BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS

Brennan Center for Justice
at New York University School of Law

120 Broadway
Suite 1750
New York, New York 10271
646.292.8310 Fax 212.463.7308
www.brennancenter.org

February 20, 2018

Written Testimony of Michael Price, Senior Counsel
Brennan Center for Justice at New York University Law School
Before the
Maryland House of Delegates
Judiciary Committee
In Support of HB 578

Good afternoon, Chairman Vallario, Vice-Chair Dumais, and members of the Judiciary Committee. My name is Michael Price and I am Senior Counsel for the Brennan Center for Justice at NYU School of Law in the Liberty and National Security Program. Thank you for holding this hearing and inviting the Brennan Center to testify in support of HB 578, establishing a Task Force to Study Law Enforcement Surveillance Technologies. And thank you to Representative Charles Sydnor for sponsoring this important initiative once again.

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Liberty and National Security Program focuses on helping to safeguard our constitutional ideals in the fight against terrorism. As a part of that work, we advocate for greater transparency and oversight of state and local surveillance activities in order to prevent abuses, promote public safety, and rebuild a growing deficit in public trust.

In recent years, the Brennan Center has published a series reports and law review articles on police surveillance practices and the need for reform.[1] We helped create an Inspector General for the New York City Police Department (NYPD) in 2013, following the department's well-documented and unconstitutional surveillance of Muslim communities. And we continue to support state and local legislation – in New York, in Maryland, and throughout the country – to address concerns about police use of powerful new surveillance technologies. Many of these tools pose profound problems for civil rights and civil liberties that must be addressed by policymakers in consultation with the public.

---

[1] See, e.g., MICHAEL PRICE, NATIONAL SECURITY AND LOCAL POLICE (2013); FAIZA PATEL & ANDREW SULLIVAN, A PROPOSAL FOR AN NYPD INSPECTOR GENERAL (2012); Michael Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247 (2016); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017).

That is why the Brennan Center is here today to support HB 578, to create a Task Force to Study Law Enforcement Surveillance Technologies.

Over the past 15 years, state and local law enforcement agencies have acquired a startling array of powerful new surveillance technologies, often without public notice, debate, or oversight from elected lawmakers. Much of this technology was designed for the battlefields of Iraq and Afghanistan and acquired through federal grant programs or private funding. As a result, state and local legislatures have been left out of important decisions about policing. It is critical for legislatures to catch up, to take stock of the surveillance technologies now in use, to ask whether they comport with our constitutional values, and to ensure sufficient safeguards for civil rights and civil liberties.

Persistent Aerial Surveillance

In Baltimore, the police department partnered with a private company from Ohio, "Persistent Surveillance Systems," to fly eight months of reconnaissance over the city, continuously recording everything within 30 square miles. The technology was originally developed for the military in Iraq, capable of casting "an unblinking eye on an entire city."[2] And despite public concern about aerial surveillance at protests over the death of Freddie Gray,[3] the program was not disclosed to public, the Baltimore City Council, or the mayor until it had been in operation for months. The governor, the state's attorney, and members of this body were likewise uninformed until media reports surfaced.[4] In fact, the program was privately-financed by a Texas philanthropist,[5] effectively short-circuiting normal democratic checks and balances.

"Stingrays" (Cell Site Simulators)

Police in Baltimore and throughout the state secretly acquired portable, fake cell phone towers, commonly called "Stingrays," designed to collect private data about the location

---

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

[3] *FBI behind mysterious surveillance flights over Baltimore, other U.S. cities*, BALTIMORE SUN (Jun. 2, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bal-fbi-behind-mysterious-surveillance-flights-over-baltimore-other-us-cities-20150602-story.html.

[4] Yvonne Wenger, *Few in City Hall knew about Baltimore police surveillance program*, BALTIMORE SUN (Sept. 9, 2016), http://www.baltimoresun.com/news/maryland/investigations/bs-md-sun-investigates-who-knew-20160902-story.html.

[5] Doug Donovan, *Billionaire donors Laura and John Arnold support far more in Maryland than police surveillance*, BALTIMORE SUN (Aug. 26, 2016), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-arnolds-20160826-story.html.

of all nearby cell phones.[6] Stingrays are suitcase-sized devices, originally designed for military use. They mimic cell phone towers and trick all phones in the area into connecting to the police instead of the phone company. As a condition of purchase, state and local agencies signed nondisclosure agreements with the FBI promising to keep the Stingray technology a secret, even in court documents and judicial proceedings.[7]

The consequences of that secrecy are now likely familiar. In *State v. Andrews*, decided by the Maryland Court of Special Appeals in 2016, Baltimore police did not seek a warrant or even mention to a judge the Stingray technology (called a "Hailstorm" in this instance) when investigating an attempted murder. Instead, they asked the judge to approve a "pen register/trap and trace" device, which does not require a warrant and does not involve location information.[8] The appeals court chastised the police, called the application misleading, and forcefully affirmed that people have a legitimate expectation of privacy in their cell phone location information.[9] The court held that police must get a warrant supported by probable cause in order to use a Stingray or similar device, suppressing evidence in the *Andrews* case and jeopardizing hundreds of other convictions.[10]

Facial Recognition Technology

Finally, Maryland police continue to use facial recognition technology to identify and track individuals whose images have been recorded by security cameras or posted on social media. According to a Georgetown University report, Maryland has been one of the most aggressive adopters of facial recognition technology, adding all driver's license photos to its mug shot database and sharing those records with the FBI.[11] Baltimore

---

[6] Courtney Mabeus, *Md. Police mum on growing use of cellphone tracking technology*, Capital News Service (May 4, 2016), https://wtop.com/maryland/2016/05/md-police-mum-on-growing-use-of-cellphone-tracking-technology/.

[7] *See State v. Andrews*, 227 Md. App. 350, 374-75 (2016).

[8] *Andrews*, 227 Md. App. at 375.

[9] *Andrews*, 227 Md. App. at 394–95 ("We determine that cell phone users have an objectively reasonable expectation that their cell phones will not be used as real-time tracking devices through the direct and active interference of law enforcement. We hold, therefore, that the use of a cell site simulator, such as Hailstorm, by the government, requires a search warrant based on probable cause and describing with particularity the object and manner of the search, unless an established exception to the warrant requirement applies.").

[10] Baynard Woods, *Stingray ruling could challenge hundreds of Baltimore convictions*, The Guardian (Apr. 5, 2016), https://www.theguardian.com/us-news/2016/apr/05/maryland-stingray-ruling-baltimore-convictions-privacy; *but see State v. Copes*, 454 Md. 581, 618 (2017) (declining to suppress evidence obtained by warrantless use of a cell cite simulator two years prior to the *Andrews* decision).

[11] Clare Garvie et al., *The Perpetual Lineup: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology at 4, 136 (Oct. 2016), https://www.perpetuallineup.org/; Kevin Rector & Alison Knezevich, *Maryland's use of facial recognition software questioned by researchers, civil liberties advocates*,

police reportedly used this system to monitor protesters after the death of Freddie Gray. Facial recognition allowed officers to arrest individuals with outstanding warrants "directly from the crowd" based on social media photos of the protests.[12]

Using facial recognition technology in this manner raises significant constitutional concerns. It has a chilling effect on freedom of speech and freedom of association. It invades personal privacy by subjecting residents to a "perpetual lineup."[13] And it raises a host of troubling questions about whether police are using technology in a discriminatory fashion, focusing only on particular protests and communities of color.

Facial recognition technology is evolving rapidly and could be adapted for real-time use in conjunction with existing surveillance cameras like Baltimore's CitiWatch network. It is also possible to use facial recognition with police body-worn cameras; Baltimore's current policy permits facial recognition on stored footage when analyzing a "specific incident" and is silent on real-time recognition,[14] raising the concern that body cameras designed for police accountability will turn into powerful new surveillance devices.

* * *

Now is the time for Maryland lawmakers to address these concerns in a systematic and forward-looking way. The Brennan Center therefore commends the legislature for considering HB 578. The bill creates a Task Force that would be empowered to assess police use of new technologies like aerial surveillance, Stingrays, and facial recognition. But it would also provide much needed transparency and accountability for other troubling types of surveillance technologies, including drones, automatic license plate readers (ALPRs), social media monitoring software.

Law enforcement may prefer not to discuss the surveillance tools they use, but a democratic society requires at least a basic level of information about what its police are doing and how they're doing it. History shows that the public will inevitably find out, through costly freedom of information litigation, through the press, or through the courts, as in *Andrews*. But reacting to one scandalous headline after another is not effective oversight. It is better to have transparency up-front, to have an informed conversation with policymakers and community stakeholders about the rules of the road *before* the police deploy new technologies. Such a proactive approach would also encourage agencies to be thoughtful in crafting policies that do not harm individual rights, undermine their relationships with communities, or waste scarce resources.

BALTIMORE SUN (Oct. 18, 2016), http://www.baltimoresun.com/news/maryland/crime/bs-md-facial-recognition-20161017-story.html.

[12] *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, Geofedia (n.d.), https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

[13] Garvie et al., *The Perpetual Lineup*.

[14] Baltimore Police Dept., Policy 824: Body Worn Camera (Jan. 1, 2018), 9, https://www.baltimorepolice.org/sites/default/files/Policies/824_Body_Worn_Cameras.pdf (accessed Feb. 19, 2018).

This is a common sense idea embraced by law enforcement leaders. In 2015, President Obama's Task Force on 21st Century Policing specifically recommended that state and local law enforcement agencies "encourage public engagement and collaboration … when developing a policy for the use of a new technology."[15] According to the final report: "Local residents will be more accepting of and respond more positively to technology when they have been informed of new developments and their input has been encouraged. How police use technology and how they share that information with the public is critical."[16] Task Force co-chair Charles Ramsey also recognized that, "Just having the conversation can increase trust and legitimacy and help departments make better decisions."[17]

In fact, the federal government routinely discloses its ground rules for using new technologies. For example, both the Department of Justice[18] and the Department of Homeland Security[19](DHS) have published policies on their use of Stingrays, requiring agents to obtain a judicial warrant and apply important back-end privacy protections. DHS has also issued Privacy Impact Assessments for use of facial recognition technology[20] and license plate reader data;[21] and issued guidance for state and local

---

[15] President's Task Force on 21st Century Policing, *Final Report of the President's Task Force on 21st Century Policing* (Washington, DC: Office of Community Oriented Policing Services, 2015), 35, https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.

[16] Ibid.

[17] Ibid; *see also Privacy impact assessment report for the utilization of license plate readers* (Alexandria, VA: International Association of Chiefs of Police, 2009), 28, http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. (recognizing that "[o]ne way to promote public confidence is to increase the transparency surrounding how [license plate reader] data will be managed by the law enforcement agency.").

[18] U.S. Department of Justice, *Department of Justice Policy Guidance: Use of Cell-site Simulator Technology*, https://www.justice.gov/opa/file/767321/download (accessed Feb. 19, 2018).

[19] Alejandro N. Mayorkas, Memorandum to Sarah Saldana, et al., "Department Policy Regarding the Use of Cell-Site Simulator Technology," October 19, 2015, https://www.dhs.gov/sites/default/files/publications/Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf.

[20] U.S. Department of Homeland Security, U.S. Customs and Border Protection, *Privacy Impact Assessment for the Facial Recognition Air Entry Pilot*, DHS/CBP/PIA-025 (March 11, 2015), https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp-1-to-1-facial-recognition-air-entry-pilot-march-11-2015.pdf (accessed Feb. 19, 2018).

[21] U.S. Department of Homeland Security, U.S. Immigrations and Customs Enforcement, *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data from a Commercial Service*, DHS/ICE/PIA-039 (March 19, 2015) https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf (accessed Feb. 19, 2018).

agencies using drones, which strongly recommended transparency and public outreach.[22] If the two federal agencies responsible for protecting our domestic national security can provide this type of information to the general public, then Maryland law enforcement could surely do so as well.

HB 578 will inform the public – and critically, members of this body – about new surveillance technologies with profound implications for privacy, civil rights, and civil liberties. Americans all want be safe, but new surveillance technologies do not just capture information about the "bad guys." They affect the rights of everyone, but especially – and disproportionately – communities of color. Without some basic information about what these technologies do and how law enforcement agencies are using them, lawmakers cannot oversee law enforcement or do their jobs effectively.

Transparency and oversight are essential features of a strong democracy, and the Brennan Center commends the Judiciary Committee and the House of Delegates for taking up this critical and timely issue. The Brennan Center strongly supports HB 578 and we encourage the legislature to pass it quickly.

Thank you again for the opportunity to testify today. I am happy to answer any questions.

[22] U.S. Department of Homeland Security, Privacy, Civil Rights & Civil Liberties Unmanned Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Systems Programs* (December 18, 2015), https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf (accessed Feb. 19, 2018).