Testimony for the Baltimore City Council, Public Safety Committee
October 16, 2018

Oversight Hearing Regarding Persistent Surveillance Systems

DAVID ROCAH
SENIOR STAFF ATTORNEY

The ACLU of Maryland, on behalf of its more than 5,000 members in Baltimore City, strongly opposes any effort to resume the persistent aerial surveillance of Baltimore's residents.

It is important at the outset to make clear what this technology does, and how it works, particularly given Ross McNutt's attempts to misleadingly downplay its capacities and implications when trying to sell it to the public (you can be sure that his sales pitches to police departments are quite different). In design and intent, Persistent Surveillance Systems technology seeks to create a permanent video record of everywhere that everyone in Baltimore goes any time they go outside. It does this by stitching together and storing incredibly high resolution wide angle photographs taken once per second that capture about half of the City in each frame. This provides a slow frame video that can be zoomed in to show individual people (or cars) moving about the city. And because the video is stored (indefinitely, it turns out), it is a virtual time machine, allowing police (or Mr. McNutt) to back in time to any location or person they are interested in, and to follow a particular person or car backwards (and forwards) in time to see where they went or came from. It is the technological equivalent of having a police officer follow you every time you walk outside. But because it is done remotely, via high tech surveillance equipment, we do not viscerally experience the intrusion that would be obvious to all if an officer did this.

AMERICAN CIVIL
LIBERTIES UNION
OF MARYLAND

MAIN OFFICE
& MAILING ADDRESS
3600 CLIPPER MILL ROAD
SUITE 350
BALTIMORE, MD 21211
T/410-889-8555
or 240-274-5295
F/410-366-7838

WWW.ACLU-MD.ORG

COLEMAN BAZELON
PRESIDENT

DANA VICKERS SHELLEY
EXECUTIVE DIRECTOR

ANDREW FREEMAN
GENERAL COUNSEL

Mr. McNutt is fond of saying that the footage is not sufficiently high resolution to allow any particular person to be identified just from the video itself. While (currently) true, this also completely misses the point, since the entire purpose of capturing the footage is to identify people or vehicles. That's what it was invented for when used in the Iraq war, and that what it is being proposed for here. This is done in multiple ways. First, the person or vehicle being tracked on the stored footage can be linked to images captured by Baltimore's network of more than 700 ground based Citywatch cameras, and people and vehicles can be identified that way. Moreover, because the aerial footage allows people or cars to be tracked forward and backward in time until the people enter or leave particular buildings, it can also, without any other technology, be used to identify those same people, which, again, is the entire point.

It is also important to note a general point regarding all of the claimed technological limitations of this surveillance technology as it currently exists. First, the development of the technology itself is purely a one-way street going towards ever more detailed surveillance. Camera resolutions are only getting higher, not lower. Camera prices per pixel of resolution are only going down, not up. Technology allowing surveillance at night via infrared cameras already exists. High resolution radar allowing tracking of vehicles through cloud cover already exists. The cost of deploying the technology is only going down, not up, because it can be (and if used, almost inevitably will be) mounted on drone

aircraft that can effectively stay aloft indefinitely, rather than on human crewed Cessna airplanes, as it currently done. And the cost of analysis will only go down, as artificial intelligence programs are used to cull through the stored footage.

And if we allow the Ross McNutt's of the world, or the Baltimore Police Department, to assemble this kind of surveillance data (whether or not at government expense), it will inevitably be used for purposes far beyond what he and other proponents now claim is the need or justification. We see this kind of mission creep in the very technology itself, which was created for the U.S. military's use when fighting in Iraq, as a means of identifying insurgents, and has now moved to domestic law enforcement. But we also have already seen mission creep in its domestic use. When Mr. McNutt or his astroturf emissaries go to community meetings promoting the technology, they claim it will only be used to solve serious crimes, like murder. But even in the limited secret deployment in Baltimore, it was used to assist police in identifying dirt bike riders, illegal dumping, and to identify who might have been responsible for traffic accidents (indeed that last use was, by far, the most common one, accounting for 42 out of 105 "case briefings" written by company analysts). And the system was also used, repeatedly, to monitor political protests, once to monitor protests in the wake of the Ceasar Goodson verdict arising out of Freddie Grey's killing, and again based on concerns that "Black Lives Matter" activists might try to disrupt an Orioles baseball game. This kind of use to monitor political activists is precisely why the mass collection of location data is so dangerous. As the Supreme Court recently said in *Carpenter v. U.S.,* 138 S.Ct. 2206, 2217 (2018), holding that the FBI's collection of a cell phone subscriber's location data without a warrant violated the Fourth Amendment, the "time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'". That is equally true of the location data that Mr. McNutt would vacuum up about every Baltimore resident on behalf of the BPD, without any warrants.

AMERICAN CIVIL LIBERTIES UNION OF MARYLAND

But mission creep within the BPD is not the only danger. The surveillance data that Mr. McNutt is collecting belongs to him, not the BPD. And he has acknowledged that he wants to sell that data to anyone he can convince to buy it, suggesting that insurance companies might want it to determine who was at fault in a traffic accident. But if he can make money selling data to insurance companies about traffic accidents, he can also make money selling data to anyone off the street interested in collecting location information about a resident of Baltimore, including politicians seeking information about opponents or critics. And as my colleague at the ACLU National Office has pointed out, this is a system is capable of recording all kinds lifestyle information that could be commercially useful, such as how often individual drivers exceed the speed limit, how often you go to the gym, how often you go to a bar, where you shop, and so on. The possibilities are almost endless.

Finally, we have seen repeatedly that bulk surveillance data like this never stays siloed within any particular government entity or agency, because it is potentially of interest to other governmental actors. For example Maryland now compiles all of the automated license plate reader data (time, date, and geo tagged data showing when and where a

particular car license plate was photographed) captured by individual police departments in a central state database, accessible to all law enforcement agencies. Even if you, incomprehensibly, trust the Baltimore Police Department and Ross McNutt with this kind of mass surveillance data, do you equally trust the Donald Trump Department of Justice (or any other possible future justice department) with what they might do with it.

Both the BPD and Mr. McNutt suggest that we can solve the privacy problems inherent in this kind of mass surveillance by having good policies restricting the use of the data. When the surveillance was first disclosed in 2016, the Baltimore Police Department claimed it was governed by strict privacy policies. That turned out to be totally false. The only policy they could point to was the general policy governing Citywatch cameras, which had nothing whatsoever to do with this surveillance, and which did absolutely nothing to address any of the privacy concerns. And if ever there was a police department that should give us good reason to doubt their ability to adhere to, or enforce adherence to, police policies, it is the BPD. That department is simply not in a position to say "trust us," particularly, but not only, because of the insane secrecy that surrounded the original deployment of this program, until they have shown that that trust has been earned.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

And with respect to Mr. McNutt, who is the actual owner and custodian of the data, there is even less reason to trust him. First, whatever "policies" he may currently claim to have is totally meaningless, because as a private businessman, he can change them at any time, to whatever he wants, in secret. And as to whether he has given the residents of Baltimore any reason to trust him, we need only look, again, at the fact that this surveillance system was deployed for almost a year in total secrecy, including from every other participant in the criminal justice system, and every elected official in Baltimore.

But even worse than that, Mr. McNutt has repeatedly misreprented what he is doing. His website has long claimed "We keep our imagery data for 45 days unless there are ongoing investigations or prosecutions associated with the data. In the case where there are investigations and prosecutions, the data is removed from our active server and stored on disk drives in classified safes to protect it and save it as evidence." https://www.baltimorecsp.com/faq-s. This turns out to be a blatant falsehood, as the BPD acknowledged in response to a public information request from the Office of the Public Defender, and as Mr. McNutt acknowledged to the Police Foundation in their "review" of the surveillance in Baltimore. Mr. McNutt kept every second of the footage he recorded in Baltimore, long after the 45 day period had expired. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/baltimore-aerial-surveillance-program-retained.

Mr. McNutt has repeatedly claimed that the ACLU has praised his privacy policies, when we have done nothing of the kind, and in fact have consistently criticized this technology as Big Brother come to life. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/baltimore-aerial-surveillance-program-retained. And he has claimed that he has asked the ACLU of Maryland to act in an oversight role regarding the use of this

technology, which is also a complete (and inexplicable) fabrication.

Mr. McNutt has also attempted to sell his services by making wild claims about the potential for reducing crime, suggesting that it will reduce homicides and shootings by one third. But he has no empirical data to back up these claims, and the promises are not worth the paper they are printed on. The data shows that during the time that the plane was secretly operating, the City experienced approximately 100 murders. The surveillance provided evidence related to only five of those, of which one was later ruled a suicide, the charges were dismissed against the suspect charged in one, and one resulted in a guilty plea, though it is not clear that the surveillance played any role.

Mr. McNutt has also been attempting to persuade community groups in Baltimore that the persistent aerial surveillance of the entire City population will somehow help address the problem of police misconduct in Baltimore. But of course, the location of the police officer (which is the only thing the persistent aerial surveillance can show) is hardly ever the key fact to be determined in evaluating a claim of police misconduct, and the advent of police body worn cameras makes it even less likely to be in question. The idea that we will meaningfully address the very real problem of police misconduct in Baltimore by putting the entire Baltimore citizenry under permanent video surveillance is beyond absurd. It is akin to turning over the keys to your house to the person who just robbed it.

Every other jurisdiction where the use or proposed use of this technology has become public has soundly rejected it. We hope that the Public Safety Committee, and the whole City Council, will unequivocally make clear to Mayor Pugh and Mr. McNutt that this technology is not welcome, and has no place, in Baltimore.