tied to the number, but if one chooses to identify themselves to a friend over the burner phone, it will be recorded along with the locations in which the phone is turned on. There is a good guide which will be linked at the end on how to effectively use a burner phone.



Signal offers *relatively* strong end-to-end encryption with other Signal users. Now, I wouldn't trust saying anything over Signal which would get feds all over you, but it works relatively well for low to medium risk conversations or simply trying to avoid Big Brother from knowing who you are close with.

However, Signal has some flaws. If someone who you were messaging gets arrested and their phone seized, all of your messages will be on display to law enforcement if the person who you were talking to did not delete their messages or have a password set up. Some tips for using Signal: set disappearing messages on, tell your friends to set disappearing messages on, set a different password on both your phone lock screen as well as signal itself. Try to use as many capitalizations, numbers, and special characters as you can in the passwords.

Even then, Signal will never be perfect. I am confident the NSA could crack Signals encryption if they *really* wanted to; but that does not mean it would be admissible in court. If we're talking about end-to-end encryption when both ends are already compromised, any assumption of privacy using Signal is relative.

While the messages sent may be protected, that does not mean the keyboard that's typing them is protected. Who is to say the NSA hasn't gotten backdoors to either the keyboard by bugging your phone with a key logger, or by monitoring the pressure points on the touch screen which can be overlaid with a keyboard to reveal the message? Another tip for using Signal is to set notifications off; that way, google cannot access the text of the incoming message by having direct access to the notification system. There are also APK packs for android online which allow you to verify and install Signal outside of the google play store so that google is involved as little as possible.