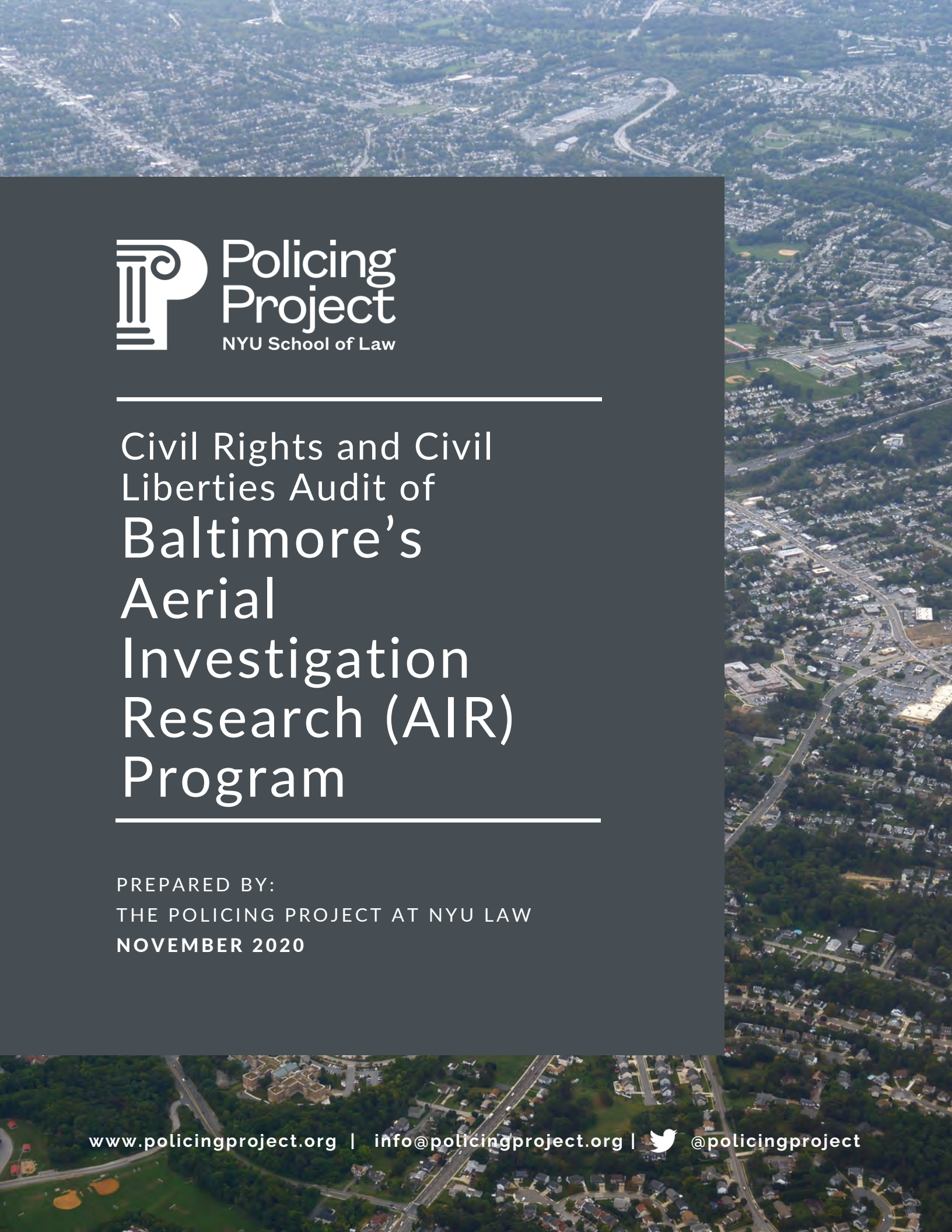

Policing Project
NYU School of Law

Civil Rights and Civil Liberties Audit of Baltimore's Aerial Investigation Research (AIR) Program

PREPARED BY:
THE POLICING PROJECT AT NYU LAW
NOVEMBER 2020

www.policingproject.org | info@policingproject.org | @policingproject

About the Policing Project at NYU Law

The Policing Project at New York University School of Law partners with communities and police to promote public safety through transparency, equity, and democratic engagement. Our work focuses on front-end, or democratic, accountability—meaning the public has a voice in setting transparent, ethical, and effective policing policies and practices before the police or government act. Our goal is to achieve public safety in a manner that is equitable, non-discriminatory, and respectful of public values.

For more information, visit www.PolicingProject.org.

This report was written by Policing Project Founder and Faculty Director Barry Friedman, Executive Director Farhang Heydari, Technology Fellow Emmanuel Mauleón, and Legal Fellow Max Isaacs.

TABLE OF CONTENTS

Executive Summary

On May 1, 2020, the Baltimore Police Department ("BPD") began a pilot of the Aerial Investigation Research ("AIR") Program, a novel investigative effort that combines aerial surveillance planes, ground surveillance technologies, and human analysts. BPD's partner in this endeavor is Persistent Surveillance Systems ("PSS"), a private company operating in Baltimore under the name "Community Support Program." PSS operates planes flying over Baltimore during daylight hours. These planes take photos of the city, which human analysts combine with information from ground surveillance devices, such as Baltimore's public CitiWatch cameras and license plate readers, to identify and track individuals and vehicles BPD believes are involved in serious crime.

This is not the first time that PSS's aerial surveillance planes have flown over Baltimore. In 2016, BPD implemented a similar program. When the existence of the program was revealed by the press, there was public backlash, and the program was discontinued.

This time around, BPD made public in advance its plans to run a pilot of the AIR Program. The program was funded by private philanthropy for a six-month trial period. Prior to commencement of the trial, BPD entered into a **Memorandum of Understanding** ("MOU") with PSS outlining the terms of the program. Under the terms of the MOU, BPD and PSS agreed to allow a number of independent evaluators access to the Program. The RAND Corporation is assessing the program's impact on addressing crime; the University of Baltimore's Schaefer Center is conducting a community survey; Morgan State University School of Social Work is conducting community focus groups and a quantitative analysis of AIR's impact.

Our organization, the **Policing Project at New York University School of Law**, was asked to perform an audit of any civil rights or civil liberties issues raised by the AIR Program. This is our report.

The report has four main parts:

Part I provides a bit of context for this audit—how we came to be involved, and the scope of our efforts. It acknowledges, as anyone must, that Baltimore suffers from very serious issues of crime and violence, and that concern for public safety requires addressing these issues. We are not the entity evaluating AIR's ability to address crime and violence, but recognize that is its purpose.

Part II lays out our understanding of how the AIR Program is operating in Baltimore. Although some of this information is public already, some of it is not. Particularly because AIR has been the subject of great controversy—including a federal lawsuit—we do our best to provide a full and objective accounting of precisely how it operates, and what it can and cannot do. The primary takeaways from Part II are:

- AIR is not just an aerial mapping technology, as many seem to conceive of it: rather, AIR is an *integrated* program of aerial overflights, ground-level surveillance devices, and PSS analysts. The MOU makes this clear, and without this integration, AIR's value would be limited considerably.

- Through this combination of technologies, AIR does precisely what it was meant to do, which is to track and identify individuals. The work is laborious, and tracking is not perfect. Still, as best we can

tell PSS never has lacked for capacity to do the work BPD has asked. Analysts can also track someone only to lose that track because of cloud cover or traffic. Analysts are able to follow the tracks of individuals and vehicles, and identify where they stop. One of the greatest values to AIR is that it can indicate precisely when an individual or vehicle being tracked passed a ground-level license plate reader or camera, so that the integrated system can capture images, confirming who was at that location and at what time. (We leave to the RAND evaluation the question of whether this sort of tracking actually furthers BPD's ability to fight crime.)

- The combination of aerial and ground technologies allows AIR to track individuals or vehicles over multiple days. The planes do not fly at night, so there are gaps, but PSS is fully capable of picking up a track the next day. In this report we describe multi-day tracks performed by PSS.

- For the most part, the AIR Program has stuck to the terms of its MOU, but there is one notable exception. The MOU states that "Tracks of individuals to and from crime scenes form the basis of the analysis." MOU at 23. This also is what the public and the federal courts were told. However, AIR is being used for other purposes as well. BPD and PSS refer to these as "Supplemental Requests." Although to the best of our knowledge these are tied to target crimes, as defined by the MOU, they include investigative actions that go beyond tracking "to and from" a crime scene. Supplemental Requests include actions such as watching the house of a person related to a person of interest, to see who comes and goes, and following the movements of a vehicle over the course of multiple days.

- Although the MOU sets the retention period of data by PSS at 45 days, because of a combination of technological issues and policy choices by BPD and PSS, a substantial majority of AIR's aerial imagery data has been (and apparently will be) retained indefinitely. This is a sharp departure from public understanding of the program.

Part III is an assessment of the AIR Program's impact on civil rights and civil liberties. In this Part, we discuss a wide range of such issues, from AIR's impact on privacy, to racial disparities, to concerns about mission creep. We also discuss the **recent decision** by the United States Court of Appeals for the Fourth Circuit ("the Fourth Circuit") holding that the AIR Program is constitutional. Some of the highlights of Part III include:

- The Fourth Circuit's recent decision relied upon a number of incorrect factual assumptions about how AIR operates, not the least of which was its unawareness of Supplemental Requests.

- Many in the public seem to perceive of AIR as a program involving only low-resolution aerial images. AIR is, in operation and by the terms of the MOU, a system that *integrates* aerial surveillance, ground-based surveillance technologies, and human analysis, to track individuals and identify them. That is precisely what it does, and it could not do it without the integration. It is a mistake to think of AIR as anything other than an integrated system of data collection and surveillance.

- Any analysis of the impact of AIR on civil rights and civil liberties must reach beyond what the Constitution says. Constitutional law provides a floor to what government may do but does not purport to provide standards for what government should be permitted to do. In addition, as we explain, there are significant gaps in constitutional law when it comes to emerging surveillance technologies such as AIR. For these reasons, the Constitution provides a starting point for our analysis, but we do not stop there.

- The AIR program has the potential to infringe on individuals' privacy—what we prefer to refer to as their "security" from the government—by subjecting them to tracking of their movements and whereabouts. This sort of tracking, if it is to be permitted at all, requires greater external checks than those imposed under the current MOU.

- An even greater potential threat to civil liberties is that AIR collects data on countless Baltimoreans daily, the vast majority of whom have done nothing wrong. This data is then held in a way that makes it accessible to the government whenever officials wish to examine it. This threat exists not just for the aerial images collected by PSS's planes, but for the wide range of surveillance devices maintained by BPD. This data is readily available to police, with what we conclude are inadequate external controls.

- AIR presents a number of other potential threats to civil liberties, including the possibility of mission creep.

- Programs of mass surveillance often present a risk of contributing to racial and socioeconomic disparities, and AIR is no exception. Decisions about whom to track and where to deploy AIR could contribute to such disparities, a point which warrants serious consideration — especially in light of the historically fraught relationship between BPD and the Black community.

Part IV turns to what we see as AIR's greatest shortcoming—that is has been deployed without robust democratic approval and oversight. Although much attention has been paid to whether the people of Baltimore support or oppose AIR, the only formal voice they were given was the Baltimore Board of Estimates' up or down approval of the MOU drafted by BPD and PSS.

In our view, any program of surveillance like AIR should be approved by a representative body with the power to adopt an appropriate regulatory framework.

- Democratic approval should not be an up or down vote. Sound evaluation of the use of a technology like AIR should take account of the relative costs and benefits and involve consideration of whether there is a regulatory framework that can return the benefits while mitigating costs to an acceptable level.

- Under current Maryland law, the people of Baltimore do not have the ability to provide appropriate democratic consideration of a program like AIR because, for historical reasons that are no longer germane, the legislature of the State of Maryland, rather than the City Council of Baltimore, retains control over BPD.

- The Maryland State Legislature should reconsider the extent of its control over Baltimore's police department. At the least, it should return democratic control over surveillance technologies like AIR to the Baltimore City Council. That body should have the ability to determine any future use of the AIR program, including what regulatory restrictions to require should the program be approved.

Finally, **Part V** puts forth a set of recommendations and considerations relevant to any jurisdiction considering the AIR Program, ideally via regulation by a democratically representative body. Our goal is not to suggest that any particular jurisdiction should or should not adopt AIR—that is precisely the question for democratic consideration—but to think through ways that *if* it does adopt a program like AIR, it can minimize some of the civil rights and civil liberties issues identified in this report. These recommendations represent our view of best practices for any powerful surveillance program like AIR. Our key recommendations include:

1. Clearly demarcate the AIR Program's capabilities and integrations at the outset and require notice and formal approval before expanding them.
2. Require policing agencies to draft a use policy and make it public before beginning operations.
3. Specify the offenses that may be investigated via the AIR program, so as to avoid any mission creep.
4. Require transparency and empirical justification for decisions about where the AIR Program operates.
5. Require and document an adequate factual predicate for any investigation before permitting access to AIR Program data. In some instances, this should involve judicial approval.
6. Specify rules regarding the tracking and identification of victims, witnesses, and associates.
7. Implement additional protections around First Amendment activities.
8. Provide specific and clear guidance around data retention.
9. Specify data security and data access procedures.
10. Study and minimize noise impact.
11. Enable and provide appropriate discovery to defense counsel.
12. Include ongoing reporting and assessment requirements.
13. Apply strict auditing procedures.
14. Specify consequences for violations of these principles.

In making these recommendations, we do not mean to judge the value of AIR. We both lack the information from RAND as to AIR's efficacy, and—more importantly—we do not speak for the people of Baltimore, especially communities of color particularly impacted by both violence and policing. These voices, along with the City's leadership—including at the Baltimore Police Department—must be the ones ultimately to weigh in on the right balance between surveillance and public safety. Our hope is that this report can help Baltimore, and any other jurisdiction considering AIR, come to a fully informed decision as to whether to use AIR, and how to regulate it if so.

I. Background and Our Civil Rights & Civil Liberties Audit

Baltimore is a vibrant city whose residents are invested deeply in their communities. Still, it is no secret that Baltimore has struggled for years with serious crime and violence. Urban crime has declined across much of America, but crime and violence in Baltimore persist at high levels.[1]

The year 2015 proved particularly difficult. In April, in response to the killing of Freddie Gray, the city saw sustained protests. That same year there also was a sharp spike in homicide and gun violence, and a drop in clearance rates of homicides.[2]

The following year, in part as a response to this sustained spike in crime, BPD launched its first partnership with PSS, flying aerial surveillance flights over Baltimore. Public approval was not sought, nor was the public even aware of the program until it was reported in the news media. In August 2016, a *Bloomberg* report disclosed that PSS was operating the planes over Baltimore.[3] The day after the *Bloomberg* story, BPD acknowledged that PSS planes had conducted 300 hours of surveillance in the first eight months of 2016. BPD and then-interim Police Commissioner Kevin Davis likened the technology to a "mobile CitiWatch camera."[4] Davis promised a "robust and inclusive community conversation" should the BPD decide to use PSS's services permanently.[5] Then-Mayor Stephanie Rawlings-Blake released a statement the day after the *Bloomberg* story's publication, indicating she was "recently made aware" of the program but supported it.[6] Nonetheless, public backlash led to BPD ending the program.

Over the next few years, Baltimore struggled with both crime and police accountability. In 2016, the United States Department of Justice issued a comprehensive report that "condemned many long-standing discriminatory enforcement practices by Baltimore police that allowed for illegal searches, arrests and stops of African Americans for minor offenses."[7] The following year, a federal district court approved a consent decree dealing with an array of negotiated changes to BPD practices—an order that remains in place today.[8] In just over a year, BPD cycled through four Police Commissioners, with Commissioner Michael Harrison taking the helm in March 2019. At the same time, violence in Baltimore remained high, with homicides staying near 2015 levels.[9]

---

[1] *See* U.S. DEP'T OF JUST., INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 14 (2016), https://www.justice.gov/opa/file/883366/download.

[2] *See* Jess Bidgood, *The Numbers Behind Baltimore's Record Year in Homicides*, N.Y. TIMES (Jan. 15, 2016), https://www.nytimes.com/interactive/2016/01/14/us/Baltimore-homicides-record.html.

[3] *See* Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance.

[4] *See* Kevin Rector, *Baltimore's Aerial Surveillance Program Goes Way Beyond Citiwatch, Experts Say*, BALT. SUN (Aug. 25, 2016), https://www.baltimoresun.com/news/crime/bs-md-ci-surveillance-differences-20160825-story.html; @BaltimorePolice, TWITTER (Aug. 24, 2016, 9:50 PM), https://twitter.com/BaltimorePolice/status/768626533791563776 (statement of Commissioner Kevin Davis).

[5] *See* @BaltimorePolice, *supra* note 4.

[6] *See Baltimore Police Respond to Report of Secret Aerial Surveillance Program*, CBS BALT. (Aug. 24, 2016), https://baltimore.cbslocal.com/2016/08/24/baltimore-police-respond-to-report-of-secret-aerial-surveillance-program.

[7] Lynh Bui & Peter Hermann, *Baltimore Officials, Justice Department Promise Sweeping Overhaul of City Police*, WASH. POST (Aug. 10, 2016), https://www.washingtonpost.com/local/public-safety/baltimore-officials-justice-department-promises-sweeping-overhaul-of-city-police/2016/08/10/f022ded2-5e72-11e6-8e45-477372e89d78_story.html.

[8] *See City of Baltimore Consent Decree*, CITY OF BALT., https://consentdecree.baltimorecity.gov (last visited Oct. 30, 2020).

[9] *See Baltimore Homicides*, BALT. SUN, https://homicides.news.baltimoresun.com (last visited Oct. 29, 2020).

In December 2019, Commissioner Harrison announced that BPD was seeking to bring back the AIR program, for a six-month pilot. The program was approved by the Baltimore Board of Estimates ("BOE") on April 1, 2020 and began operations on May 1, 2020. Flight operations ended on October 31, 2020. The pilot was supported primarily by funds from Arnold Ventures, a private philanthropic entity whose mission is "to invest in evidence-based solutions that maximize opportunity and minimize injustice."[10] The Abell Foundation provided funding for an independent auditor and Morgan State University's evaluation of the program.

Arnold Ventures and BPD jointly required that the AIR program be subjected to independent evaluation. The Schaefer Center for Public Policy at the University of Baltimore conducted community surveys to better understand how Baltimore residents perceive the technology and BPD. Morgan State University is conducting community focus groups and a quantitative analysis of AIR's impact. The RAND Corporation is studying the efficacy of the program, including the usefulness of the technology to police investigators, and its effect on crime rates, clearance rates, and prosecutions. The Policing Project at New York University agreed to evaluate any civil rights, civil liberties, and racial justice issues raised by the AIR Program.[11]

The Policing Project partners with communities and police to assure policing is equitable, transparent, and democratically accountable. Insofar as policing technologies are concerned, the Policing Project's position is that they should be adopted in democratically responsive ways, there should be assurance that the benefits of using the technology outweighs any costs, and policies should be in place to mitigate any costs. The Policing Project works with community members, technology vendors, and policing agencies to ensure that the use of policing technology is consistent with the requirements of civil rights and liberties, and racial justice.[12]

In the course of its work, the Policing Project has developed an evaluative framework for policing technologies, which can be found in **Appendix A**, and which guided our work here.

Our audit proceeded in three stages:

First, we gathered information. We reviewed documents and conducted interviews with BPD and PSS personnel to understand AIR's capabilities and operations. We also consulted with a number of community and civil rights leaders in Baltimore to understand better the concerns they might have about AIR, as well as the historical context in which the program was adopted. Finally, we attended community meetings regarding the program and participated in biweekly status calls with PSS, BPD, and research partners.

As with many current initiatives, the timeline and substance of this project has been impacted by the COVID-19 pandemic and resulting travel restrictions. Beginning in mid-March 2020, New York University, the institution within which we are housed, restricted non-essential employee travel, which kept us from being able to visit Baltimore. This limited our ability to conduct some of the anticipated portions of our audit, namely

---

[10] *See* Emily Opilo, *Privately Funded Surveillance Planes to Begin Patrolling Baltimore Skies*, WASH. POST (Apr. 2, 2020), https://www.washingtonpost.com/local/legal-issues/privately-funded-surveillance-planes-to-begin-patrolling-baltimore-skies/2020/04/02/92cd0daa-752c-11ea-a9bd-9f8b593300d0_story.html; *About*, ARNOLD VENTURES, www.arnoldventures.org/about (last visited Oct. 30, 2020).

[11] The Policing Project receives funding from a range of sources, including individual donors, corporations, and philanthropic foundations. Prior to our involvement in this project, we had received support from Arnold Ventures to expand our work on cost-benefit analysis in public safety. *See Applying CBA to Public Safety*, POLICING PROJECT, https://www.policingproject.org/cba-rps.

[12] The Policing Project has, among other things, conducted a number of civil rights and civil liberties audits of policing technologies, including a privacy audit of ShotSpotter's gunshot detection system, facilitating the research and public reports of the Axon AI and Policing Technology Ethics Board, and many more forthcoming audits. *See Responsible Use of Policing Technology*, POLICING PROJECT, https://www.policingproject.org/policing-tech-landing.

on-site review of AIR operations. We adjusted by holding frequent video conferences, calls, and other workarounds to substitute for in-person review. Although our preference would have been to conduct several aspects of this audit in person, we are confident that we have performed a thorough and thoughtful review of AIR and its components and understand its operation.

Next, we prepared a draft report summarizing our findings. Our draft report included both our findings about how AIR operates, as well as a set of recommendations for what the State of Maryland, the City of Baltimore, BPD, and PSS should do to minimize the civil rights and civil liberties impact of AIR. We requested PSS and BPD identify any factual misstatements or omissions in our report. PSS and BPD were both very helpful in ensuring our factual description was correct.

This report is our final step. It documents our understanding of how AIR works, its impact on civil rights and civil liberties, and contains our recommendations for minimizing these impacts.

II. How the AIR Program Works

A. Overview of the AIR Program

AIR is a surveillance program that incorporates aerial photography, ground surveillance tools, and human analysts. The integration of these three—they necessarily work in combination, as clearly contemplated in the AIR MOU—allows AIR analysts to track individuals and vehicles of interest and to provide information that leads to identifying individuals.

AIR's connective tissue is aerial imagery from planes operated by PSS. PSS's planes are equipped with powerful cameras that take photographs capturing much of the city. The planes take one photo every second, which PSS's software stiches together to create a second-by-second "map" of the activity below. Because the cameras are set to capture a wide area, images, once zoomed in, have low definition: cars appear as several pixels, and individuals as one to a few pixels. Although with this limited definition analysts can sometimes determine general information about a vehicle, such as its color, they cannot see something as specific as a license plate number, and they cannot identify individuals from the air.

What the AIR maps do make possible is tracking the movement of a person or vehicles across the city. Because the resolution is relatively low, the use of information from ground-based surveillance technologies—such as red-light cameras, automated license plate readers (ALPRs), and CitiWatch cameras—both assist in tracking and are critical to helping analysts find identifying information about a specific car or individual. This is why the aerial, ground-based, and human resources should be thought of as one composite system. Without the use of ground-based surveillance devices, the aerial imagery is of far lesser value to BPD.

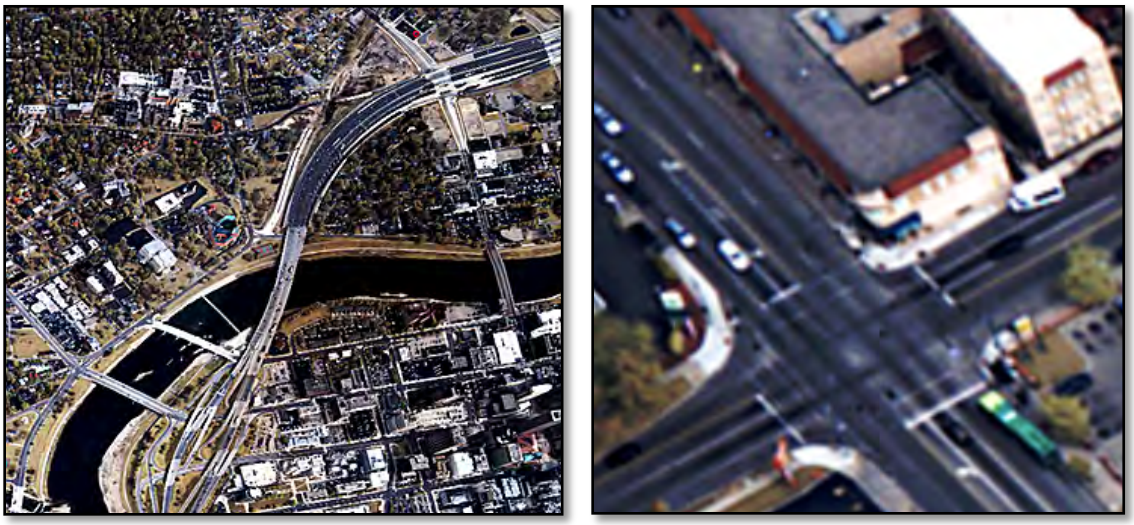

Fig. 1: A small portion of an aerial surveillance image, and a zoomed in portion of the same image

Prior to the announcement of the AIR pilot, PSS described three uses of the technology. First, as a tool to help solve and deter crime. Second, as a tool to support criminal defendants, by providing aerial imagery and other evidence to defense attorneys. Third, as a tool of police oversight, by helping with investigations of alleged misconduct or disproving an officer's account of events.

During this six-month pilot period, AIR only has been used for the first of these purposes. PSS has reached out to defense organizations (*e.g.*, public defenders and bar organizations) to provide information about AIR, but as of the release of this report there have been no defense requests for AIR imagery from the 2020 pilot (although PSS has provided support to defense counsel based on 2016 imagery). To date, we likewise have seen no evidence that AIR has been used to investigate police misconduct during the 2020 pilot.[13]

The primary anticipated use of AIR at the outset of the pilot was to identify individuals who were present at crime scenes, but it also has been used for a number of other purposes, which BPD and PSS refer to as "Supplemental Requests." We discuss the specifics of how AIR works, and the nature of these Supplemental Requests, in the sections that follow.

B. Rules of the AIR Program, and Adherence to those Rules

This section outlines some of the MOU's more important rules regarding utilization, and indicates whether (to the best of our knowledge) there has been compliance.

The basic rules regarding use of AIR during this pilot are outlined in the a MOU between BPD and PSS. That MOU was approved by the Baltimore Board of Estimates on April 1, 2020. Those rules apply only to imagery captured during the six-month test period.

No Night Flights: Although it technically is able to do so, PSS is prohibited from flying at night. To the best of our knowledge, PSS planes have flown only during daylight.

Coverage of City: PSS was to fly three planes, for a minimum of 40 hours per week, enabling it to cover substantial areas of the City of Baltimore. In particular, PSS planes were to fly in four predefined orbits over the city, covering areas in which 92% of the previous year's murders had occurred.[14] For most of the pilot, however, PSS had only 1 or 2 planes, thus requiring PSS and BPD to choose where to fly their planes. Over the first five months of the pilot, 99% of the flights were in the West and East orbits over the city; though these orbits were expanded early in the pilot period to cover more ground. All of the orbits are depicted in *Figure 2* on the following page.

[13] The 2016 program may have captured imagery of police misconduct. Some supporters of AIR contend that this imagery led to a criminal defendant's exoneration, but this has not been confirmed. *See* note 45, *infra*.

[14] At times, PSS and BPD have made statements indicating that AIR would achieve 90% coverage of Baltimore. Such statements, even if inadvertent, may have suggested that AIR would cover substantially all of the city, and not primarily focus on specific areas such as East and West Baltimore.

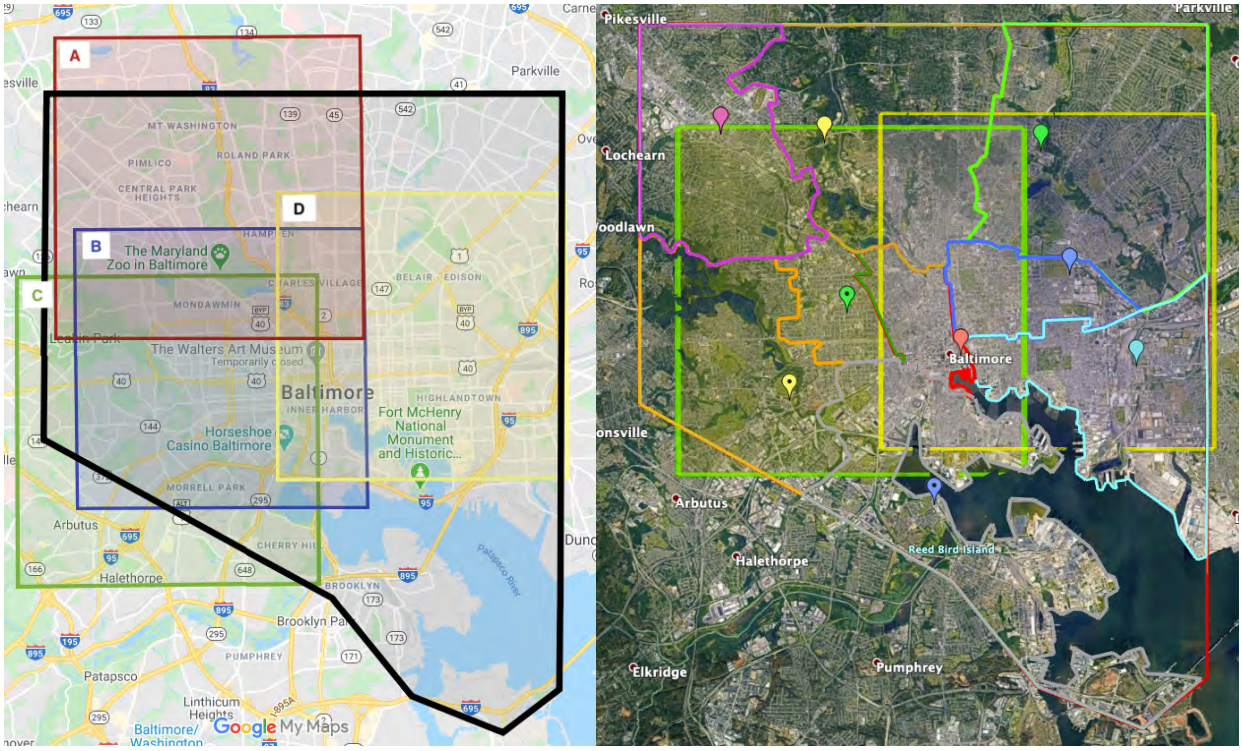

Fig. 2 – Maps of AIR coverage. PSS initially planned on flying four orbits (left). The colored boxes indicate the coverage of each orbit — North (A), West (B), South (C), and East (D). However, virtually all AIR flights used the East and West orbits. During the course of the pilot, PSS increased the coverage area of these two orbits from 32 to 45 square miles (right).

Limitations on Categories of Crimes: Absent written approval by the BPD Commissioner, PSS is restricted to assisting with investigations of homicides and attempted murders, shootings with injuries, armed robberies, and car-jackings. The Commissioner has not authorized any investigations beyond the enumerated target crimes, and PSS's focus has been only on target crimes. This does not mean, however, that everyone tracked is suspected of having committed a target crime. As discussed in more detail below, AIR has been used to track individuals not suspected of any wrongdoing, such as possible victims or witnesses. In addition, in executing the "Supplemental Requests," which we also discuss below, individuals have been tracked who had contact with those suspected of having committed a target crime.

Limitations on Types of Investigations: The MOU outlines the types of investigations that AIR will pursue, although the MOU is less clear on this point than on categories of crimes. The MOU includes a "Scope of Services" that PSS is permitted and required to provide during the six-month pilot period. *See* MOU at 18-24. Those services repeatedly are described as observing crime scenes and tracking individuals to and from those crime scenes.[15] The MOU's section on the "Privacy Protection Program" explicitly states that "[t]racks of individuals to and from crime scenes form the basis of the analysis." *Id.* at 23. This crime-scene limitation also is reflected in public statements made by PSS representatives in community meetings, and in the federal court proceedings regarding the constitutionality of AIR.[16]

---

[15] *See* MOU at 1 ("Individuals and vehicles are unidentifiable but are shown as a single dot and/or movement that can be tracked *from a crime scene*"); *id.* at 21 ("Contractor data is transmitted from the aircraft to Contractor's ground to station where Contractor analysts use imagery data *to locate crimes*, track individuals and vehicles *from a crime scene* and *extract information* to assist BPD in the investigation of Target Crimes").

[16] *See* Decl. of Ross T. McNutt at 2, *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, No. RDB-20-0929 (D. Md. Apr. 15, 2020), ECF No. 30-1 ("Both vehicles and people are tracked *from a reported crime scene* forwards and backwards in time" (emphasis added)); *id.* at 3 ("Analysts will examine the images and 'tag' vehicles or individuals that *were at or near the crime scene at or near the time of the crime*. Analysts will then

During the course of the pilot, however, BPD concluded—with the approval of its lawyers—that it could request PSS engage in an additional category of investigations. These investigations make use of AIR even when aerial imagery does not capture a crime scene (for example, because the crime occurred at night), and therefore it would be impossible to track individuals or vehicles to and from the crime scene. BPD and PSS refer to these requests as "Supplemental Requests"—a term that is not found in the MOU. Although these investigative requests still relate to a target crime, this additional category of investigations goes beyond tracking an individual or vehicle to and from a crime scene. Supplemental Requests have included a wide range of tracking and identification—from watching a particular house for a period of time in order to try and identify who comes and goes, to trying to find the location of a particular vehicle of interest within the City of Baltimore based on fixed location information provided by BPD (such as from a match from an ALPR). Supplemental Requests also can include the tracking of individuals over a number of days. In one case in particular, AIR was used to track a vehicle over 3 days and document 11 locations where the vehicle stopped. *See* Page 16, *infra*.

We do not believe a fair reading of the MOU permits for Supplemental Requests, although we acknowledge some ambiguity. For example, in a section requiring that PSS provide certain investigative reports within a fixed time period, the MOU refers to PSS producing reports that "include tracks of people and vehicles that met with people who were tracked from the crime scene." MOU at 21. But the natural reading of this section still requires that PSS begin its investigation by tracking someone to or from *a crime scene*—something that, by definition, is not the case with Supplemental Requests. Any other interpretation of this provision would strip the crime scene limitation of any meaning. In explaining this program to the public, and in arguing for its constitutionality in federal court, PSS, the city, and its lawyers all stressed the crime scene limitation.

The crime scene limitation is not an arbitrary one; it matters because it is a major constraint on BPD's discretion in conducting tracks of individuals and vehicles. When a track is requested by PSS to and from a crime scene, that request is "self-auditing," which is to say the fact that a crime occurred at a specific time and location guides the analysts' tracking, and the fact of that crime occurring easily can be verified. PSS conducts this type of investigation for all target crimes captured by its planes. But with a Supplemental Request, PSS analysts must rely on BPD's direction and discretion, including which locations to target and for what period of time. This makes them fundamentally different.

Although BPD has interpreted the MOU to allow Supplemental Requests, it has ensured those requests adhere to other explicit limitations within the MOU. During the pilot, the question arose whether BPD could use AIR to locate individuals with open warrants for target crimes. After some internal debate, BPD ultimately determined that this use went beyond the purposes listed in the MOU.

Limitation on Initiation: PSS analysts are not permitted to initiate investigations; only BPD personnel may do so. PSS would like to initiate investigations as soon as a call comes through to police dispatch, but to the best of our knowledge it has adhered to this limitation.

Limitation on Real Time Tracking: PSS is not permitted to provide "real-time support" except in exigent circumstances, upon written request of the Commissioner. *See* MOU at 21. We have seen examples of uses from 2016 that come quite close to real time. For example, requests that come in soon after a crime occurred

---

manually track the 'tagged' moving dots (which represent individuals and vehicles) *to and from the incident location*… These tracks of people *to and from the crime scene* generate leads for investigators to follow to identify potential suspects or witnesses to help solve crimes" (emphasis added)); *id.* at 4 ("Relatedly, the system is *not capable of monitoring a particular individual reliably over a period of multiple days*"; "PSS will provide BPD a more detailed report within 72 hours, which will include information regarding relevant ground-based cameras . . . *along the routes taken to or from the crime scene*") (emphasis added).

allow an analyst to track a person or vehicles movement up to the present (minus a three-second image capture, processing, and transmission delay). For the 2020 pilot, however, to the best of our knowledge PSS has not provided real-time tracking; the closest has been on a delay of a few hours.

Independent Auditor: Under the terms of the MOU, there was to be an independent auditor to ensure PSS's and BPD's compliance by with governing policies and to review PSS's internal operations. But funding for the auditor was not secured at the time AIR flights began. As a result, the work of that auditor did not begin until July. The auditor will report its findings to BPD directly. The MOU also required PSS to conduct internal reviews. *See* MOU at 23. PSS charged its corporate compliance officer with performing internal audits of data access and investigating internal complaints and violations of PSS's corporate policies. PSS's corporate compliance officer has conducted those internal audits and provided regular updates on its findings in weekly reports to BPD. Although PSS has identified some irregularities in data access, its internal investigations have concluded that these were the result of software malfunctions, defective keycards, or outdated procedures, and not of misconduct by analysts. The corporate compliance officer did not audit other aspects of compliance, including some we discuss here.

C. Tracking Based on Aerial Imagery

This Section provides additional detail about how AIR works in practice. More detail about PSS's planes and operations can be found in **Appendix C.**

Although PSS cameras are powerful enough to deliver high resolution images, , for technological reasons, there is a tradeoff between coverage and definition of objects at ground-level. PSS prioritizes a wide coverage area over high definition. PSS also believes it can address privacy concerns preemptively by programming a resolution limit into its software, thereby making it impossible to identify anyone from the air. This resolution limitation is built into the photograph—zooming cannot improve the resolution.

PSS's camera system is calibrated to have one pixel represent approximately 1.45 square feet on the ground, with some variation based on flight altitude. PSS and BPD generally describe the program's capabilities as "one pixel per person," and though this is not precisely correct, it is close enough. At the current level of resolution that PSS is using, most people appear as one to a few dimly colored pixels. Not only is it impossible to identify any individual from these photographs alone, but until a person moves, it can be difficult to distinguish them from an inanimate object such as a bush. The most one can see from these pixels alone is general coloration. For example, PSS analysts sometimes can tell if a person is wearing a lighter colored shirt as opposed to a dark shirt by comparing the color of the ground surrounding the pixel. They cannot discern a person's race.

Similarly, at the level of resolution PSS is using, vehicles are represented by approximately 15–20 pixels. This means that PSS analysts sometimes can determine a vehicle's general color, general body-type, the direction the vehicle is facing, and other distinguishing characteristics, such as a sunroof. Analysts often can distinguish law enforcement and other emergency response vehicles from the aerial imagery alone, either from their appearance or from the vehicle's behavior. Furthermore, based on the direction a vehicle is facing, analysts often can determine if a person enters or exits a driver or passenger side door.

Although aerial photographs, on their own, cannot be used to identify particular persons or vehicles, they can be used to track the movements of individuals and vehicles. Once PSS analysts have a person or vehicle of interest, the analysts can follow the target, creating a trail of movements around the city, called "tracks." This

manual tracking process is time-intensive—PSS represents that it takes at least 2 hours of analyst time to track an individual through 1 hour of AIR imagery. Although time intensive, during this pilot period PSS analysts have been able to fill all of BPD requests and perform all of the tracking required. This tracking process does not always work; in some cases, analysts simply are unable to create uninterrupted tracks of the movements of a person or vehicle.

Still, tracking the movements a person or vehicle can provide PSS analysts with a fair amount of information about the subject. For example, PSS analysts can observe what they believe to be significant subject behaviors, such as when an individual ran from the scene of a crime or entered the driver or passenger side of a vehicle that drives away quickly. They can note when vehicles swerved through traffic, ran stop signs or red lights, took wrong turns down one-way streets, took indirect routes or side streets, or exhibited other unusual driving behaviors. The sample tracks in the Figure below show examples of such information:

1	16:39:00	Coordinated driving begins
2	16:41:30	Pass incident location
3	16:42:50	Pull up together [redacted]
4	16:44:30	Arrive on [redacted]
5	16:49:12	Leave [redacted]
6	16:54:42	Parked on [redacted]
7	16:59:36	Leave [redacted]
8	17:05:02	Parked on [redacted]
9	17:13:58	Move up on [redacted]
10	17:21:07	**Incident Occurred** and vehicles depart
11	17:21:46	Erratic driving, passing cars, run red light
12	17:21:53	Split up

Fig. 3 – Two sample tracks with tracker notes from an AIR Program investigation.

From these observations, PSS analysts categorize and label the tracks they identify into the following categories:

- ***Primary*:** Individuals or vehicles that are suspected of being involved directly in the commission of a crime.
- ***Associate*:** Individuals or vehicles that interacted with primary tracks and that are suspected of being involved indirectly in the commission of a crime.
- ***Determined Not Involved*** ("DNI"): Tracks determined not to be involved in the commission of a crime.
- ***Undetermined*:** Tracks whose involvement cannot be determined.
- ***Witness*:** Tracks that could have been a witness to a crime.

Finally, PSS analysts can gain additional information by laying a track they have created atop a basic street level map using Google Earth. In this way, analysts can follow the track of a person or vehicle of interest to a particular address and inform BPD about the significance of those locations. For example, one PSS report determined that the target visited a shopping mall, a food market, and finally a gas station. In another investigation, an analyst noted that the target "[drove] to [a local] University," and flagged that "there are no classes going on currently." In certain circumstances, particularly with large buildings or complexes, PSS even may be able to note if a subject entered a particular door, walked through a courtyard, or parked in a particular parking spot. Such tracking can help with identification of the vehicle or person. Still, the value of aerial maps, standing alone, is somewhat limited.

D. Investigations Combining Aerial Imagery and Ground Surveillance Tools

AIR's aerial and ground-based components are mutually reinforcing. That is, the utility of aerial images is enhanced considerably with ground-level surveillance tools. Likewise, the aerial images allow BPD to maximize the value of existing ground-level surveillance technologies. Integrating these technologies makes it possible for BPD and PSS to identify the actual people being tracked, and to track their movements over time.

The most useful of these ground technologies is BPD's high-definition cameras, known as "CitiWatch cameras." Each of these cameras has a field of view spanning nearly two city blocks. The video resolution of these cameras is high enough to, on occasion, show a vehicle's license plate number, make, and model, or the face, clothing, or other identifying characteristics of an individual in the vehicle. PSS has direct access to CitiWatch footage—in one sample investigation we reviewed, one tracked subject passed by over 70 cameras as they moved through Baltimore—though they do not have the ability to pan or zoom in. PSS analysts select and share still images from these cameras with detectives.

Another ground technology that is quite useful to PSS analysts is information provided by automatic license plate readers, or ALPRs. ALPRs take pictures of vehicle license plates, geo-stamping them with time and location. Although PSS analysts do not have direct access to ALPRs, they use ALPRs in two ways: First, by collaborating with BPD detectives, analysts can track an unknown car to an ALPR and then the detective can use the ALPR to obtain the license plate number. Second, BPD detectives can search the ALPR database for a specific vehicle of interest, and use the geo-stamp to alert PSS analysts, who then can begin tracking that vehicle backward and forward in time from the ALPR.

In addition to CitiWatch cameras and ALPRs, PSS analysts are able to identify other cameras that may have footage of interest to BPD detectives. For example, if a track crosses paths with an MTA bus, analysts can suggest detectives obtain that bus footage. Analysts also can identify when tracks cross private businesses that analysts believe are likely to have cameras, such as gas stations or banks. Obtaining private imagery requires BPD detectives to do some legwork and is slower than the acquisition of city-owned images.

Part of the difficulty BPD faces with using ground surveillance tools on their own is figuring out exactly when and where a subject passed by such surveillance. The aerial aspect of AIR mitigates this problem. Aerial imagery provides a second-by-second account of a vehicle or individual's movements. PSS's specialized software then makes it easy for analysts to see exactly when a person or vehicle passes one of these ground-based surveillance

devices. This saves investigators countless hours of sifting through ground imagery. PSS analysts can direct BPD personnel to precisely the ground-level surveillance image they require.

This integration of aerial and ground-surveillance can be used in a number of ways.

First, it makes it far easier to identify an individual in a track that PSS is following. For example, once the aerial map identifies a subject crossing a ground device, PSS analysts can use the ground device to get a clear image of a license plate, which then can be cross referenced with DMV records. They also can obtain images of a person's face, which can then be shown to a witness or run through facial recognition software. In one investigation, analysts used an aerial image to track a suspect past a private store camera, pinpointing the exact time the suspect passed the camera. Detectives then were able to view the subject's face in that private camera footage, use facial-recognition software to identify the individual, and apprehend him.

Second, easier identification makes it possible for PSS to track persons and vehicles over multiple days. Although PSS's planes do not fly overnight, analysts can use ground surveillance to reidentify a person or vehicle on multiple days. For example, if PSS is tracking a vehicle on Day 1, they then can use ALPRs to find the vehicle again on Day 2 and continue tracking. That said, the ability to carry out a multi-day track can vary from case-to-case. If a car parks outside a home in the evening and does not move until the next morning, the reidentification and continuation of the tracking is relatively simple. Reidentification is also straightforward when a vehicle passes a nearby ALPR or CitiWatch camera. But in other cases, the reidentification process can require a fair amount of analyst work and is not guaranteed to succeed.

PSS also imposes its own limitation on multi-day tracks, in an effort to keep AIR within constitutional bounds. The Supreme Court has imposed a seven-day limitation on warrantless tracking of individuals using cell site information. To address concerns about whether that would pose constitutional problems for the use of AIR, PSS instructed its analysts to limit multi-day investigations to four days in length. PSS permits detectives to make multiple such requests in one investigation; we have not seen an example of this.

E. Supplemental Requests

Although the public was told that AIR would be used to track individuals and vehicles from crime scenes, and although in our view the best reading of the MOU includes this limitation, over the course of this pilot, BPD and PSS developed a category of AIR investigations not limited to such tracking, which were labeled "Supplemental Requests." *See* Page 10, *supra*. Supplemental Requests have been used to investigate crimes even when the original crime itself is not captured by AIR imagery, if BPD believes that AIR imagery of another location will assist with the investigation of a target crime.

Supplemental requests can take a variety of forms, including but not limited to the following:

- Monitoring one or more locations (not crime scenes) to determine if a suspect visits those locations, or to log vehicles coming or going from the location. The insert on the following page is an example of this type of information provided by PSS:

We were asked to survey the location XXXXX (event track) for any vehicles that may be arriving or leaving. The address belongs to the mother of the person of interest in relation to the shooting at location YYYYY on MM/DD/2020.

Primary Vehicle 2: Analyst started reviewing imagery from HH:MM:SS and went backwards, while tracking backwards the vehicle passed several ground cameras:

[TIME STAMP 1] – [CAMERA ADDRESS 1],
[TIME STAMP 2] – [CAMERA ADDRESS 2], and
[TIME STAMP 3] – [CAMERA ADDESS 3].

In another such investigation, analysts were asked to observe a residential location and identify all vehicles arriving or leaving. Analysts tracked three such vehicles, following them as they passed ground-based cameras, and provided that information to BPD. We also have seen an example of BPD requesting that PSS conduct location monitoring in order to build a list of "associates" of a person of interest, but have not seen PSS produce this type of output.

- Tracking a particular person or vehicle over multiple days, making note of where the subject traveled, locations where the person or vehicle stopped, and the subject's interactions with other individuals. For example, if BPD already has a particular suspect or person of interest, it can provide PSS with a license plate that it wants tracked. BPD can notify PSS when the vehicle crossed a license plate reader, thereby time and geo-locating that vehicle; then PSS can use AIR imagery to track that vehicle to its future and past locations. The insert below is an example of this type of information provided by PSS:

Analysts located Vehicle 1 in [PSS's software] iView, coordinating with ALPRs and Ground Cameras to verify Vehicle 1's identity. iView imagery was available on 7/17, 7/18, and 7/22. On 7/19 – 7/21, no iView imagery was available.

Vehicle 1 stops at several locations of interest multiple times on multiple days.

On 7 /17 Vehicle 1 stops at the following locations:

- *[STREET ADDRESS 1] at 11:48:00*
- *[STREET ADDRESS 2] at 11:55:31*
- *[STREET ADDRESS 3] at 13:39:03*
- *[STREET ADDRESS 4] at 13:40:46*

On 7 /18 Vehicle 1 stops at the following locations:

- *BP Gas Station at the corner of [STREET ADDRESS 5] at 10:28:40 and again at 15:46:13*
- *[STREET ADDRESS 6] at 10:37:57*
- *[STREET ADDRESS 7] at 10:41:18 and again at 11:35*
- *[STREET ADDRESS 8] at 10:59:07*

On 7 /22 a female is observed driving Vehicle 1. Vehicle 1 stops at the following locations:

- *[STREET ADDRESS 9] at 12:50:04*
- *Crown Gas Station, corner of [STREET ADDRESS 10] at 13:49:46*
- *[STREET ADDRESS 11] at 13:41:16.*

F. Information Sharing Between PSS & BPD

The MOU sets out a regularized process of information sharing between PSS and BPD. An AIR investigation begins with a request from a BPD detective. The detective provides information about the crime and clarifies the type of investigative support sought—be it identification, movement tracking, or some combination. The MOU requires that analysts compile preliminary briefs for BPD investigators within 18 hours of receiving a request. These briefs include the BPD request, aerial imagery, observable actions at the scene of the crime or other locations, all subject tracks, and the locations to which subjects were tracked. Within 72 hours, analysts provide BPD with a full investigative report which, in addition to the information included in the initial briefing, includes:

- Track files and designations for possible suspects, possible associates (individuals or vehicles that interacted with suspects and are suspected of being indirectly involved in the commission of a crime), and possible witnesses;
- Notes as to where targets stopped, and other significant behavior observed by the analysts;
- Images and video drawn from ground surveillance sources;
- Street-level images of the locations where the target started or stopped; and
- Narrative notes documenting overall findings.

These two briefing packets are required by the MOU, but PSS analysts and BPD detectives are also often in regular communication during the course of an AIR investigation. For example, it is common for detectives and analysts to communicate back and forth as an investigation proceeds, with detectives providing information to narrow down the analysts' search, and the analysts providing investigative leads.

At the close of an investigation, PSS transfers evidence to BPD via BPD's electronic evidence management system, Evidence.com. This evidence includes tracks created by PSS analysts and still images of tracked individuals and vehicles obtained during the investigations.

G. Data Retention

Under the MOU governing this pilot, PSS is required to delete aerial footage after 45 days, unless it is part of an ongoing investigation. In court filings BPD stressed that the "vast majority of the imagery…will be deleted" and "any imagery not identified as relevant to a criminal investigation and reduced to an evidentiary packet will be destroyed after 45 days."[17]

In practice, however, a substantial majority of the aerial imagery generated during the AIR pilot has been—and will be—retained.[18] This has occurred because so long as PSS initiates an investigation of a target crime on a particular day, PSS retains the entire day's AIR imagery, not just the relevant tracks PSS performed. PSS does so in part is because of a technological limitation—the current version of PSS's software does not allow it to retain reliably only part of an image, such as where tracks appear. But in part this is a policy choice—PSS prefers to retain the entire day's worth of data even if only a few hours are relevant to an investigation, because

[17] Defs Opp. to Expedited Hearing, Leaders of a Beautiful Struggle et al. v. Baltimore Police Dep't, No. 20-1495 at *3–4 (4th Cir. June 18, 2020); Defs Mem. in Support of Mot. to Dismiss, Leaders of a Beautiful Struggle et al. v. Baltimore Police Dep't, No. RDB-20-0929 at *3 (Dist. Md. Aug. 12, 2020).

[18] BPD and PSS did not delete any data for the first three months of the pilot, but later began regular deletion. Because of technical issues and detectives' unfamiliarity with the program, PSS did not receive requests for approximately 50-55% of AIR target crimes that occurred during the first three months of the program. Therefore, on July 20, 2020 BPD directed PSS to suspend its data deletion policy, and retain all data—whether or not it was older than 45 days—so that detectives would have time to complete request for target crimes that occurred since the start of the program. This pause was lifted at the end of August.

PSS feels that all the imagery might later be useful to the prosecution or the defense, should a criminal case result. These choices mean that on any day in which there is a request from BPD, and AIR has captured relevant imagery, the entire day's data is stored. Given the volume of cases BPD initiates, these policies mean all the imagery is kept for most days. And once imagery has been retained for use in one investigation, nothing prevents BPD from requesting that PSS use the imagery in another case.

As a point of reference, the official retention period for CitiWatch camera footage is 28 days, after which footage should automatically be deleted. *See* BPD Policy 1014 – Video Surveillance Procedures (Aug. 2016) at 1. In addition, the retention period for ALPRs is set by BPD policy at 18 months, although the statewide clearinghouse retains ALPR reads for 12 months. As with AIR, if any CitiWatch of ALPR data becomes potential evidence in a criminal case, it is retained longer.

H. Data Security

Because AIR investigations gather an array of sensitive personal and law enforcement information, data security is essential.

On paper, AIR employs relatively robust security measures. Data is stored on secure servers. BPD conducts background checks and clearance for all PSS employees. In theory, keycard access is required for each computer. PSS analysts may not have cellphones while operating the terminals and security cameras and software tools monitor analyst work. PSS has the ability to audit every action that analysts take when investigating AIR imagery, including what images they view and if they are looking anywhere outside of the area BPD has requested. User access logs are verified nightly Monday-to-Friday, and any issues are self-reported as part of PSS's weekly reports to BPD.

We cannot say, however, how robust these data security practices operated in practice. PSS conducted auditing of user access logs on its own, but BPD also hired an outside firm to independently review these logs—this review, which began in July but covered the entire pilot period, remains in progress and will touch on all aspects of PSS's internal operations.

III. Potential Civil Rights and Civil Liberties Issues with the AIR Program

We have been asked to address whether the AIR program is consistent with legal, ethical, and democratic norms. To do this we apply an evaluative framework that can be found in **Appendix A**. That framework is a straightforward application of benefit-cost analysis, tailored to the particular costs of using surveillance technologies in policing.

It is common in the public sphere for positions to be taken sharply for or against the use of particular policing technologies, when an all or nothing approach may not be the right answer. Too often policing agencies adopt technologies with the hope that the technology will help fight crime while failing to pay sufficient—or even any—attention to the social costs of using the technology. At the same time, those who oppose use of a technology often do not consider whether there are use policies or guardrails that could allow government to capture the benefits of a technology while minimizing costs to an acceptable level.

The proper approach, in our view, is to consider the use of technology in policing in three steps:

Step 1: Clearly define the problem(s) one seeks to solve by using the technology, and assess the benefits or potential benefits of a given technological approach.

Step 2: Identify the costs associated with the approach, including not only hard costs but also social costs, such as potential intrusions into personal privacy and security, and whether the costs will be distributed in racially disparate ways; and

Step 3: Determine *if* there is a regulatory framework—i.e., a set of legal requirements or internal guardrails governing use—that can eliminate or substantially mitigate the costs, so that the benefits can be obtained. (We emphasize *if* to leave open the possibility that the costs of a particular technology are so high, and cannot be mitigated sufficiently, that the particular use of the technology should be banned entirely. Even in this case, some uses may be permissible, and others not.)

In many ways, the current process around this iteration of the AIR Program embraced Steps 1 and 2 laudably. Independent research partners have been brought in to evaluate AIR, both with regard to its benefits and costs. This approach is markedly different than how most decisions to deploy advanced surveillance technologies are made, and ought to serve as a model for police deployment of emerging technologies more generally. Where this process could have been improved substantially was around Step 3, the regulatory framework.

Which brings us to a critical point—the importance of democratic approval before any powerful policing technology is deployed. We can, and will, offer our views of the relevant social costs involved with AIR, and will suggest regulatory means that could be adopted to minimize these costs. Ultimately, however, whether a program like AIR should be adopted is a decision for the people of Baltimore to make. The technology is being used for their benefit, and they are the ones who will bear any costs, particularly social costs. As we explain in Part IV, there is a quirk of Maryland law that may deprive Baltimoreans of this authority, placing it in the state legislature. We view that as nothing short of tragic, but our point remains: any decision about whether to

adopt powerful surveillance technology, including the guardrails on that technology if it is to be used, should rest in democratically accountable hands.

Before we turn to the benefits and costs of AIR, one final point about the role of race in this discussion. The debate in Baltimore about AIR is, as one might expect, heavily inflected with concerns about racial impact. Baltimore is a majority-Black city with a deeply troubled history regarding policing. The Baltimore Police Department currently is operating under a federal consent decree, which the city signed to address BPD's racially discriminatory practices. For that reason, any assessment of AIR must focus closely on issues of race. We do this toward the end of this Part, rather than at the outset, because the racial impact of AIR is, at least in part, the cumulation of all the other potential costs of AIR that also fall disproportionately on the Black population of Baltimore.

A. The Potential Benefits of AIR

All agree Baltimore suffers from a horrific crime problem, and particularly one of gun violence. Although BPD has tried to address the violence, those efforts have been unsuccessful, in part because of difficulties BPD faces in identifying those responsible.

What AIR promises to do is assist with identifying individuals responsible for specific violent crimes. It does so by allowing trained analysts to track individuals from the scene of crimes, enabling their identification. The tool allows investigators to generate leads when all they have to begin with is the location of a crime scene. AIR also is being used for additional uses beyond identification, such as tracking individuals' movements once identified, and connecting them with associates. As we explained above, some of these uses may reach beyond what the MOU permits. *See* Part II.E *supra* (discussing supplemental requests).

We cannot know if AIR delivers the benefits it promises. The efficacy of AIR is being assessed by the RAND Corporation, and until those results are public, the benefits remain speculative. The theory that AIR will assist in identifying individuals responsible for violence is a plausible one, particular when the investigation begins with a crime scene. What's more, AIR is less reliant on potentially problematic eyewitness statements or informant tips and allows much more efficient use of ground-based surveillance. But whether AIR proves to be useful—and how useful, for there are tradeoffs, as we document here—remains unknown at present. AIR's utility may depend upon variables such as the limits of the pilot program (*e.g.*, the ban on night flights) and the capacity of BPD to use the information from the AIR program effectively.[19]

It is worth nothing that BPD's difficulty in tackling violent crime may be in part because in Baltimore—as is the case in other American cities—the relationship between police and the community they serve is so fractured that there is no mutual cooperation and support in suppressing violence and making neighborhoods safe. To the extent this is true, unless AIR is operated in a manner fully cognizant of the associated costs, and with appropriate guardrails, it runs the risk of exacerbating the difficulties BPD faces, rather than helping with them.

[19] In this regard, we note that courts evaluating technologies like AIR under the Constitution often simply assume efficacy, without any evidence, which we view as a mistake. Government ought to bear a burden of establishing the value when its actions jeopardize individual rights.

B. Concerns About "Privacy" and Security

What is at Stake?

One of the primary concerns expressed about AIR is the implications of giving government license to photograph and monitor the public movements of people throughout much of Baltimore using the aerial and ground surveillance technologies that are integrated into AIR. Many frame this set of concerns as involving matters of "privacy."

The concern about privacy, as we understand it, is threefold.

First, AIR collects data *in bulk* about the movements of people in its range, the vast majority of whom have done nothing in particular deserving of the government's attention. Cameras on planes overhead capture these movements for *all* people present and mobile in the areas where AIR flies. And this data can be integrated with yet more data collected on people by ground cameras such as CitiWatch or automated license plate readers (ALPRs). Some portions of this data are retained for a long period of time.

Second, this data can be used to track the movement of people around the City of Baltimore. This sort of information can reveal the personal details of our private lives. In *Carpenter v. United State*s, a recent Supreme Court case involving tracking of movements using cell site location information, the Chief Justice explained that this sort of location information "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.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

Third, the decision about whom to track, and under what circumstances, is left to the unchecked discretion of law enforcement. It is true that there is an MOU in place limiting when AIR is supposed to be used, but there is no enforcement mechanism, and for much of this pilot there was no external auditing to ascertain whether the MOU was being followed. And, as we noted above, the Supplemental Requests arguably exceed the terms of the MOU, and certainly exceed what people understood as the intended use of AIR. Absent clear rules, an auditing mechanism, and consequences for violations, police discretion will remain unchecked, potentially subjecting any Baltimorean within the range of AIR to tracking. Guardrails exist not for what is supposed to happen, but for what might.

We prefer to think of the potential harm to liberty posed by these cumulative concerns as one of "security," rather than "privacy." Although privacy is important, and people value it, using that word minimizes the extent of the threat of mass monitoring of individuals by the government. The Fourth Amendment of the United States Constitution refers to the "right of the people to be *secure* . . . against unreasonable searches and seizures." People often think of the government, and the police in particular, as charged with keeping us secure, but what the Framers of the Constitution understood is that the government itself poses as great or greater a threat to the security of the people if it is not constrained properly. *See* THE FEDERALIST NO. 51 (James Madison) ("You must first enable the government to control the governed; and in the next place oblige it to control itself.").

Method of Analysis

In analyzing the question of the extent to which AIR poses a threat to the security or privacy of Baltimore residents, it is natural to look to the Constitution and constitutional law. As we just noted, the Fourth Amendment addresses these interests. And, in fact, contemporaneous with our review there has been ongoing litigation in federal court challenging the constitutionality of the AIR program on Fourth Amendment grounds. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the Plaintiffs argue that AIR violates the Fourth Amendment (and First Amendment) rights of the residents of Baltimore. The United States Court of Appeals for the Fourth Circuit—the federal appellate court that sits over the State of Maryland—recently **ruled** against the Plaintiffs' request for a preliminary injunction, permitting the AIR program to continue, pending further litigation.[20] The vote in the case was 2-1, with Chief Judge Roger Gregory arguing in dissent that the AIR program is unconstitutional. *See id.* at *23. In our view, the Fourth Circuit majority opinion was based on an incomplete understanding of how AIR operates. *See* **Appendix B** (detailing differences between our understanding of AIR and the Fourth Circuit majority opinion).

We will analyze the AIR program under the Constitution, but we also will look beyond it. There are four reasons for this, each of them critically important to our ultimate conclusions.

First, under our system of government, the Constitution is a floor below which the conduct of government may not fall, not a permission slip for what government may do. When courts decide something is unconstitutional, that thing is absolutely prohibited thereafter, making courts understandably reluctant to rule things off the table on constitutional grounds. But even if courts ultimately conclude that something is constitutional, a given tactic or technology still can present sufficiently serious risks to individual rights and racial equity that as a matter of policy the public may decide to ban it, or—as we have explained—regulate it carefully. Constitutional law and constitutional decisions do not purport to say anything about this. Decisions such as these are for the people and their elected representatives to make.

Second, the public cannot count on the Fourth Amendment to impose the sort of carefully crafted guardrails that may be needed for a program such as AIR. For example, if the tracking of individuals under AIR is a "search" under the Fourth Amendment, then it only can be used if the police obtain a warrant first. As we explain, warrants may make sense in some circumstances, but not in others. The Fourth Amendment is a blunt instrument; there may be better safeguards available. And as currently interpreted by courts, the Fourth Amendment says nothing about some critical aspects of regulating a technology, such as limits on data retention, or data security.

Third, Fourth Amendment law around emerging policing technology is very much in flux; there are large gaps as the law applies to surveillance technologies such as AIR. Those gaps exist because—as the Supreme Court itself has recognized—technology is advancing rapidly, and constitutional law has not been able to keep up. *See* Pages 23–24, *infra*.

Finally, existing Fourth Amendment law tends to focus on specific pieces and uses of technology rather than seeing them as an integrated whole. Whatever the precedents say about pieces of technology standing alone, it is impossible to consider the risk AIR poses to personal privacy and security without looking at what it actually is—an integrated system for collecting vast amounts of data on individuals and using it to track their movements using both aerial and ground-based technology.

---

[20] *See Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495, 979 F.3d 219, 2020 WL 6500931, at *10 (4th Cir. Nov. 5, 2020), *affirming* 456 F. Supp. 3d. 699, 719 (D. Md. 2020).

We ultimately conclude that if AIR is to be used, it should be democratically authorized under an enforceable set of strict guardrails that do not exist at present, and which courts, relying on current Fourth Amendment precedents, cannot replicate. To reach this conclusion, we start with the Fourth Amendment, but necessarily move beyond it.

Is AIR a "search" under the Fourth Amendment?

Under current Supreme Court precedent, the Fourth Amendment's protections against unreasonable searches are triggered only if the government's action is deemed to be a "search." A search occurs when the government action violates a person's "reasonable expectation of privacy." *Katz v. United States*, 389 U.S. 347, 360 (Harlan, J., concurring). Some traditional law enforcement actions, like a search of a person's clothing or their home, obviously violate one's reasonable expectation of privacy and therefore are considered searches.

But when it comes to government use of surveillance technologies, the rules regarding what constitutes a "search" for Fourth Amendment purposes are underdeveloped, and often point in conflicting directions.

There are *two* aspects to the AIR program that might be considered a search.

First, there is collection in bulk of data regarding the public movements of countless Baltimoreans who have done nothing wrong. AIR's nodes—aerial cameras, CCTV, license plate readers—capture the movements of everyone within dozens of square miles. The data then is retained (sometimes for long periods of time) for later access at BPD's behest.

Second, there is the actual tracking of the movements of particular individuals. The tracking abilities of the AIR program are not perfect. In addition to limits on when and where the planes fly, tracking and identification require time and effort, and depend on the track not being lost or confused with other tracks. Still, this sort of tracking is precisely what AIR was adopted to do and is what AIR analysts are doing. We have seen no evidence that AIR fails because of a shortage of labor.

We will take these in reverse order.

AIR tracking may be a Fourth Amendment search—and should be regulated in any event.

The Supreme Court never has encountered a *system* of surveillance like AIR, and so it is difficult to reach a firm conclusion as to whether the tracking of individuals by AIR is constitutional under those precedents.

The Supreme Court has decided a number of cases that permit aerial surveillance, but each of those involved one or two flights over a very particular piece of property, such as someone's backyard, to look for something specific. They do not involve the sort of ongoing overflights that are at issue in AIR, let alone the integration of technologies that make tracking by AIR effective. *See Florida v. Riley*, 488 U.S. 445, 448–49 (1989) (police circling a helicopter over defendant's property two times to identify the contents of a greenhouse); *California v. Ciraolo*, 476 U.S. 207, 209 (1986) (police flying over defendant's backyard to identify marijuana plants and take photographs "with a standard 35mm camera"); *Dow Chemical Co. v. United States*, 476 U.S. 227, 238 (1986) (federal agency taking aerial photographs of an industrial complex, revealing no "intimate details" of constitutional proportion nor utilizing "highly

sophisticated surveillance equipment"). Other than involving a vehicle in the air, these decisions are not particularly applicable—and for what it is worth, those decisions have been subjected to relentless criticism.[21]

The Supreme Court also has decided a number of cases about police use of technology to track an individual's public movements. *See United States v. Knotts*, 460 U.S. 276 (1983); *United States v. Jones*, 565 U.S. 400 (2012). The lesson from these cases is that short-term tracking—i.e., of a single trip—is acceptable, but long-term tracking is not. Compare *Knotts*, 460 U.S. at 281, 283, with *Jones*, 565 U.S. at 431 (Alito, J., concurring). Even those cases required police to identify a particular subject and track the subject forward in time; they did not involve a technology that constantly creates a historical record of everyone's movements, allowing them to be tracked retrospectively. *Cf. Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (stored location information "gives police access to a category of information otherwise unknowable," allowing the government to "travel back in time to retrace a person's whereabouts.")

The closest Supreme Court precedent to the AIR program is the *Carpenter* case, in which the Supreme Court decided that the government violated the Constitution by acquiring over seven days of cell site location information about a person from a cell service provider without a warrant or probable cause, for the purpose of tracking that individual's movements. *See id.* at 2217 n.3, 2219.

What does *Carpenter* say about AIR's constitutionality? This is a question that can be argued both ways.

On the one hand, there are ways in which cell-site location information is more powerful than AIR tracking: AIR's aerial surveillance does not operate at night (although it can track across multiple days); other technological or real world conditions may limit the ability of AIR to track movement effectively (although no one can "opt out" of this tracking, unlike a person who chooses not to carry a cell phone); and human analysis is required to trace movement through aerial imagery (although we have never seen this operate as a practical limit on AIR's function).

On the other hand, there are ways in which AIR potentially is more powerful than cell-site tracking.

First, AIR is not hampered by some of the technical limitations of cell-site tracking—the necessity of first determining a suspect's current cell phone number, and the need either to obtain location data from a service provider or to deploy a cell site simulator. Second, when available, AIR can allow analysts to track with great precision, perhaps even more so than CSLI. For example, AIR investigators can determine if a person entered the driver or passenger side of a vehicle; they can also determine if a person went into a particular location or remained outside the building. CSLI, although improving in accuracy, is generally not so fine-grained.[22] Finally, AIR allows investigators to gather at least as much associational information as with CSLI, and perhaps more. Investigators could determine who a person interacted with, where a vehicle traveled, or which people gathered at a particular location. In this respect, AIR—like the CSLI in *Carpenter*— potentially 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.'" *Carpenter*, 138 S. Ct. at 2217 (citation omitted).

---

[21] *See* Elizabeth Schutz, *The Fourth Amendment Rights of the Homeless*, 60 FORDHAM L. REV. 1003, 1014 n.96 (1992) (noting that the Court's overflight cases have been "widely criticized"); Laura L. Krakovec, *The Constitutionality of Warrantless Aerial Surveillance*, 77 J. CRIM. L. & CRIMINOLOGY 602 (1986) (cases evidence a "parsimonious view of constitutional protections").

[22] *See* Br. of Technology Experts as *Amici Curiae* in Supp. of Pet. at 18, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (CSLI can "pinpoint a phone's location to an accuracy of within 50 meters or less under many circumstances"); Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and the Need for Fourth Amendment Protections*, 106 J. CRIM. L. & CRIMINOLOGY 167, 176 (2016) (noting that technological advances could improve accuracy to "fewer than ten feet" in some cases).

In the end, the constitutionality under existing precedents of the tracking aspect of AIR mostly comes down to precisely how long someone is tracked, a point with which the Supreme Court justices are struggling. The judges concurring in *Jones* admitted they could not draw a clear line between "short-term" and "long-term" tracking. The seven-day limitation in *Carpenter* is wholly arbitrary, appearing nowhere in the Constitution.

There is a solution to the difficulty courts are having in drawing lines regarding emerging technologies such as AIR—democratic accountability. Rather than expecting the Fourth Amendment to be the sole source of guardrails on the government's use of surveillance technologies, legislative bodies can and should play a role in deciding whether the technology will be used, and, if so, drawing just the sort of lines the courts cannot—including by drafting a full set of guardrails, not just on how long tracking can occur but on much else. In the *Jones* case, Justice Alito—writing for four justices—made the point that for emerging technologies, the very best answer was legislative control in the first instance. "In circumstances involving dramatic technological change," Justice Alito observed, "the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Jones*, 565 U.S. at 429–30 (Alito, J., concurring) (citation omitted). On multiple occasions the State of Maryland has done exactly that. [23] In Parts IV and V, we recommend just this course.

Existing constitutional law has little to say about the bulk data collection aspects of AIR, which makes democratic oversight all the more essential.

AIR's collection and storage of data in bulk regarding the movements of all individuals within its range also might be considered a "search." The mass collection of imagery data, both aerial and ground, allows law enforcement to record the movements and associations of entirely innocent people, and permits tracking them if and when the police so choose. This collection is analogous to the creation of cell-site location data. As the Chief Justice described in *Carpenter*, it was the creation and storage of this sort of data that permitted the government to "travel back in time to retrace a person's whereabouts "…Only the few without cell phones could escape this tireless and absolute surveillance." *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018). In *Carpenter*, of course, the data was created and collected by private companies to provide cellular service; with AIR, the government is creating the data for the explicit purpose of using it for investigative purposes.

The Supreme Court has long recognized that a central aim of the Fourth Amendment is "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (2018) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Nearly fifty years ago, Justice Douglas cautioned that advances in technology one day could allow the government to spot "unorthodox or aberrational behavior across a wide spectrum." *United States v. White*, 401 U.S. 745, 757 (1971) (Douglas, J., dissenting). Predicting that the harms of such innovations would not be borne by criminal defendants alone, Justice Douglas forewarned that "every person is the victim, for the technology we exalt today is everyman's master." *Id.*

Justice Douglas's fear of a surveillance state was hardly a novel concern. Some scholars argue the Fourth Amendment was meant to address precisely such fears. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 98–99 (2013). The notion that pervasive government monitoring may warrant special consideration appears frequently in the Supreme Court's Fourth Amendment jurisprudence. *E.g.*, *Knotts*, 460 U.S. at 284 (suggesting that "dragnet type law enforcement practices" may be governed by "different constitutional principles"); *Jones*, 565 U.S. 416 (Sotomayor, J., concurring) (low-cost GPS monitoring, which enables police to surveil "any person . . . in [their] unfettered discretion," may "alter the relationship

[23] *See, e.g.*, MD. CODE § 3-701 (limiting use of certain intrusive investigative tactics with respect to First Amendment activities); MD. CODE CRIM. PROC. § 1-203.1 (requiring police obtain a warrant for real-time location tracking of devices such as cell phones).

between citizen and government in a way that is inimical to democratic society"); *Carpenter*, 138 S. Ct. at 2218 (expressing concern that, because CSLI is logged for all cell phones, the government's "newfound tracking capacity runs against everyone").

The federal courts have never ruled on the question of whether such mass data collection is permissible. One analogy to AIR's widespread data collection is the National Security Agency's bulk collection of telephone metadata, part of the "Snowden revelations" about government surveillance in the aftermath of the terrorist attacks of September 11, 2001. *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 821–25 (2d. Cir. 2015). Although the United States Court of Appeals for the Second Circuit ultimately held that Congress had not authorized that collection—a point that resonates with our main message here about democratic authorization, and therefore did not reach the plaintiffs' First and Fourth Amendment claims, the court noted that such widespread collection could raise serious constitutional concerns. *Id.* at 824.

But even if constitutional law has not yet addressed the bulk collection of data, that does not mean that from a policy matter this sort of collection should be left unchecked.

By setting rules around the *collection* of data—not just rules around use of that data for tracking—legislatures can do much to protect the security of their communities. Rules around data retention and access are a prime example of where this sort of regulation is needed. BPD and PSS ostensibly set a 45-day retention period for both the 2016 and the 2020 programs, a point on which the Fourth Circuit majority relied. But as we have explained, that supposed limit does not reflect what actually is happening. *All* the data from the 2016 pilot still remains in PSS's hands. At present, for any day that AIR is investigating a target crime, the full day's aerial images are retained. As a result, a substantial majority of the aerial imagery generated during the pilot will be retained indefinitely. And, unlike in a case such as *Carpenter*, that data in effect is being held by the government. It is true that formally the data rests in PSS's hands, not BPD's. But for all intents and purposes, PSS is BPD. In *Carpenter*, the judicial process (a subpoena) was used to obtain the cell site data; still, the Supreme Court concluded even that was not enough—a warrant based on probable cause was necessary. With AIR, there is no intermediary; BPD requests searches and PSS performs them.

Again, even if constitutional law has nothing to say at present about the bulk collection aspect of the AIR program (and we think considered constitutional guidance is needed), if AIR is to be used, there should be in place an effective set of guardrails to ensure against the obvious dangers of government overreach. At present, there are not.

Is AIR an "unreasonable" search under the Fourth Amendment? (Yet another argument for democratic guardrails.)

Under the Fourth Amendment, if something is a "search," the next question is whether it is "unreasonable." That depends on what kind of search it is. If the search is targeted at a person based on "suspicion" that they have done something wrong—like the tracking aspect of AIR—then it is impermissible without a warrant based on probable cause of wrongdoing. If it is a mass "suspicion-less" search—such as a drunk driving roadblock or airport security, or the data collection aspect of AIR—then the Supreme Court applies a balancing test that weighs the government interest against the intrusion into individual security.

The irony is that under both of these tests AIR would face serious constitutional obstacles, perhaps even stricter than we recommend in Part V.

Take the tracking. Should BPD need to get a warrant from a judge each time it asks PSS to track someone? Under a carefully drafted set of guardrails the answer might be "it depends on which kind of track." A short-term track only of pixels fleeing a crime scene has the "cause" of the search built in, and perhaps a written request from BPD, signed off on by a superior officer, capable of being audited after the fact, might be enough. On the other hand, there may be every reason to require a judicial order for BPD's Supplemental Requests, which are not self-limiting in the same way as a track from a crime scene, and involve a huge amount of discretion on the part of BPD officials in deciding whom to track and for what reason. Arbitrary police searching and unfettered discretion go to the core of what the Fourth Amendment was written to address. *See Delaware v. Prouse*, 440 U.S. 648, 653–54 (1979) (constraining discretion of government officials to "safeguard the privacy and security of individuals against arbitrary invasions" is the "essential purpose" of the Fourth Amendment); *accord Camara v. Muni. Court of City and Cty. of S.F.*, 387 U.S. 523, 528 (1967). The Fourth Amendment does not allow for this sort of nuanced decision-making, but democratically-authorized regulations could.

But the real problem under the Fourth Amendment is with the mass data collection that makes AIR work in the first place. If this constitutes a search, then under governing Supreme Court precedent it is forbidden altogether. *City of Indianapolis v. Edmond* bans programmatic government searches—i.e., searches that are conducted against everyone, without cause to believe anyone has done anything wrong—if they are for the purpose of ordinary law enforcement. 531 U.S. 32, 41–42 (2000) (narcotics checkpoint program violated Fourth Amendment where its "primary purpose" was "to uncover evidence of ordinary criminal wrongdoing"). And AIR assuredly is being used for ordinary law enforcement.

For what it is worth, we think the *Edmond* decision is problematic, and may limit government too much. How can one distinguish if a drunk-driving roadblock is for special needs (to address the dangers of driving under the influence) or for ordinary law enforcement (because people driving under the influence are going to be arrested)? In truth, the criminal laws are used regularly to further societal needs. We think the better approach is not to focus on the *purpose* of the mass search, but rather to focus on the safeguards put in place to protect individual rights. *See* Barry Friedman & Cynthia Benin Stein, *Redefining What's 'Reasonable': The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 319 (2016).

And so, yet again, our prescription is the same: the correct approach, if AIR is to be deployed at all, is for a sufficient set of safeguards to be imposed. They are not at present; and in Part V we detail what (at a minimum) they ought to be.

C. First Amendment Concerns: Associational Liberty

Because AIR allows the tracking of people, it also implicates associational concerns. These often are described as First Amendment liberties, though again the question before us is broader than the Constitution. Speaking of the Constitution alone though, the Supreme Court has made clear that "implicit in the right to engage in activities protected by the First Amendment [is] a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984). This right extends to *privacy* in one's associations, for this "may in many circumstances be indispensable to preservation of freedom of association." *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958). The right to privacy in one's associations is crucial for groups that espouse "dissident beliefs." *Id.*[24]

[24] *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143–44 (2007) ("Courts sometimes have found that government surveillance of political activities can implicate the First Amendment. . . . [W]hen plaintiffs have produced evidence of deterrence . . . . , courts have found cognizable First Amendment injuries.").

But such privacy also is important for the public more generally, because "[a]wareness that the government may be watching" can chill associational and expressive freedoms. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Several of the plaintiffs in the ongoing federal litigation express their concern about how mass data collection with the capacity of tracking inhibits their associational freedom.[25]

All-too-recent history makes clear that concerns about police intrusion into these liberties in Baltimore, and more generally in Maryland, is not hypothetical at all. A 2008 report commissioned by then-Governor Martin O'Malley concluded that the Maryland State Police had "covertly monitored individuals and groups engaged in anti-death penalty and anti-war activism," despite lacking "any information indicating that those individuals or groups had committed or planned any criminal misconduct."[26] In 2015, the FBI, in response to the scheduling of "large scale demonstrations and protests" after Freddie Gray's death, deployed surveillance planes—hidden behind shell companies—that were equipped with "sophisticated thermal-imaging and night-vision capabilities."[27] And this June, it was revealed that the Department of Homeland Security had deployed helicopters, airplanes, and drones in fifteen cities to surveil demonstrations after the death of George Floyd.[28]

Although we have not seen any evidence that AIR is being used in any way that would target First Amendment activities, one must be wary of this potential. The very purpose of guardrails is to ensure inappropriate action cannot occur. The recommendations we make in Part V about a regulatory framework take these associational concerns into account.

D. Mission Creep

Experience with policing technologies shows a natural inclination for their uses to expand over time.[29] Fusion centers, introduced in the wake of the September 11 attacks to promote intelligence sharing and counterterrorism efforts, now are used widely to pursue "all crimes" and "all hazards."[30] License plate readers, deployed originally to identify and locate stolen vehicles, now are used to collect and store location data, and to stop vehicles for things as minor as unpaid fines.[31] In evaluating any technology, one must be aware of the possibility of mission creep.

---

[25] The Fourth Circuit concluded that AIR did not interfere with the plaintiffs' associative rights because "people do not have a right to avoid being seen in public places," and "it is a stretch to suggest people are deterred from associating with each other because they may show up as a dot under the AIR Program." *Leaders of a Beautiful Struggle*, 2020 WL 6500931, at *9. Regardless of the merits of the plaintiffs' First Amendment claims, there may well be instances in which surveillance—even if limited to recording one's presence at a public location—could chill expressive conduct. *E.g.*, Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, ASSOC. PRESS (Feb. 23, 2012), https://bit.ly/3joMxi7 (NYPD surveilled mosques, "collect[ing] license plate numbers of congregants as they arrived to pray"). There is no evidence suggest that the AIR Program was involved in such surveillance, but the point is that safeguards ought to be in place to ensure it is not.

[26] STEPHEN H. SACHS, REVIEW OF MARYLAND STATE POLICE COVERT SURVEILLANCE OF ANTI-DEATH PENALTY AND ANTI-WAR GROUPS FROM MARCH 2005 TO MAY 2006 (2008), https://bit.ly/30pxRsr.

[27] Andrea Peterson, *FBI Spy Planes Used Thermal Imaging Tech in Flights Over Baltimore After Freddie Gray Unrest*, WASH. POST (Oct. 30, 2015), https://wapo.st/30850s6.

[28] Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. TIMES (June 19, 2020), https://nyti.ms/305PFIU.

[29] *See, e.g.*, SECOND REPORT OF THE AXON AI & POLICING TECHNOLOGY ETHICS BOARD: AUTOMATED LICENSE PLATE READERS (Oct. 2019), https://www.policingproject.org/axon-alpr (discussing expanded use of ALPRs over time); Neha Thirani Bagri, *Local US Police Departments are Creating Their Own DNA Databases of Unsuspecting (and Innocent) Citizens*, QUARTZ (Sept. 15, 2016) (noting "law enforcement's expanding use of DNA and the lack of regulation").

[30] *See* U.S. DEP'T OF HOMELAND SEC., IMPLEMENTING 9/11 COMMISSION RECOMMENDATIONS 3 (2011); ARIZ. COUNTER TERRORISM INFO. CTR., 2014 FUSION CENTER ASSESSMENT INDIVIDUAL REPORT 2 (2014).

[31] *See* AXON AI & POLICING TECHNOLOGY ETHICS BOARD, AUTOMATED LICENSE PLATE READERS 23–24 (2019), https://bit.ly/3pg0Md5.

Mission creep can trigger another concern—the over enforcement of low-level offenses. There is an emerging consensus that from the 1980s onward, the United States relied too much on arrest, incarceration, and the imposition of many criminal fines, often to address minor offenses or to police social problems that should have been dealt with in a non-criminal way. Mission creep can implicate this form of "overcriminalization" because technologies often first are adopted to address serious crimes, and later the use is expanded to include all manner of offenses.

There is evidence of the potential for mission creep around AIR. The MOU defined the "scope of services" PSS was to provide, stating that analysts would track individuals and vehicles *traveling to and from* the scene of a target crime. This is also how BPD described the program to the public and to the federal courts. And yet, because the MOU didn't expressly state that analysts *couldn't* engage in other forms of tracking, PSS undertook broader investigations at BPD's request—for example, following an individual's movements over the course of multiple days and tracking individuals traveling to and from a private home that was not the scene of a crime. In our view, this change materially expanded the scope of the program beyond what was originally described. This expansion occurred without democratic authorization or even public notice.

At the same time, there has been some sensitivity to mission creep. During the pilot, the question was raised as to whether AIR could be used to assist in locating individuals with outstanding arrest warrants for target crimes (e.g., a murder warrant). Ultimately, the decision was made by BPD that this use would go beyond the MOU, and was not permitted. The 2020 AIR Program also was more circumscribed than the 2016 program. During the 2016 program, PSS assisted in investigating lower-level crimes including hit and runs, illegal dumping, and "motorcycle/dirt bike related gang activity." It also engaged in real-time support. The 2020 MOU limited both of these.

In our view, the *possibility* of mission creep—a possibility that exists with all surveillance technologies—is yet another reason for a comprehensive regulatory structure, one that provides clear, unambiguous rules regarding what surveillance is and is not authorized. And it signals a broader need for BPD to become more democratically responsive—to view duly enacted rules not as barriers, but as manifestations of the public will regarding its assent (and its limits) for the use of powerful surveillance technologies.

E. Racial Disparity

Many have expressed concern about the potential for AIR to have disparate racial and socioeconomic impacts. These concerns are worthy of serious consideration because the various costs of crime and law enforcement are not borne evenly by the citizens of Baltimore. Rather, as is often the case, the impact of mass surveillance "is heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status." Barton Gellman & Sam Adler-Bell, **The Disparate Impact of Surveillance**, CENTURY FOUND. (2017).

The Historical Basis for Concern about Race and Policing in Baltimore

No consideration of AIR's impacts can be divorced from Baltimore's fraught history around race, class, and policing.[32] During our audit, we spoke with a number of civil rights and community leaders about the AIR

[32] *See, e.g.*, Monique Dixon, *NAACP Legal Defense Fund: Spy Plane Planned for Baltimore is Unconstitutional*, BALTIMORE SUN (Apr. 23, 2020), https://bit.ly/33BlMzP ("Amid Baltimore's history of unlawful and racially discriminatory policing practices, the new aerial surveillance program will likely serve to further erode trust between communities of color and the police department.").

Program, and the single most pervasive concern expressed was the belief that this technology would be used disparately against Black and brown communities. Almost every person with whom we spoke emphasized that this disparity cannot be considered in a vacuum, but must be understood against the background of the history of the Baltimore Police Department.

Although we cannot even attempt to document all of the history relevant to racial concerns in Baltimore, we think it important to provide some context.

The initial news that BPD had deployed an aerial surveillance plane in 2016 without notifying the public came roughly one year after the death of Freddie Gray in the back of a BPD police transport van, and in the midst of some of the largest sustained protests for police accountability in recent memory. Evidence has surfaced that BPD used covert surveillance to target those protests.[33]

In August 2016, the U.S. Department of Justice's Civil Rights Division found that BPD had engaged in a pattern and practice of conduct that violated the First, Fourth, and Fourteenth Amendments, and various federal laws. This led to the department being placed under a federal consent decree.[34] The DOJ found that BPD's enforcement strategies had "produce[d] severe and unjustified disparities in the rates of stops, searches and arrests of African Americans."[35] The "[r]acially disparate impact . . . present at every stage of BPD's enforcement actions," DOJ found, served to "erode the community trust that is critical to effective policing."[36]

This was not the first time that BPD's policing of Black Baltimoreans had come under scrutiny. Over fifty years before the DOJ's findings, the International Association of Chiefs of Police issued a report sharply critical of BPD's relationship with the city's Black community. See DAVID SIMON, HOMICIDE 109–10 (1991). "[W]ell before the 1960s," David Simon writes, "the contempt felt for the department" within the Black community "was close to universal" in light of the Department's treatment of Black residents. Id. In 1980, the NAACP called for a federal investigation into police brutality, which had heightened tensions between BPD and the Black community.[37] And these racial disparities deepened with the advent of BPD's "zero tolerance" strategy in the late 1990s.[38]

This is some of the context in which the racial impacts of AIR must be considered.

Racial Disparity and AIR

In evaluating the racial impacts of AIR, we focus on *disparities*. A disparity is a difference in outcomes for different groups. The law distinguishes between disparity and discrimination; the latter is used legally to refer to the *intention*

---

[33] See Jonah Engel Bromwich, et al., *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. Times (Oct. 11, 2016) (discussing BPD's use of social media tool Geofeedia to monitor and respond to Freddie Gray protests); see also Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG BUSINESSWEEK, Aug. 23, 2016 (discussing use of aerial surveillance to "monitor the city's reaction" to the acquittal of a BPD police officer tried for Freddie Gray's murder).

[34] See CIVIL RIGHTS DIVISION, U.S. DEPARTMENT OF JUSTICE, INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT (Aug. 2016), https://www.justice.gov/crt/file/883296/download; Consent Decree, United States v. Police Department of Baltimore City, Case 1:17-cv-00099-JKB (Dist. Md. Jan. 12, 2017).

[35] DEP'T OF JUST., *supra* note 1, at 3.

[36] *Id.* at 7.

[37] Sheryl Gay Stolberg, *Baltimore's 'Broken Relationship' with Police*, N.Y. Times (Apr. 24, 2015), https://nyti.ms/32GdZTr.

[38] German Lopez, *Baltimore Cops Stopped an Innocent Mid-50s Black Man 30 Times in Less than 4 Years*, VOX (Aug. 10, 2016), https://www.vox.com/2016/8/10/12418430/baltimore-police-racial-bias-justice-department.

to treat groups differently. But even if a disparity is not the result of intentional conduct, it still is a cost that must be considered.

As with the question of whether the use of AIR constitutes a search under the Fourth Amendment, there are two potential sources of racial and other demographic disparities in the use of AIR.

First, one must consider the possibility of disparities in the tracking of particular individuals as part of AIR investigations. We do not have the data to evaluate this possibility in detail—AIR analysts do not, and often cannot, record the demographics of everyone they track. The Department of Justice's 2016 investigation found that law enforcement in Baltimore "intrudes disproportionately upon the lives of African Americans at every stage of its enforcement activities."[39] Until the problems underlying those findings are remedied, there is reason for concern that these same disparities might exist with regard to the tracking of individuals by AIR.

As AIR is described in the MOU, there are features that would limit discretion, which often is the cause of troubling disparities in law enforcement. First, AIR is used for only the most serious crimes. Second, BPD implemented a policy requiring that *all* target crimes investigations request AIR support. Finally, the MOU was designed to limit the use of AIR to tracking individuals to and from crime scenes. As we explained in the context of the search issue, using AIR only to track individuals to and from crime scenes (including individuals whose paths they cross along the way) both curtails discretion and is capable of verification.

But once again, the use of Supplemental Requests undermines these limitations on discretion. It allows the picking and choosing of which investigations to pursue, and against whom. We cannot know whether this has resulted in inappropriate disparity, but the potential is there. Supplemental Requests might be a reasonable part of an AIR program, but additional protections then would be needed to guard against discretion being misused.

Second, one must evaluate the possibility of disparity in the bulk collection of movement data that feeds the AIR Program. As initially conceived, AIR posed little danger of racial or socioeconomic disparities in aerial coverage. The plan was to fly four separate geographic orbits, the coverage of which, in aggregate, would include virtually all of Baltimore City. But PSS did not have enough operational planes to fly all four orbits. Instead, PSS conducted nearly all flights centered on East and West Baltimore—predominantly Black areas. To be sure, AIR covered many majority-white neighborhoods adjacent to East and West Baltimore. But PSS flew the northern orbit—which includes Roland Park, Mount Washington, and surrounding areas, as well as sections of Baltimore County—on only two occasions. This both limited coverage of the wealthy areas in the city's northern end (as well as some nearby predominately Black neighborhoods). The limited coverage also resulted in fewer crimes being captured overall. Once these twin problems became clear—limited coverage and greater disparity—PSS and BPD attempted to address these shortfalls by increasing the flight coverage area from 32 to 45 square miles. PSS claims this change eliminated any racial disparities, but we cannot be sure—although PSS increased coverage of some white areas, it also increased coverage of several Black areas.[40]

It is worth noting that the aerial aspect of AIR is not the only potential source of disparity. AIR depends on its integration with CitiWatch cameras. Although certain wealthier and whiter neighborhoods have a high

---

[39] *See* DEP'T OF JUST., *supra* note 3, at 47 ("BPD officers disproportionately stop African Americans; search them more frequently during these stops; and arrest them at rates that significantly exceed relevant benchmarks for criminal activity. African Americans are likewise subjected more often to false arrests.").

[40] Teasing out the extent of any racial disparity with regard to AIR is exceedingly difficult. Coverage area alone will not answer this question. Not all aerial coverage is created equally – on average, those areas closer to the edges of an aerial coverage area will have lower quality; to the extent that PSS flights are centered over Black neighborhoods in East and West Baltimore, disparities may result.

concentration of cameras, overall, CitiWatch cameras are deployed in eleven of Baltimore's fifteen majority-Black ZIP Codes, but only three of its majority-white ZIP Codes.[41] The cameras also are located on a number of public housing units, meaning that AIR's capacity to conduct tracking is increased for the predominantly Black and low socioeconomic status residents of those units.[42] Other neighborhoods may have a greater number of private cameras, but PSS analysts only have direct access to CitiWatch cameras.

The simple fact is that in a deeply segregated city such as Baltimore, decisions about where to deploy surveillance almost always will have some degree of disparities.

As we have said, even if there are racial or socioeconomic disparities, one cannot equate this with deliberate discrimination. Surveillance deployment decisions generally are made based on crime data. In this case, flight paths were based in part on recent data regarding where homicides were occurring in Baltimore. And BPD Commissioner Michael Harrison has argued that the ground cameras "may coincidentally be in black and brown neighborhoods" as a function of where crime is occurring.[43]

Still, even if placement of surveillance tools is motivated only by the location of criminal events, racial disparities nonetheless are real. Each of the impacts we discussed above—the privacy and security concerns, the chilling of associational liberty, the risk of mission creep, etc.—will fall disproportionately on people of color if the surveillance primarily is in the communities in which they live. This is just a fact. Moreover, concentrating surveillance in discrete communities can be stigmatizing, causing residents to feel that they're being unjustly targeted.[44]

While these are costs; AIR also may have benefits. And if those benefits exist, they may especially benefit the Black community, which bears the brunt of the violence AIR is designed to combat.

All of which leads us to our central point in this Report – that the decision to use AIR must be made by a democratically-accountable body. Race and policing is a deeply salient issue in Baltimore, and for good reason given the history we recounted briefly. It is because of Baltimore's history around race and policing, above and beyond any other, that the decision whether to deploy the AIR program—and where to deploy it—must be made by the public, in a way that the public believes is legitimate, and that accounts for legitimate public concerns. That is the only plausible way to take seriously the racial concerns we heard so often expressed. It is to this issue that we now turn.

---

[41] See *CCTV Locations*, CITY OF BALTIMORE (last updated Feb. 18, 2019), https://bit.ly/3klxmHh.

[42] See Balt. City Dep't of Hous. & Cmty. Dev., Consolidated Annual Performance & Evaluation Report (2019), https://bit.ly/2RNwYVO.

[43] Fern Shen, Without Much Zeal, Harrison Backs 'Spy Plane' as City Approves Agreement, BALTIMORE BREW (Apr. 1, 2020), https://bit.ly/32CWxyR.

[44] See Madison Organizations Push for Community Control Over Police Use of Surveillance Technology, ACLU (Sept. 20, 2016), https://www.aclu-wi.org/en/press-releases/madison-organizations-push-community-control-over-police-use-surveillance-technology ("The increasing, secret use of surveillance technologies by local police, especially against communities of color and other unjustly targeted groups, is creating oppressive, stigmatizing environments in which every community member is treated like a prospective criminal."); Hassan v. Hassan v. City of New York, 804 F.3d 277, 287–88 (3d Cir. 2015) (civil rights plaintiff arguing that surveillance of Muslim community created stigmatic harms); Tina G. Patel, Surveillance, Suspicion and Stigma: Brown Bodies in a Terror-Panic Climate, 10 SURVEILLANCE & SOC. 215, 217 (2012) ("Surveillance is a powerful means by which negative labels are created and strengthened."); cf. Jeffrey Fagan et al., Stops and Stares: Street Stops, Surveillance, and Race in the New Policing, FORDHAM URB. L.J. 539, 567 (2016) ("The dignitarian concerns pose one type of harm: the fact that one is a target of surveillance signals to other observers and perhaps to the watching public the person is a potential threat. That alone can have stigmatizing consequences throughout the community of the observed.").

IV. Democratic Accountability

The foregoing discussion about investigative uses and potential harms brings us to the issue of democratic accountability—namely, what voice the public had (and ought to have) in setting the rules for the AIR program.

In advocating for clear democratic accountability around AIR, this Part make three key points: (a) ensuring that there exists meaningful democratic accountability over a technology is not the same as surveying public opinion; (b) although the 2020 AIR Program operated with better democratic accountability than the 2016 version, there was still room for improvement; and (c) we believe Maryland law must be changed to restore to the Baltimore City Council formal regulatory authority over programs like AIR.

A. Meaningful democratic accountability requires more than just assessing public opinion

The decision to deploy technology such as AIR is a momentous one. Some substantial portion of the population is subjected to surveillance, in the hope of advancing public safety. Were it not for the concern for public safety, there would be no need for surveillance. But surveillance comes with costs, as we have pointed out throughout this report. It deprives people of their security. It puts substantial power in government hands—notably the police, which in Baltimore have their own accountability and trust issues. It chills association. And, as we have explained, it presents a risk of contributing to racial and socioeconomic disparities.

All involved clearly understand this when it comes to AIR, which is likely why the question of whether the people of Baltimore support or oppose the AIR Program has been a topic of discussion and study on a number of fronts.

PSS executives have attended dozens of community meetings over the last few years and have argued that they were "asked to return to Baltimore by a wide range of members of the community and community groups." In the federal litigation, BPD claimed that the program has "widespread support." *See* Br. of Appellee at 12, *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, No. 20-1495 (4th Cir. 2020) ("Proponents include Governor Larry Hogan and dozens of victims and community groups, the business advocacy group Greater Baltimore Committee, and the United Baptist Ministry Convention, which includes more than 100 churches."). Both the Fourth Circuit and the federal District Court cited BPD's "evidence" of community support in support of permitting the program to continue.

But there are those who dispute the extent of AIR's community support. The Plaintiffs in the federal litigation, for example, represent a number of community-based public safety organizations, and their litigation filings cite evidence of community opposition to AIR. *See* Br. of Appellant at 55, *Leaders of a Beautiful Struggle* (stating that "scattered evidence of pockets of support for the AIR program" do not provide "the full picture," and citing evidence of opposition to AIR). Some, including members of the City Council, also have questioned the way in which PSS gathered support from organizations and individuals in Baltimore.[45]

[45] *See* Ethan McLeod, *City Council Members Grill Spy Plane Company, BPD Over Privacy Concerns, Lobbying*, BALT. FISHBOWL (Oct. 17, 2018), https://baltimorefishbowl.com/stories/city-council-members-grill-spy-plane-company-bpd-over-transparency-lobbying-privacy-concerns.

Rather than rely on anecdotal evidence, the MOU required a formal evaluation of community sentiment regarding AIR. The University of Baltimore's Schaefer Center was engaged to conduct a survey to gauge public knowledge and opinion about the program, with a focus on communities that were most likely to be impacted. Morgan State University also is conducting community outreach. Whether assessing the views of the entire city or focusing on those most impacted by surveillance and violence, quantitative studies must be representative for their conclusions to have weight.

Even formal studies of community opinion will have limited value unless respondents have clear details about how AIR works, not to speak of evidence about whether AIR works. It is all too common around policing simply to assume the supposed benefits of a technology. RAND currently is studying the benefits of AIR, including its impact on clearance rates. This report has discussed the serious social costs AIR entails. Until people have all this information, there is a real limit to what sort of conclusions one can draw from claims of public support or lack thereof.

But there is a yet more fundamental point. A decision to employ a powerful surveillance technology like AIR is the sort of decision that, in our view, is too weighty not to be made without some form of formal democratic decision-making and the accompanying accountability.

Public forums may be useful for general education, and for mustering a set of views that can feed into a proper democratic process. But community meetings cannot approve a program like AIR, which affects the population of the city. In the discussions around AIR, some have touted the voices in the community that favor the program, while others have pointed to those who do not. Government may take account of public opinion surveys, but it does not govern that way. Instead, we have formal democratic bodies charged with making decisions such as these. A program such as AIR involves serious tradeoffs. Nor is it, as we have stressed repeatedly, an all or nothing decision, because there always is the option of adopting a program like AIR with serious guardrails in place.

Community sentiment alone cannot make decisions, nor put in place a regulatory framework. Only formal democratic decision-making can do that.

B. Improving democratic governance around AIR

Which brings us to the democratic process around the adoption of AIR.

To be sure, the 2020 version of the AIR Program operated with greater democratic accountability than the 2016 version. Whereas the public only learned about the 2016 version of the program from the media after months of flights, in this instance BPD and the donor who is funding this pilot jointly decided, appropriately, that a more transparent and open process was needed, including submitting the MOU for approval to the Baltimore Board of Estimates.

Although these efforts mostly were commendable, we still think it was possible to do better.

First, community sentiment and even government approval are shaped by what is—and is not—disclosed to the public, and from our perspective, there were serious problems regarding how AIR was presented. Some of the information made public during and in advance of the pilot period differed in important ways from how

the program actually operated. As we have stressed above, the creation of Supplemental Requests and the amount of aerial data being retained are both, at a minimum, different from what people were led to understand. Moreover, AIR was advertised as not only a tool for crime-fighting, but also as a tool for investigating police misconduct and for defense attorneys. But neither of these latter uses played a meaningful role in the program.[46] PSS representatives also overstated AIR's efficacy and legality, claiming in one public meeting that AIR had increased closure rates by "two to three times" and that "Supreme Court decisions have upheld this program as legal and constitutional." If public approval is to be meaningful, the public must have precise facts.

Second, we believe that given the nature of the AIR Program, it would have made more sense for approval for the program to come from a more majoritarian body, such as City Council, rather than the BOE. In this instance, the AIR Program approval went through the BOE because it was funded by private philanthropy and the funds went directly to PSS. The MOU was made public only shortly before the BOE's virtual hearing on the matter. Had the funding gone to BPD instead, which in turn would have funded PSS, the City Council would have needed to pass a supplemental appropriation ordinance and the mayor would have needed to approve it.[47]

Although the BOE has been used to approve a range of agreements relating to BPD technology and equipment, those agreements are different largely in kind and certainly in degree than a program like AIR, which bears substantially on many individuals' rights. The BOE has approved agreements relating to police duty gear, radio equipment, federal funding for the hiring of crime analysts, police vehicles, and DNA testing for missing persons cases. The BOE also recently approved funding for body worn cameras and license plate readers, though these either were extensions of existing contracts or for maintenance and support of existing equipment, not new deployments.[48]

Given that AIR affects wide swaths of Baltimoreans, potentially implicating both their public safety and their rights, we believe City Council approval would have been more appropriate. Legislative bodies, being the most representative, have the best chance of making the tradeoffs presented by a program like AIR in accord with popular preferences.[49]

---

[46] At one public meeting, attendees were told that the 2016 program had led to a criminal defendant's acquittal—a claim that is somewhat of an oversimplification. In January 2020, prosecutors moved to vacate the conviction of Jawan Richards — one of 790 convictions considered "tainted" by BPD's Gun Trace Task Force scandal. *See* Brandon Soderberg, *Baltimore Defense Attorneys Claim Surveillance Plane Footage Contradicts Law Enforcement Account of Police Shooting*, THE APPEAL (Feb. 13, 2020), https://bit.ly/32FBH1t. One of Richards's attorneys filed a separate motion to vacate based in part on AIR imagery from the 2016 program. It is unclear whether AIR imagery played a decisive role—or any role—in the court's vacatur of Richards's sentence. *See* Justin Fenton, *Baltimore Police Misconduct Prompts Conviction to be Overturned. The Spy Plane Caught Scene, But Added Little Clarity.*, BALT. SUN (Mar. 2, 2020), https://bit.ly/3IrlSD5.

[47] Balt. City Charter, Art. VI § 8(B)(2).

[48] *See* MINUTES, BALT. BD. OF ESTIMATES 2541 (June 24, 2020) https://comptroller.baltimorecity.gov/sites/default/files/2416-2556_2020-6-24.pdf (body worn cameras); MINUTES, BALT. BD. OF ESTIMATES 3676 (Aug. 7, 2019), https://comptroller.baltimorecity.gov/sites/default/files/3605-3721_2019-08-07.pdf (license plate readers).

[49] Legislative bodies have their own shortcomings, of course, including that the decisions they make may be driven more by special interests or by passion of the moment than rational analysis of all relevant variables. That is why many decisions are allocated to administrative bodies, which may be less subject to popular or regulatory capture, and which can assess the tradeoffs dispassionately. Even there, however, there are controls in place to ensure that the decisions that are made can be overturned by legislative bodies should they so wish.

C. A Historical Relic Limiting Democratic Accountability in Baltimore

It is precisely at this juncture that one runs into a problem of democratic accountability in Baltimore that is staggering. For historical reasons that have nothing to do with the present, the Baltimore City Council (and therefore, the people of Baltimore) do not have democratic control over their police department. In 1860, control over BPD was taken by the state legislature, and never has been returned.[50]

Today, the only control City Council exercises over the police department is through the budgetary process. That would allow the City Council to vote a project like AIR up or down, but not to implement the very sorts of guardrails and conditions on BPD's use of AIR that we believe are essential.[51] To make matters worse, under current law the City of Baltimore has to pay for the police department—with only a fraction of BPD's budget coming from state appropriations.[52] One cannot help but hear echoes of our Founders' concerns about taxation without representation.

Nor, while we are on the point, do we believe that mayoral control over BPD is sufficient to meet democratic concerns. Mayors control the police through the power to hire and fire the Commissioner (or Superintendent, or Chief, depending on the city). But this is wholesale control, when what is needed is for a program like AIR is democratic regulation at retail—the specification of policies and practices on how AIR will operate. The Mayor could not enact into *law* the sorts of provisions we identify in the next section.

Given the troubled history of race and policing in Baltimore, allowing legislative control over BPD and the AIR Program to remain in the hands of the state legislature is deeply troubling. Representatives of Baltimore City make up only 12.7% of the State Senate and 11.3% of the House of Delegates.[53] This means that the legislature will made decisions that profoundly affect the people of Baltimore, for which they are not democratically accountable.

In 2017, one of Baltimore City's delegates to the Maryland General Assembly introduced a bill that sought to require the Baltimore Police Commissioner to notify Baltimore City officials of the development and implementation of "new tactics, technologies, and devices."[54] The bill specifically identified aerial surveillance as an example of a technology about which the Police Commissioner must provide notification. The Maryland Assembly, the vast majority of which is not elected by the people of Baltimore, ultimately failed to pass the bill.

The City Council itself has recognized that the current situation is untenable. A resolution of the City Council states that it is "impossible for the City to permanently set policies regarding the Police Department through its

---

[50] *See* Art. IV, § 32 of the 1860 Maryland Code (providing that "no ordinance heretofore passed or that shall hereafter be passed by the mayor and city council of Baltimore shall hereafter conflict or interfere with the powers or of the exercise of the powers of the Board of Police…"); *see also* H.H. Walker Lewis, *The Baltimore Police Case of 1860*, 26 MD. L. REV. 215 (1966); George A. Nilson, *The Baltimore Police Department: Understanding Its Status as a State Agency*, 32(2) ABELL REPORT 1 (Mar. 2019), https://abell.org/sites/default/files/files/Abell%20Baltimore%20Police%20Department%20Report.pdf.

[51] The best City Council could hope to do, perhaps—and we are not sure if this would be lawful—is regulate PSS, hoping that is sufficient to achieve all the safeguards we set out in the final section.

[52] *See* SUMMARY OF THE ADOPTED BUDGET, FISCAL 2020, CITY OF BALT., MD. (2020), https://bbmr.baltimorecity.gov/sites/default/files/Final%20SOTA%20FY20-compressed%20web.pdf.

[53] *See General Assembly, Members by County, Baltimore City*, MD. MANUAL ON-LINE, https://msa.maryland.gov/msa/mdmanual/07leg/html/gacobcit.html (last visited Nov. 2, 2020).

[54] *See* Maryland H. Bill 58, *Baltimore City – Police Tactics and High Crime Zone Notification* (2017), http://mgaleg.maryland.gov/2017rs/bills_noln/hb/fhb0058.pdf.

own legislation."[55] A 2019 bill to return control of BPD to Baltimore passed 137–0 in the Maryland House of Delegates. Despite strong support for the bill from the City Council, then-Mayor Catherine Pugh, and Commissioner Harrison, the bill died in the Maryland Senate.[56]

In our view, any future decision to operate AIR should reflect a democratically evaluated assessment of the relative benefits and costs. Approval should not be a mere up or down vote, but should include the possibility of an effective set of guardrails to mitigate any harms. Under current Maryland law, the people of Baltimore do not have the ability to provide appropriate democratic consideration of a program like AIR because the State legislature, not the City Council, retains control over BPD. We urge the Maryland State Legislature to reconsider the extent of its control over BPD, and at the least to return democratic control over surveillance technologies. The Baltimore City Council should have the ability to determine the fate of the AIR Program in the future.

[55] Request for State Action – Create a Board of Police Commissioners and Transfer Full Control of the Baltimore City Police Department to the City of Baltimore, Balt. City Council Res. 18-0067R (Feb. 5, 2018).

[56] *See* Luke Broadwater, *Bill to End State Control of Baltimore Police Won't Pass This Year After Opposition From City Senators*, BALT. SUN (Apr. 5, 2019), https://www.baltimoresun.com/politics/bs-md-local-control-police-20190405-story.html.

V. Regulatory Framework

In Part III, we analyzed the civil liberties and civil rights impacts that AIR might entail, among them imperiling individuals' privacy, chilling First Amendment activity, and deepening racial disparities around policing. As we explained, some of those may be innate to using AIR at all. But many are attributable, at least in part, to specific decisions made by BPD and PSS about how the AIR program will operate.

The point of Part IV is that for a program like AIR—with potential benefits, but also with notable potential harms—the decision regarding deployment should be made by a democratically-accountable body. That decision need not be all or nothing. Even if there is interest in proceeding with AIR, such a decision should involve a crafted regulatory scheme that seeks to maximize the potential benefits while mitigating harms. That is precisely the work such a democratically-accountable body should be doing.

To be clear, such democratic authorization never is the final word. Judicial review of the constitutionality of AIR still would remain. But such review only would be aided by the presence of legislation that made clear what AIR does and what it is not permitted to do.

This final Part tackles the question of what a regulatory framework for AIR might look like in a future iteration of the program. Although some of this framework discusses BPD and the AIR Program, these recommendations easily could apply to any jurisdiction considering PSS's services. We note that this sort of regulatory structure is not unique to AIR but contains the bones of what should be in place for the use of any powerful policing technology. Nor do we presume to have landed on the precisely correct set of solutions—once again, that is for the appropriate regulatory body or democratically accountable entity to decide, in any jurisdiction that is considering deploying AIR or a program like it. But we believe unequivocally that if AIR is to be utilized at all, some structure like this one is needed to address the very serious risks we identified in Part III.

1. Clearly demarcate the AIR Program's capabilities and integrations at the outset, and require notice and approval before expanding them.

A crucial first step towards adopting a responsible regulatory framework is clear specification of AIR's capabilities and integrations. Decision-makers need to know precisely how AIR will be used. Some of this, such as the crimes for which AIR is deployed, or the resolution of the cameras, should be set out in the initial authorization, and there should be adherence absent formal approval of any change.

The difficult question is how to allow AIR the flexibility to grow while still maintaining democratic control over critical decisions. A body approving AIR might require a return to it for any substantial change, such as a decision to deploy night vision photography, or to increase the resolution of the aerial photographs.

Yet, this also could prove unwieldy. An alternative is to allow decision-makers—such as the Mayor and Police Commissioner acting in concert—to make these interim decisions, so long as they are made transparently, thus allowing a democratic body to alter them if that is the will of the people of Baltimore.

In either event, it is essential to recognize that AIR is not a single, static technology, and cannot be treated as such. It certainly is an error to think of AIR as involving solely aerial photography. We are skeptical it would

have made any sense to deploy AIR absent its integration with ground surveillance, including CitiWatch cameras and license plate readers. Any number of features could be changed in the future, including the resolution of photographs taken by the plane, the addition of night vision photography, the crimes for which it is deployed, processing images obtained by AIR analysts via facial recognition, or the incorporation of new ground-based surveillance. There must be an acceptable process for approving such changes that is transparent to the public and subject to ultimate democratic control.

2. Require policing agencies to draft a use policy and make it public before beginning operations.

Even with a sound regulatory approach, any agency that seeks to operate the AIR Program should draft a use policy and make that policy public. This requirement helps ensure that key decisions about program operations are made by high-ranking policymakers in the department, not on an ad hoc basis. Setting policy at a departmental level also ensures that officer discretion is constrained. Making the policy public ensures that the public is aware of these decisions and provides a degree of public accountability. Rather than viewing this process as a burden, agencies should view it as an opportunity for community engagement.

At a high level, any agency policy regarding the AIR Program should address implementation of the regulatory framework discussed above, and should discuss:

- which agency personnel are authorized to use the program;
- what training is required before agency personnel can access the program;
- what responsibilities supervisors will have, if any, to document and review each deployment or use;
- the specific steps agency personnel must take, including required documentation, to initiate an AIR investigation;
- the process by which data will be deleted after the retention period elapses;
- the circumstances (if any) under which data will be shared with other government agencies; and
- the manner in which the program will be documented, audited, and reported to the public, consistent with the regulatory framework.

3. Specify the offenses that may be investigated via the AIR Program, so as to avoid any mission creep.

An extremely important aspect of any regulatory structure is specifying the offenses that may be investigated using AIR. This was a central feature of the MOU; BPD was limited to using AIR to investigate homicides, attempted murder, shootings with injuries, armed robberies, and car-jackings. This type of limitation ensures that the AIR Program's powerful surveillance capabilities are reserved only for those offenses the public believes are most serious and warrant the intrusion, avoiding undue surveillance and mission creep.

4. Require transparency and empirical justification for decisions about where the AIR Program operates.

Decisions about where to deploy AIR's aerial surveillance planes should rest on an objective, demonstrated basis to believe that target crimes are more likely to occur in the areas being surveilled than the areas not being surveilled.

AIR's aerial surveillance aspect is an example of suspicionless policing—surveillance conducted without any belief that a particular individual, place, or item subject to it is involved in unlawful conduct. Like CCTV cameras and license plate readers, aerial surveillance covers a geographic area and gathers information in that location indiscriminately. It is essential, therefore, that decisions about where to deploy this technology are guided by evenhanded, neutral criteria that are set in advance, and not set arbitrarily or on the basis impermissible characteristics, such as race or ethnicity. A regulatory framework can help ensure this either by setting those neutral criteria in advance, or by requiring policing agencies (with input from their communities) to set those criteria, with some mechanism for review.

As discussed in Part III, decisions about where to deploy a new technology, even if based on neutral criteria, still may contribute to racial, religious, or other disparities. This especially is the case in cities with high levels of residential segregation. For this reason, it is essential that policymakers, in setting deployment criteria, carefully consider the possibility of disparate impacts and how best to mitigate them.

5. Require and document an adequate factual predicate for any investigation before permitting access to AIR Program data. In some instances, this should involve judicial approval.

There should be a clearly-stated factual predicate for commencing AIR investigations. At present, investigations begin on the say-so of BPD personnel alone. The plaintiffs in the federal litigation, in stark contrast, would have required BPD to obtain a warrant any time BPD seeks access to the data — in part because the Fourth Amendment, as currently construed, requires warrants for individualized searches.

Enacting a regulatory framework allows for a more nuanced approach.

The key to avoiding unnecessary and arbitrary access to AIR Program data begins with clearly articulating (1) the set of circumstances under which AIR Program data may be accessed and (2) who will be responsible for ensuring that these predicate circumstances have been met. We can envision a two-tiered system, although others are of course possible.

For basic tracking of persons and vehicles to and from the scene of a target crime, we think it would be reasonable to establish a procedure that requires only probable cause that a target crime has occurred, not that the particular person of interest committed the crime. Such tracking may not necessitate a court order—although warrants are an important limitation on officer discretion in many cases, discretion is limited naturally when officers simply are tracking subjects traveling to and from the documented scene of a crime. Adherence to this rule can be obtained by strict auditing, and clear consequences for not following the rules, which we discuss below. Instead of requiring a warrant, policymakers could require a sworn affidavit from the investigating officer. And because long-term tracking represents a more substantial incursion upon individual privacy, AIR investigations of this type might be limited to a certain duration—such as 3 hours before and after the crime.

For more involved tracking, such as Supplemental Requests that were not tied to the scene of a crime or involved tracking over multiple days, it is reasonable to include more rigorous requirements. The regulatory framework might, for example, require that police establish probable cause that a particular person or vehicle committed the target crime, and limit tracking to that particular person or vehicle. Duration again would be

limited, and a court order could be required for this type of tracking. *Cf.* MD. CODE CRIM. PROC. § 1-203.1(b)(1) (requiring probable cause and a court order for real-time location tracking of cell phones and GPS devices). These rules would apply as well to the use of AIR to locate the subjects of arrest warrants for target offenses.

6. Specify rules around tracking and identification of victims, witnesses, and associates.

AIR's reach is not limited to suspects, but has been used to track and identify possible victims, witnesses, and individuals who associate with suspects. In our view, any regulatory structure should specify the circumstances and rules under which this type of tracking is permitted.

As we noted in the previous section, discretion naturally is limited when officers simply are tracking individuals traveling to and from a crime scene. But once officers have confirmed that an individual whom they are tracking is not a suspect, a different set of considerations comes into play. As much as society prefers that witnesses and victims come forward—and they generally have strong incentives to do so—there are compelling reasons why this is a matter of individual choice. Individuals may fear retaliation or gang violence, for example. Some may worry about immigration consequences if they interact with law enforcement. Still, most jurisdictions allow prosecutors to subpoena witnesses to testify and, in certain circumstances, allow officers to seize and bring witnesses in. *See* MD. RULE 4-267 (Body Attachment of Material Witness).

It is not self-evident how to balance the need to generate investigative leads with the conflicting individual interests that some may have. Ultimately, communities must make this decision for themselves, determining whether some degree of additional process, such as a prosecutor or grand jury's sign-off, might be appropriate.

7. Implement additional protections around First Amendment activities.

A regulatory framework also ought to include additional protections around protected First Amendment activities, such as protests and marches, and First Amendment locations, such as houses of worship. For example, it might be appropriate to require more specific documentation or additional high-level supervisory approval before an investigation is permitted to touch on these events or locations. One might also include data minimization requirements — requiring faster deletion of footage of protests or demonstrations absent evidence of a target crime.

8. Provide specific and clear guidance around data retention.

As discussed above, AIR's current data retention practices leave much to be desired. The MOU sets the data retention period at 45 days. Although the Program gave the initial impression that little aerial imagery would be retained beyond 45 days, in practice approximately a substantial majority of the data is retained indefinitely and can be accessed freely for any target investigation. *See* Part II.G *supra*. Also, there is no coordination of retention periods for aerial imagery and data from ground-based sources, which does not make a great deal of sense.

A regulatory framework should set clear and enforceable retention limits, subject to after-the-fact auditing. Absent some reason we are missing, retention periods should coincide with the retention period for the ground cameras that are so critical for the AIR Program's operation. The framework should specify how much footage is to be retained—for example, rather than retaining the entire day's footage when there is a target crime, perhaps retention only should cover the period of time that a person or vehicle was being actively

tracked. A regulatory framework also could mandate deletion after the specified retention period and require that data retained in connection with one case be moved to a separate secure server, inaccessible for any other investigation absent a court order.

A regulatory framework also could require that PSS design its technology in a way that limits the data it must retain. At present, PSS has no way of retaining only the part of an aerial image that is of interest to an investigation. Nor does it have a way to delete certain portions of an image—such as areas that fall outside city limits. A regulatory framework should require a fix to this problem, thereby allowing PSS to retain far less data per investigation, and even creating additional protections for particular locations. This type of approach is akin to the minimization requirements included in a number of state and federal statutes regulating various surveillance activities. *See, e.g.*, Title III of The Omnibus Crime Control and Safe Streets Act of 1968.

9. Specify data security and data access procedures.

Given the sensitivity of AIR data, particularly when it is combined with ground surveillance, there must be effective data security and careful access procedures. These sorts of rules should be written into law.

10. Study and minimize noise impact.

A regulatory framework for AIR should address the noise created by the surveillance planes.

Given that the aerial component of the program involved flying manned aircraft in orbits over densely populated sections of Baltimore, it perhaps is not surprising that noise emerged as an issue. In fact, noise complaints were the single largest source of complaints about AIR from members of the public.[57] To mitigate noise impacts, PSS generally did not fly orbits below 4,500 feet above sea level. PSS also states that it has sought approval from the Federal Aviation Administration to equip its planes with mufflers.

Any attempt by state or local policymakers directly to regulate the noise impact of AIR flights may raise difficult legal questions. State and local governments generally are limited in their ability to regulate aircraft noise directly.[58]

But in deciding whether and how police should be permitted to utilize AIR, policymakers certainly should consider the noise impacts on residents. Policymakers should study both the extent of the noise impacts and their location—different areas of the city may experience different degrees of noise, depending on the flight paths taken. Policymakers could consider any changes that PSS can make to the program, including equipment modifications or altering flight paths or times.

---

[57] *E.g.*, Kathy Helzlsouer, *Reader Commentary: Noisy Spy Plane Needs To Be Grounded*, BALT. SUN (Sept. 17, 2020) https://bit.ly/32j575s ("[E]ven through closed windows the plane drones on, constantly. There is no escaping the noise pollution . . . ."); Glenn Schwartz, *Reader Commentary: Whether the Day Is Cloudy or Sunny, City's Surveillance Planes Are a Noisy Aggravation That Should Be Discontinued*, BALT. SUN (June 5, 2020), https://bit.ly/38ndwsa ("It's an annoying blare that I hear every 8 minutes almost every day . . . ."); Megan Beller, *Reader Commentary: Surveillance Plane Generates a Noise Baltimore Could Do Without*, BALT. SUN (May 18, 2020), https://bit.ly/3p9hye3 ("Please make it stop."); Louis Krauss, *In Baltimore, Complaints About the Sounds of Surveillance*, BALT. BREW (May 13, 2020), https://www.baltimorebrew.com /2020/05/13/in-baltimore-complaints-about-the-sounds-of-surveillance (comparing the sound of the planes to a "leaf blower"). BPD's mid-term report on AIR shows that fully two-thirds of citizen complaints about the program pertained to noise. *See* BALT. POLICE DEP'T, AERIAL INVESTIGATION RESEARCH (AIR): PILOT PROGRAM MID TERM REPORT 18 (2020).

[58] *See City of Burbank v. Lockheed Air Terminal Inc.*, 411 U.S. 624, 640 (1973); *Friends of the E. Hampton Airport, Inc. v. Town of E. Hampton*, 841 F.3d 133, 139 (2d Cir. 2016); 8A AM. JUR. 2D AVIATION § 17 (2020) ("Congress has occupied the entire field of regulation related to aircraft noise, and attempts by local governments to enforce their police powers to control noise or affect flight patterns are preempted.").

11. Enable and provide appropriate discovery to defense counsel.

At present, our criminal system contains an unacceptable imbalance between prosecutorial and defense counsel access to emerging technologies. A regulatory structure for the AIR Program should recognize this imbalance and specify the conditions under which defense counsel will be given access to AIR data.

First, the legislature should provide defense counsel with the ability to access AIR data for defense purposes. PSS advertised this use and featured it prominently in community meetings regarding the program. Yet, there have been no requests for AIR imagery from defense counsel. A regulatory approach could specify the circumstances under which defense counsel can request AIR imagery, whether defense can request access to ground surveillance as well, and the proper allocation of costs. It is unclear why prosecutors and the police should have access to technology to pursue charges, but defense counsel should lack the same access to defend against them.

Second, any regulatory framework should specify the discovery rules that apply. For example, the regulatory framework should require PSS analysts to document fully the reasoning behind any investigative conclusions they reach (*e.g.*, whether an individual is deemed a suspect or not involved). PSS analysts and police officers should be required to document fully their conversations, including all information conveyed in both directions. And most importantly, the regulatory framework unequivocally should prohibit officers from concealing their use of AIR in investigations—a practice known as parallel construction.[59] Officers should be required to inform prosecutors and the court in any case in which AIR was used as part of an investigation that results in a prosecution.

12. Include ongoing reporting and assessment requirements.

Law enforcement's use of surveillance technologies, particular ones as powerful as AIR, must be operated transparently and with public input. Adopting a clear, front-end regulatory structure like the one outlined here substantially furthers these goals. But transparency is not a one-time event. A regulatory framework should include ongoing reporting requirements.

In stark contrast to the 2016 version of the AIR Program, the 2020 AIR Program has implemented an impressive degree of ongoing reporting and assessment. The existence of outside evaluators—RAND to report on weekly usage and study efficacy, University of Baltimore to assess community sentiment, Morgan State University to conduct community focus groups and a quantitative analysis of AIR's impact, and the Policing Project to assess civil rights and civil liberties impact—has required PSS and BPD to be more open about how they are using the program.

A regulatory framework could require similar outside transparency on an ongoing basis, revealing information such as the number and nature of investigations opened, whether AIR was successful in identifying involved individuals, and the like.

[59] See Justin Fenton, *Baltimore Police Department Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html (noting that BPD concealed its use of cell-site simulators from prosecutors and judges in thousands of cases between 2007 and 2015).

13. Apply strict auditing procedures.

Limitations such as we are discussing are only meaningful if police and PSS abide by them. For this reason, recordkeeping and auditing procedures are essential. Policymakers might consider requiring that every request for AIR support be made in writing, accompanied by a signed and sworn statement from the requesting officer specifying the target crime at issue and the factual basis for the investigation. Policymakers then could include after-the-fact auditing and public reporting provisions to verify that every use of AIR related to a proper predicate offense. *See, e.g.*, 18 U.S.C. § 2519(3) (requiring annual reporting to Congress regarding uses of federal Wiretap Act).

14. Consequences for violations of these principles.

The regulatory framework here is intended to ensure AIR follows strict rules in an effort to limit any inappropriate impacts. But rules like these are feckless in the absence of consequences for those who violate them, particularly if done knowingly. Anyone involved in a program like AIR should receive careful training as to those rules. And any regulatory structure should involve consequences for violating those rules. There are a range of options here, from exclusion of evidence to statutory damages. In cases of serious violations, a court might be given the power to enjoin the program. Whatever the case, such remedies for violations should be sufficient to ensure they do not occur in the first place.

Appendix A

Policing Project Evaluative Framework for Responsible Use of Policing Technologies

New technologies promise to make policing safer and more effective. But there is widespread concern about these technologies, including invasions of privacy, inaccuracy, and perpetuation of racial bias. Too often, adoption of new policing technology is debated as a matter of being "for" or "against" it. We believe the better approach is to figure out if society can benefit from a particular technology. Then, if there are benefits to be had, the question becomes whether it is possible to minimize or eliminate any harm. (Some harms, like constitutional violations, are impermissible in any degree.) We also believe it is essential that any decision to use technology has democratic legitimacy. We evaluate policing technologies using this framework:

Potential Benefits. Any analysis necessarily begins by asking about the assumed benefits of the technology. Particularly when use of a technology has attendant social (and hard) costs, it is important to identify the specific problem the technology is designed to address or solve, or social improvement it is intended to bring.[60] We do so in the following stages:

1. **Specify the Problem & the Benefit:**

- What is the specific problem(s) the tech is intended to solve?
- How important/what is the magnitude of the problem the tech expect to solve?

2. **Evaluate Certainty of the Benefit:**

- How certain is it that the technology will address the problem?
- Have there been evaluations (either internal or external)?
- Are there product performance concerns that might limit effectiveness?
- If the tech succeeds in addressing the problem, will benefits be evenly distributed, or do they favor one segment of society over another?
- What countermeasures might individuals take in response to the adoption of this tool, and how much would such countermeasures reduce the expected benefits?

3. **Evaluate Unintended or Secondary Benefits:**

- Minimize criminalization of low-level offenses?
- Additional control and protection of personal data?
- Mitigation of racial and/or identity bias?
- Improved transparency or public trust?
- Better compliance with U.S. constitutional requirements?
- Other societal benefits?

[60] "Problem," here, might be a law enforcement problem (e.g., improving law enforcement methods), it might be a social problem, or it might be a problem relating to the internal operations of a police department. It is important, when framing the problem as a "law enforcement" problem, to be able to articulate the public safety goal that would be addressed through the use of technology, rather than considering "law enforcement needs" as an end in itself.

Potential Costs. Only if a technology has identifiable, concrete benefits should one turn to considering potential costs, including attendant social costs.[61] To facilitate this technology-specific evaluation, we evaluate a number of criteria that often arise in the case of new policing technologies.

4. Transparency.

- **With the Public:** Do members of the public know about and/or consent to this information capture? Does the company itself make the public aware of where and how its product operates? How does the company's public description of its capabilities compare to actual capabilities? How does the company's public description of benefits compare with to actual benefits? How open is the company in dealing with the public and media?

- **Public Clients of Technology Companies**: How and to what extent are customers prevented, permitted, encouraged, or required to inform or engage with the public about the customer's decision to acquire or use the technology? To share information about the nature of the product or data it generates?

5. Personal Information Privacy.

- **Data capture:** What information can or does the tech capture, measure, collect, or use? Is all of this data relevant and necessary to accomplish the purpose of the technology? From whom is this data collected?
- **Data aggregation and mining:** Does the tech aggregate data and if so, how? Is the data stored in an anonymized fashion? Does the system analyze data to identify previously unknown facts or patterns (aka data mining)?
- **Data retention:** Is data retained by the company or the customer? What are the guidelines/limits for doing so? How long is data retained? Can individuals request access to or deletion of their personal data?
- **Data ownership and sharing:** Who owns the data collected? Who has access to that data? Does the company use any third-party data processors and for what purpose? Can customers share data with a third party? Does the company or the customer sell or otherwise monetize data?
- **Data control and security:** How/where is data stored? Is personally identifiable information separately stored and or encrypted? What are the physical, technical, and administrative protocols for data storage and access? Are there built-in audit trails to determine what type of data is collected and/or accessed by an end user? What are the protocols in place for a data breach? Will those whose data is acquired by notified? Is there risk of physical harm to individuals or locales in the event of a security breach?
- **Compliance:** How does the vendor monitor compliance with data policies?

6. Racial or Other Identity Disparities.

- **Disparities in design** (e.g., whether the technology itself has any inherent bias, including algorithmic bias relating to personal identity, for example, by employing unrepresentative training data or exhibiting algorithmic bias)?

[61] Any true benefit-cost analysis must take into account hard costs, including but not limited to long-term retention and data storage costs. Although these types of costs are an important consideration both to police departments and their communities, we focus here on ethical considerations, not financial ones.

- **Disparities in operation** (e.g., whether the technology might be deployed or used in ways that create or exacerbate identity bias and/or disparities)?

7. Increased Criminalization. Will use of the tech lead to more people being stopped, ticketed, arrested, or incarcerated? If so, for what type of crimes? Is enforcement of these crimes a net contribution to society or a net harm (i.e. are you contributing to low-level criminalization)?

8. Evidentiary Risk. Does the tech produce evidence to be used at trial? Under what circumstances? Does it meet chain-of-evidence, Daubert, and other rules of evidence? Are there protocols in place to ensure all necessary information is turned over to prosecutors and the defense?

9. Constitutional Risks. To the extent not already discussed, does use of the technology risk directly or indirectly violating constitutional rights, including but not limited to:

- 1st Amendment (speech, press, religion, assembly, association, petition)
- 2nd Amendment (right to bear arms)
- 4th Amendment (searches, seizures, excessive force)
- 5th Amendment (self-incrimination, Brady & impeachment evidence, due process)
- 6th Amendment (right to counsel, speedy/public trial, cross-examine witnesses)
- 8th Amendment (cruel & unusual punishment, excessive bail, excessive fines/fees)
- 14th Amendment (equal protection)

10. Other Potential Social Costs. Are there other potential social costs that have not yet been considered, including but not limited to:

- Whether there might be a unique impact on any specific subgroup (e.g., youth, LGBTQ communities, particular religious groups, socioeconomically disadvantaged communities)?
- Whether there are historic considerations that may make particular communities distrustful of this technology?
- The potential for mission creep (either over time or in response to critical events)?
- The impact of how others in the industry will respond?
- Global/international human rights impact?

11. Less Costly Technologies? Once the social and other costs are identified, unless it is all benefit and no cost, there is one important last question: Are there alternative means of addressing the problem or providing the social benefit that are less costly, less-invasive, or avoid the costs identified here?

Operational Concerns. In additional to considering potential costs and benefits, there are several categories of operational concerns that one must always keep in mind thinking through the potential impact of new policing technologies:

12. Tactical Impact: How will the product impact the performance of police officers? Will these changes create additional risks for officers or for the public?

13. Integration Risks. Can the tech freely integrate with other tech, and how might such integrations impact the risks discussed above? Can it be augmented with outside software (e.g., adding face recognition to CCTV or body-worn cameras)?

14. Intended Use vs. Actual Use. Can the product be used differently than originally intended? Does this different downstream use present additional risks to consider? What are the vendor's terms-of-use and do they adequately limit how the tech can be used? Other than terms of use, what policies, procedures, or design features exist to limit, monitor, or audit downstream use or misuse?

15. Internal Policies & Procedures. Has the agency implemented a use policy? What internal policies and protocols are in place to ensure the product is used in the manner described above?

16. Training. What type of training do analysts, officers, and supervisors receive? Does the vendor provide on-going training and/or support?

Appendix B

Analysis of Factual Assumptions in Fourth Circuit Panel Opinion

Our view of the constitutional issues presented by AIR differs from the Fourth Circuit majority opinion in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, No. 20-1495, 979 F.3d 219, 2020 WL 6500931 (4th Cir. 2020). But we want to stress one reason in particular: that court may not have been clear about the facts. As detailed in our *amicus* brief, the Fourth Circuit's factual misunderstandings likely were due to the procedural posture of the case, as well as other factors outside of our control. We view it as regrettable that a potentially important constitutional decision—one whose reasoning may in the future be applied beyond AIR—was handed down on an incomplete and inaccurate record.

Without attempting to be comprehensive, here are some errors of fact (or lack of clarity about the facts) in the Fourth Circuit decision:

- The Fourth Circuit states that "[a]n individual will not have his public movements tracked unless he happens to be at the scene of one of these violent crimes." *Id.* at *7. Supplemental Requests go further. AIR has been used not only to track individuals traveling to or from a crime scene, but individuals traveling to or from other locations, such as a private home. AIR also has been used to track individuals who were not present a crime scene, but who interacted with someone who was.
- The Fourth Circuit assumes, consistent with the MOU, that aerial photographs only will be retained for 45 days, *id.* at *8, when in fact, as we detail in Part II, AIR imagery is being held in perpetuity for a substantial majority of the days AIR operated.
- The Fourth Circuit concludes that "[b]ecause they do not fly at night, AIR surveillance cannot be used to track individuals day-to-day." *Id.* at *5; *see also id.* at *6 ("[w]hereas CSLI could be used to reliably track an individual's movement day to day, AIR can only be used to track someone's outdoor movements for twelve hours at most."). In fact, the program is not so limited; as we explain in Part II, AIR has been used for multi-day tracks.
- The Fourth Circuit stated that unlike cell-site location tracking, which "is used by law enforcement to learn detailed information about someone it is already monitoring," "AIR is used to identify suspects and witnesses to crimes; it takes no deep dive into an individual's life and in fact can tell the police very little about an identified person." *Id.* at *6. Again, there is a discrepancy between what PSS and BPD told the public and what is happening under the Supplemental Requests procedure. At the least, AIR was used to track the movements of already-identified individuals just like CSLI and perhaps more reliably in some instances (depending on cell-site coverage). And because AIR can be used to track not only suspects but also people they meet, in some instances it may capture more information than CSLI. This will vary case to case, of course.
- Repeatedly the Fourth Circuit says that the AIR analysts can access the aerial photographs only when specific violent crimes occur. *E.g.*, *id.* at *1 ("The control room can access the photographs only when specific violent crimes — shootings, robberies, and carjackings — are reported in a particular location."), *2, *7. But in fact, PSS can access aerial material any time it wishes, and can access ground surveillance any time BPD grants access. The opinion makes it seem that there is some technological control in place regarding access to data, when the only actual limit is whether or not PSS and BPD adhere to the MOU.

Appendix C

Additional Information regarding AIR Program Operations

Additional Information Regarding PSS's Aerial Cameras

AIR Program planes are to fly between 3,000 to 12,000 feet above the ground, below cloud cover, and cannot fly in inclement weather. During the pilot program each plane was to fly over the City of Baltimore during daylight hours for a minimum of 40 hours per week, in approximately six-hour intervals before refueling. Generally, in order to minimize noise complaints, PSS did not operate below 4,500 feet above sea level.

PSS's aerial surveillance system is comprised of several hardware and software components. Single engine airplanes are mounted with one of PSS's proprietary camera systems—either the HawkEye II or HawkEye III. Both feature an array of ultra-high-definition cameras (twelve for the HawkEye II, sixteen for the HawkEye III), which are pointed at varying angles to the ground, allowing each plane to survey an approximately 32-square-mile area.

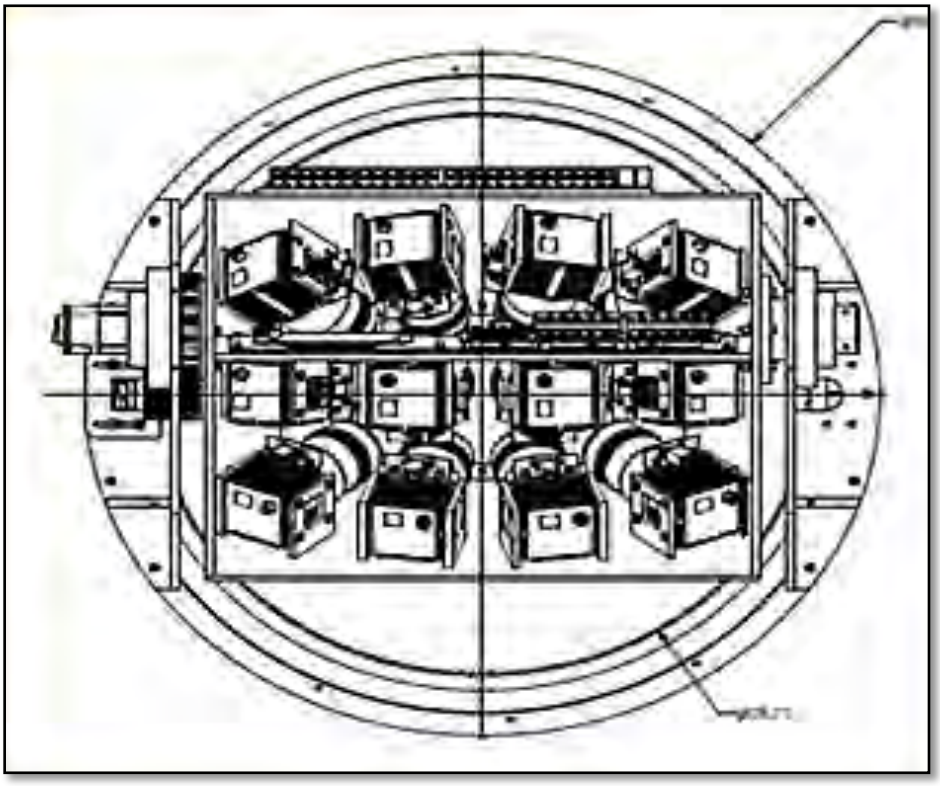

Fig. 4—Diagram, HawkEye II 12-camera array: The HawkEye II Wide Area Motion Imagery aerial surveillance system combines hardware and software components to create seamless large format images of the area under surveillance. The system contains an array of twelve 16-megapixel full-color cameras and inertial measurement unit, with each camera composed of industrial imaging elements and lenses, and proprietary PSS circuitry, assembled by PSS. Each of the HawkEye III's sixteen cameras contains a 31-megapixel sensor.

Once images are taken, proprietary software captures and merges each individual camera's images into a large, contiguous image of the area below the plane, and aligns the image onto a map of the city. Using CamLink, a proprietary PSS software, the images captured by each of the twelve cameras are stitched together into a seamless whole by a computer onboard each airplane, which also corrects various lens, topographic, and camera-tilt distortions through a process called orthorectification. The software takes the stitched-together image projections and overlays them onto a map aligned to the city street grid.

These processed image files then are transmitted wirelessly and stored on PSS computers in its analyst center in Baltimore. Once images are captured and processed by the onboard computer, they are transmitted via a proprietary high-speed air-to-land system ground connection, PSS DownLink and PSS GroundControl, to ground stations located on the roofs of the East and West District Police Headquarters, and then sent to the PSS analysis center. Though the raw images captured by the cameras are each in excess of 500 mb in size, the images are processed and compressed to approximately 60 mb prior to transmission. Raw images—meaning unprocessed image sensor output—is only ever saved for plane calibration flights. Such images are available only to the flight system operator and camera installation crew—not to PSS analysts or BPD—and are destroyed after calibration is confirmed, or within five days, whichever comes first. Furthermore, PSS states that its raw image data "is not significantly higher resolution then [sic] the processed imagery." We have not reviewed any raw image data. The process takes 3–5 seconds, providing analysts with near real-time images at a rate of 3600 images per plane per hour.

HawkEye II images have a maximum resolution of approximately 268 million full-color pixels. The HawkEye III is a more powerful and sensitive camera system than the HawkEye II, with a maximum resolution of approximately 604 million full-color pixels. According to PSS, the gain in pixels in the HawkEye III system will be used to surveil a greater coverage area—not the same coverage area in greater detail. At the time of this writing, the plane mounted with the HawkEye III is not yet operational—therefore we cannot evaluate the appearance or level of detail in HawkEye III images as compared to the HawkEye II images.

Both PSS and BPD have described the AIR Program's aerial surveillance image resolution as "one pixel = one person." Practically speaking, most people appear as one to a few colored pixels. This is because, under normal conditions, both the camera systems are calibrated to have one pixel represent approximately 1.45 square feet on the ground, though variations in flight altitude may impact the actual resolution. The theoretical maximum resolution of these systems, hard-limited by the software, is equal to approximately one pixel representing slightly less than 1.0 square feet.[62]

Because different cameras in the Hawkeye systems capture images at more acute angles than others, the areas directly below the plane are generally of minimally higher resolution than the far edge of the surveillance area. The areas immediately below the planes also offer a more direct viewing angle of the streets below, minimizing vertical obstructions like buildings and trees. Greater viewing angles expose more vertical surface area of a person or vehicle to the camera, however, increasing pixel counts per subject.

[62] PSS's website describes the HawkEye II's image resolution as "1/2 meter resolution throughout" its coverage area. *See HawkEye II Resolution*, Persistent Surveillance Systems. PSS has set a hard-coded field of view limit into its CamLink software for the HawkEye II camera system, which cannot be set below a 3 x 3 mile coverage zone, resulting in a theoretical maximum resolution cap of just under one square foot per pixel. Normally, however, the HawkEye II system uses a 4.5 x 4.5 mile coverage zone when flying at low altitudes, leading to a theoretical maximum resolution of 1.45 square feet per pixel. PSS has shared, however, that sensor limitations, physical interference, and atmospheric interference mean that "true ground resolution will not reach this maxima, even at low altitudes." As with the HawkEye II, the AIR Project will hard-code a 4.6 x 4.6 mile resolution limit into the HawkEye III image processing, resulting in a maximum ground resolution of approximately one square foot per pixel.

Absent movement, it may be difficult to distinguish a person from an inanimate object, such as a bush. Because the images are chronological, however, analysts are quickly able to pick out movement between image frames, and thus identify people. Although this level of resolution is minimal, one might be able to discern certain characteristics about a person based on these pixels alone. PSS informs us that there have been no circumstances where any analyst has been able to determine someone's skin color based upon the current technology. In one homicide however, a person's clothing appeared lighter than the asphalt and later in the homicide appeared darker than the asphalt. Later in ground camera images, analysts were able to determine the suspect changed out of his light clothing worn prior to the homicide into darker clothing worn after the homicide. Additionally, PSS states a person's relative position to the cameras—standing erect, running, or laying down—potentially could affect how much an analyst might be able to observe about their characteristics.

Vehicles are represented by approximately 15–20 pixels, meaning analysts not only are able to determine a vehicle's color, but also general body-type, the direction the vehicle is facing, and other distinguishing characteristics on occasion, such as a sun-roof. For example, we've been told analysts can often distinguish law enforcement and other emergency response vehicles from the aerial imagery alone by their actions at the scene and certain distinguishable characteristics like vehicle size. Furthermore, analysts can determine if a person enters or exits a driver or passenger side door of a vehicle based on the direction the vehicle is facing.

Because of agreed upon limitations requested by BPD, PSS did not fly its planes at night, and therefore did not produce nighttime imagery. Its cameras are not equipped with infrared, night-vision, nor thermal imaging components. However, the HawkEye II camera sensor is sensitive enough to track subjects through the city using ambient light; the HawkEye III system is 70-times more sensitive to light, increasing its low-light tracking capabilities. Though it has not occurred during the AIR Program, PSS has stated that in previous iterations of the program analysts have been able to track vehicles at night based on their headlights and taillights alone.

Additional Information about PSS Analysts and Trackers

PSS employs approximately 25–30 trackers and analysts for the AIR Program. The majority of analysts were hired from the Baltimore area, although several senior analysts were brought in from PSS's headquarters in Dayton, OH, to support operations and train new hires. Trackers earn approximately $12–17 dollars per hour; analysts earn approximately $17–30 per hour. Dr. McNutt stated that PSS has trained approximately 150 analysts who went on to work for the Department of Defense, either at Fort Meade, Aberdeen Proving Grounds, or at the National Air and Space Intelligence Center (NASIC) in Dayton, Ohio.

Trackers are responsible for tracking either individuals ("subjects") or vehicles from image to image, second by second. They do so by zooming in on a location on an aerial surveillance image and clicking their mouse cursor over the subject they hope to track. PSS's iView tracking software also includes tools that allow analysts to alter image attributes (contrast, sharpness, and color) to aid in tracking.

Once clicked, the video advances (either backward or forward) one frame, and they repeat the process. Additionally, trackers make notes of tracked subject's behaviors, such as "subject runs to X" or "subject parks near X." They also may brief BPD personnel orally on their investigations. Several trackers may work a single investigation, and all of their tracks and notes are saved into an investigation folder as "track files."

Trackers complete about 70 hours of formal instruction and practical training on PSS's mission, policies, investigatory protocols, software, and on how to construct and present briefings. According to Dr. McNutt,

once trackers have demonstrated to PSS trainers' satisfaction that they have the "ability to show sound analysis in tracking, clearly articulate investigative findings and narrative, communicate information and briefs orally, and maintain unbiased and factual reporting" they are awarded a PSS certification and allowed to begin work on active investigations.

Analysts are high-level trackers who have demonstrated proficiency in tracking and analysis, and are charged with analyzing subject tracks to determine which ones might either be a person or vehicle of interest to the investigation, or a subject who does not appear to be involved and should be excluded from an investigation. They make these determinations by observing what they believe to be significant subject behaviors, such as when an individual ran from the scene of a crime, or got into a driver or passenger side of a vehicle which drove away quickly. They note when vehicles swerved through traffic, run stop signs or red lights, took wrong turns down one-way streets, took indirect routes or side streets, or other unusual driving behaviors. Other observations may include "scouting" the scene of a crime before it was committed, or driving in an apparently coordinated manner with other vehicles, such as when two subject tracks meet before a crime occurred, separated, and came together again after the crime. Notes of such behaviors are saved along with tracks into PSS investigation files.

The 2016 AIR Program

We have some information about the 2016 operations, though it was not the focus of our audit. PSS completed 314 hours of surveillance missions in this trial, spanning from January 15 to August 18, 2016. During the operations, PSS conducted over 1,800 hours of analysis of this imagery, and created over ninety investigative briefings on various crimes, including murders, shootings, stabbings, rapes, robberies and burglaries, as well as lower-level crimes including hit and runs, illegal dumping, and illegal motorcycle and dirt bike riding. PSS integrated existing BPD technology into its analysis center, including the city's CitiWatch CCTV cameras, ShotSpotter gunshot detection microphones, and computer-aided dispatch system, and wrote software to map calls for service onto the surveillance images at the correct times. BPD directed PSS to maintain all the data it collected in the 2016 trial, and PSS continues to retain all of that data to this day because BPD has not rescinded its directive.

For more information about the 2016 program, see NAT'L POLICE FOUND., A REVIEW OF THE BALTIMORE POLICE DEPARTMENT'S USE OF PERSISTENT SURVEILLANCE (2017).