AMERICA UNDER WATCH

FACE SURVEILLANCE IN THE UNITED STATES

GEORGETOWN LAW
Center on Privacy & Technology

www.americaunderwatch.com

MAY 16, 2019

AMERICA UNDER WATCH

FACE SURVEILLANCE IN THE UNITED STATES

GEORGETOWN LAW
Center on Privacy & Technology

Clare Garvie, *Senior Associate*
Laura Moy, *Executive Director*

DESIGN
Rootid

www.americaunderwatch.com

MAY 16, 2019

TABLE OF CONTENTS

I. INTRODUCTION

"Real-time video surveillance appears to be a simple question of supply and demand. As the technology improves, we anticipate that real-time face recognition systems will become commonplace."[1]

—*The Perpetual Line-Up, 2016*

Figure 1: Surveillance cameras in Beijing, China. (Source: Louis Constant/Shutterstock, all rights reserved.)

Authorities in Guiyang have eyes everywhere. Thanks to a vast, sophisticated camera system blanketing this Southwest Chinese city, police are purportedly able to locate and identify anyone who shows their face in public—in a matter of minutes. They can trace where you have been over the past week. If you are a citizen they can "match your face with your car, match you with your relatives and people you're in touch with … know who you frequently meet."[2]

This is a reality made possible by real-time face surveillance. Thanks to face recognition technology, authorities are able to conduct biometric surveillance—pick you out from a crowd, identify you, trace your movements across a city with the network of cameras capturing your face—all completely in secret. No longer is video surveillance limited to recording what happens; it may now identify who is where, doing what, at any point in time.

It's tempting to think that it is a remote, future concern for the United States. But for the millions of people living in Detroit and Chicago, face surveillance may be an imminent reality. Detroit's million-dollar system affords police the ability to scan live video from cameras located at businesses, health clinics, schools, and apartment buildings. Chicago police insist that they do not use face surveillance, but the city nonetheless has paid to acquire and maintain the capability for years.

For millions of others in New York City, Orlando, and Washington, D.C., face surveillance is also on the horizon. And for the rest of the country, there are no practical restrictions against the deployment of face surveillance by federal, state, or local law enforcement.

For the millions of Americans living in Detroit and Chicago, face surveillance may be an imminent reality.

There is no current analog for the kind of police surveillance made possible by pervasive, video-based face recognition technology. By enabling the secret and mass identification of anyone enrolled in a police—or other government—database, it risks fundamentally changing the nature of our public spaces.

Free Speech. When used on public gatherings, face surveillance may have a chilling effect on our First Amendment rights to unabridged free speech and peaceful assembly. This is something law enforcement agencies themselves have recognized, cautioning: "The public could consider the use of facial recognition in the field as a form of surveillance …. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."[3]

Privacy. Supreme Court Chief Justice John Roberts wrote for the majority in *Carpenter v. United States*: "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."[4] The Court, examining police use of historic cell-site location information, noted that for the government to "secretly monitor and catalogue every single movement" of someone across time unconstitutionally violated society's expectations about what law enforcement can and should be able to do.[5]

Face surveillance technology can facilitate precisely this type of tracking, locating where someone is and has been by the location of the camera that captures that person's face. If mounted on churches, health clinics, community centers, and schools, face surveillance cameras risk revealing a person's "familial, political, professional, religious, and sexual associations," the very "privacies of life" that the Supreme Court in *Carpenter* suggested receive protection under the U.S. Constitution.[6]

Bias. The risks of face surveillance are likely to be borne disproportionately by communities of color. African Americans are simultaneously more likely to be enrolled in face recognition databases and the targets of police surveillance use.[7] Compounding this, studies continue to show that face recognition performs differently depending on the age, gender, and race of the person being searched.[8] This creates the risk that African Americans will disproportionately bear the harms of face recognition misidentification.

II. DETROIT'S "REAL TIME VIDEO FEED FACIAL RECOGNITION"

A sign on the side of Summit Medical Center designates it as a Green Light Partner with the Detroit Police Department (DPD). It informs the public that this women's health care clinic is monitored by video cameras whose feeds are viewed down at DPD headquarters.[9]

This sign, and ones just like it at more than 500 locations across Detroit, is meant to deter crime and make residents feel safe, informing the public that the area is being watched.[10]

What the signs do not say is that many of these video cameras may also be connected to a face surveillance system, enabling them to record not only what is happening at a given location, but who is at that location at any given moment. DPD has purchased the capability to locate and identify anyone who has an arrest record, in real-time, using video cameras mounted across the city.[11]

From the perspective of quickly solving the crimes that aren't deterred by the Project Green Light Signs, this may sound like a good thing. Police are able to more quickly identify repeat offenders and make arrests.

But face surveillance doesn't identify crime; it identifies people. With such a system, all people caught on camera—passersby, patrons, or patients—are scanned, their faces compared against the face recognition database on file. For patients visiting Summit Medical Center to terminate a pregnancy, receive HIV treatment, counseling, or another service, this probably sounds less like a guarantee of safety and more like an invasion into a deeply personal moment in their lives.

A. AN EXPENSIVE, EXPANDABLE FACE SURVEILLANCE SYSTEM

Detroit purchased its face surveillance system in July of 2017 as part of a three-year contract with vendor DataWorks Plus, totaling $1,045,843.20.[12] Under the contract, Detroit licensed DataWorks Plus' "FACE Watch Plus real-time video surveillance" software, a system that "provides continuous screening and monitoring of live video streams."[13]

The system is designed to operate on "not less than 100 concurrent video feeds," assuming it meets the requirements set out in Detroit's 2015 call for proposals to build the system.[14] According to the proposal, these feeds come from the cameras installed as part of Project Green Light, a public-private partnership the city launched in 2016.[15]

"DPD may connect the face recognition system to any interface that performs live video, including cameras, drone footage, and body-worn cameras."

DPD's face surveillance system may expand

Figure 2: Signs, security cameras, and a flashing green light designate Briggs Houze, an apartment building in downtown Detroit, as a Project Green Light Partner since July 2017.

beyond Project Green Light as well. The Department's face recognition policy, which went into effect on July 1, 2018, states that DPD "may connect the face recognition system to *any* interface that performs live video, including cameras, drone footage, and body-worn cameras."[16]

In addition to face surveillance, the 2016 DataWorks Plus contract also includes investigative face recognition software and an application that enables an unlimited number of DPD officers to run face recognition searches on their mobile devices. All three face recognition capabilities are configured to compare unknown faces in photo or video against Detroit's database of 500,000 mug shot photos. DPD's Crime Intelligence Unit is additionally authorized to run face recognition searches on Michigan's Statewide Network of Agency Photos (SNAP), a database that includes state driver's license photos.[17]

PROJECT GREEN LIGHT DETROIT

How the face surveillance system is designed to work

Detroit's real-time face surveillance is designed to operate together with a program called Project Green Light Detroit, an initiative launched in January 2016 that has dramatically expanded the city's network of surveillance cameras.[18] The city has pitched the initiative as a way to deter crime and improve police response times to incidents at locales across the city. Its original focus was on businesses open during late-night hours such as gas stations, fast food restaurants, and liquor stores.[19] Partner locations now also include churches, hotels, clinics, addiction treatment centers, affordable housing apartments, and schools.[20]

Under the project's public-private partnership program, businesses purchase and install high-definition indoor and outdoor video cameras that feed directly into DPD's Real Time Crime Center. In exchange, the Real Time Crime Center has dedicated staff—and advanced technology—to monitor and analyze the video feeds. The businesses also receive "special police attention," including weekly officer site visits and "Priority 1" status for police response to 911 calls.[21]

As of April 2019, more than 500 businesses, churches, apartments, and other locations were enrolled in Project Green Light.[22] Schools began to be added in April of 2018,23 and in late 2018, DPD was in discussion with the Detroit Housing Commission to expand the program to public housing locations.24 The Detroit Mayor's Office has also considered making participating in Project Green Light mandatory for businesses open later than 10pm.[25]

B. SURVEILLANCE RISKS NOT MITIGATED BY EXISTING RESTRICTIONS

The way in which Detroit's face surveillance system is set up poses risks that may not be adequately mitigated by the existing policy that governs its use. The policy recognizes some of the risks that face recognition technology poses. The policy states, for example, that officers and agencies using the system:

> "…will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law."[26]

However, because of its pairing with Project Green Light, DPD's face surveillance system runs the risk of doing just that.

Project Green Light Partners are still predominantly gas stations, liquor stores, and other late-night businesses.[27] But an increasing number of community centers and support services are also part of the city's growing

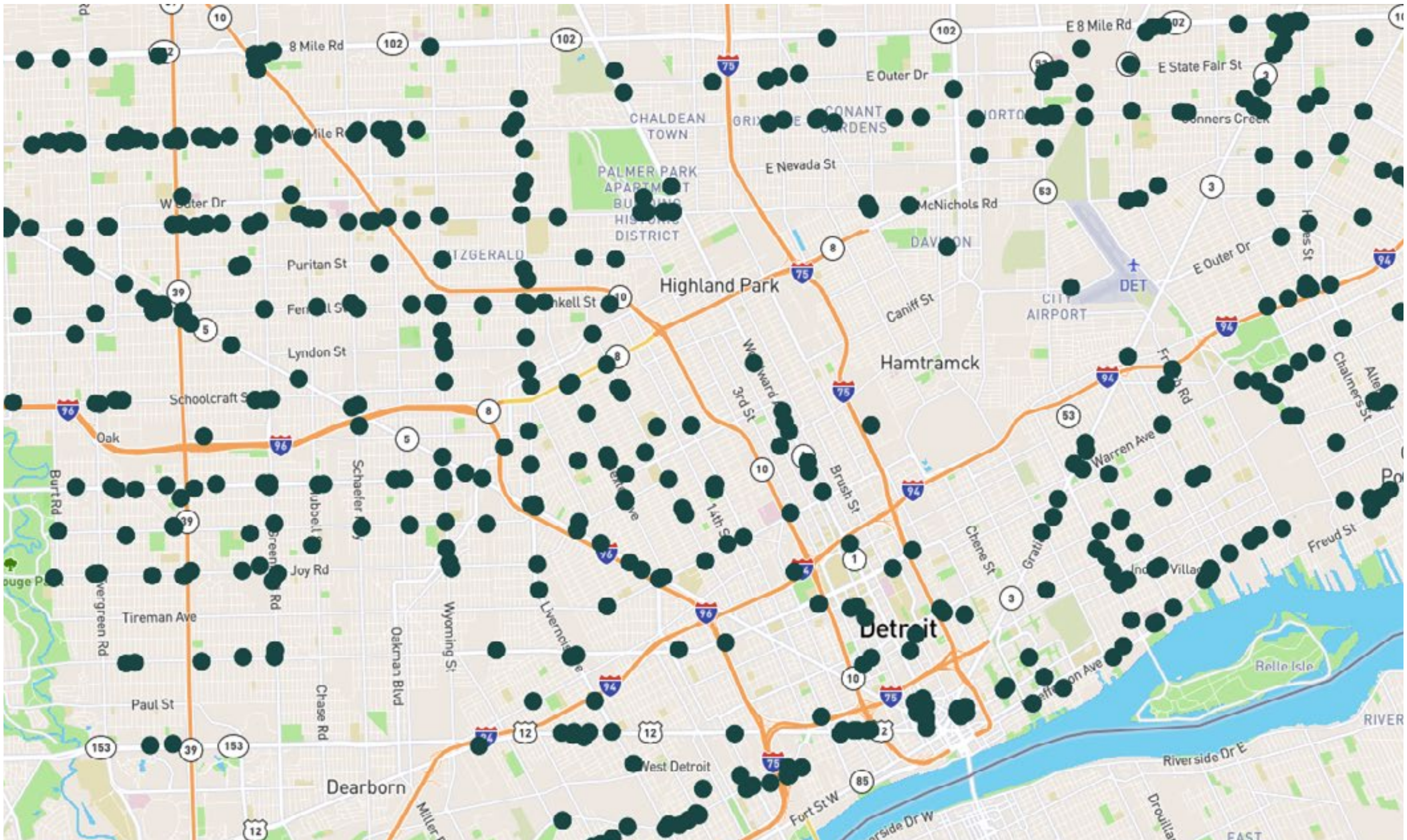


Figure 3: As of May 2019, Project Green Light has cameras in at least 535 locations across the city of Detroit. (Source: Detroit Open Data Portal.)

camera network. As of April 2019, Project Green Light partners included 11 churches, 12 stand-alone pharmacies, eight schools, and at least 15 clinics—providing addiction treatment, reproductive health and family planning services, counseling, and youth-specific care to Detroit's residents.[28] More than 30 residential locations—including apartment buildings, senior living centers, and hotels are also current partners. Other churches, schools, and support centers are not part of Project Green Light but are immediately adjacent to partner businesses and potentially within range of their neighbors' cameras.[29]

Attending many of these locations reveals deeply personal information about a resident's "religious, political, or social views or activities" or "participation in particular noncriminal organization or lawful event.[30] While these activities may occur in public, most of us do not expect to be sharing our attendance at a church service or an addiction treatment center with law enforcement. We do not have to be hiding illegal activity to desire privacy in a choice to worship, seek counseling or treatment, or obtain an abortion or other medical service.

Without restrictions on where face surveillance is deployed, the Project Green Light system may inadvertently violate the very policy established to protect residents against its potential harms. The goal of these surveillance cameras is to make Detroit's residents feel safe going about their daily lives. Adding face surveillance to these cameras risks doing the opposite.

C. DESPITE ASSURANCES, A SYSTEM OBSCURED FROM PUBLIC VIEW

As of publication of this report—almost two years after Detroit purchased a real-time citywide face surveillance system—the system has never received the public scrutiny it deserves. This is in spite of the fact that around the time of purchase, DPD Assistant Chief James White dismissed any suggestion that face surveillance would be obscured from the public. "This isn't some super-secret piece of technology," he stated.[31]

But the website dedicated to providing the public with information about Project Green Light Detroit fails to mention the use of face recognition, real-time face surveillance, or any kind of automated face analysis technology even once.[32]

Even the partner locations appear unaware that they may be contributing to a massive face surveillance program. None of the information provided to prospective partners informs them of the fact that face surveillance is part of Project Green Light, and may be used on their camera feeds. Neither the partnership agreements that locations are required to sign nor the application to participate mention the use of real-time face surveillance.[33] And while the locations of all Project Green Light partner businesses are public, there is no available information about which cameras are face surveillance–enabled.[34]

In light of the sensitive nature of many of the camera locations, this is a critical omission. A clinic like Summit Medical Center may see a real benefit from participating in a program that deters crime and ensures rapid police response to any incidents at its business. But when making the decision to enter this partnership, the center deserved to be aware that the cameras may also be capable of identifying its patients.

III. "... FACIAL RECOGNITION ON CHICAGO'S VAST CAMERA MONITORING SYSTEM"

"If cities like Chicago equip their full camera networks with face recognition, they will be able to track someone's movements retroactively or in real-time, in secret, and by using technology that is not covered by the warrant requirements of existing state geolocation privacy laws."[35]

Illinois, the state with the strongest commercial biometric privacy law on the books, is also host to one of the most advanced biometric surveillance systems in the country.[36] The Chicago Police Department (CPD) and the Chicago Transit Authority have had face surveillance capabilities since at least 2016.[37] DataWorks Plus, the vendor that provides the system to the Chicago, describes it as follows:

> "… a Real Time Screening System (RTS) and a Facial Recognition System (FRS). The project objective included Real Time Screening using Facial Recognition on Chicago's vast camera monitoring system which includes nearly 20,000 street, transit and other video cameras located throughout the city. DataWorks Plus integrated its RTS system with Chicago's Genetec Omincast [sic] camera video streams that allow Chicago to select any number of cameras to monitor using facial recognition and a special persons of interest Watchlist mugshot database."[38]

The system is configured to compare faces captured on video surveillance footage to Chicago's database of around seven million mug shots.[39]

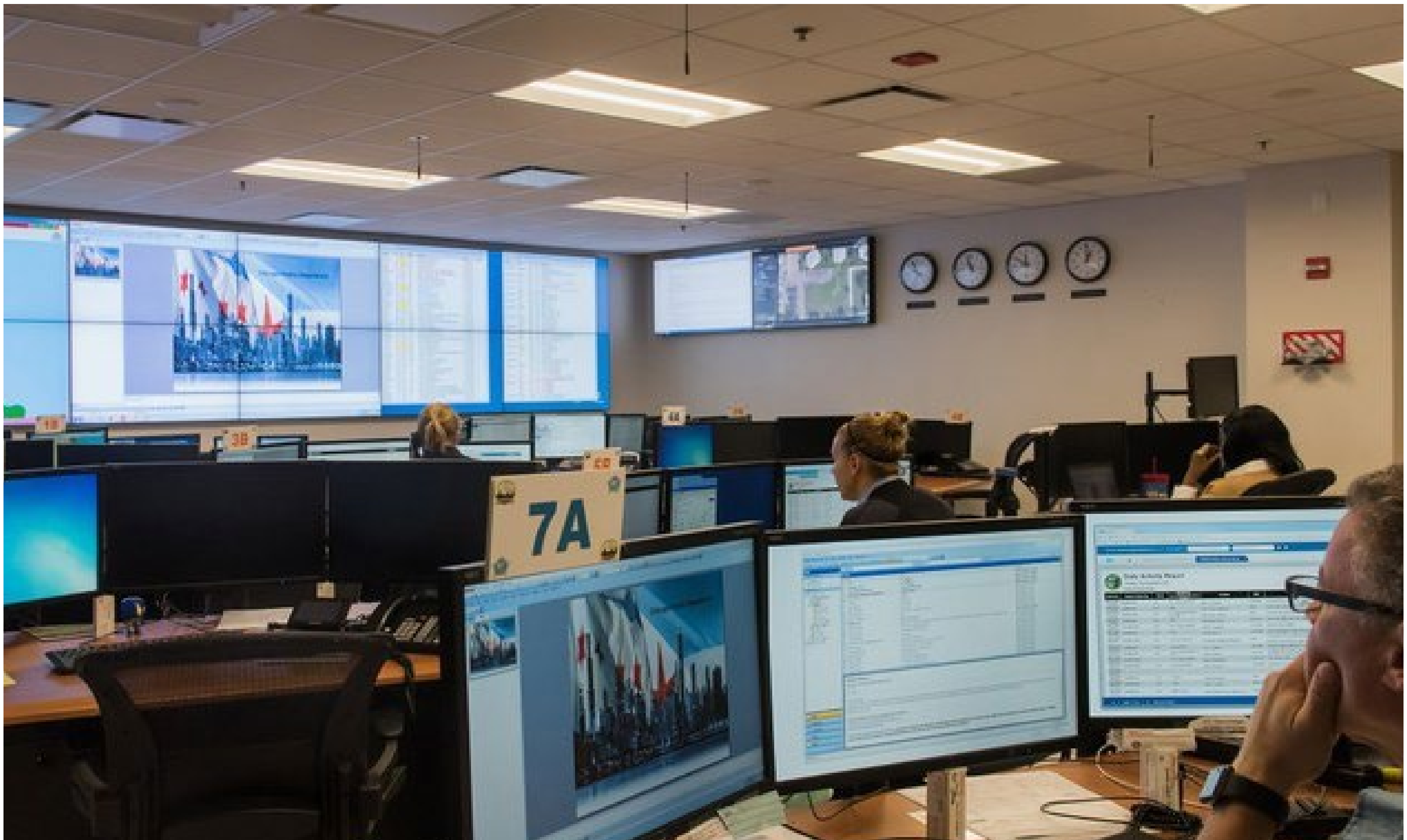


Figure 4: Personnel in Chicago Police Department's Crime Prevention and Information Center monitor surveillance video from around the city. (Source: FBI.)

Chicago sought to implement a face surveillance system in as early as 2009. That year, CPD applied for a grant of more than $13 million from the Department of Homeland Security (DHS) to support the creation of a "regional transit terrorism prevention and response system."[40] The proposal included a face recognition system that would initially operate on the existing Chicago Transit Authority (CTA) CCTV system, to be expanded first to "partner agency camera feeds" and eventually "to include additional cameras outside of Chicago" as well.[41]

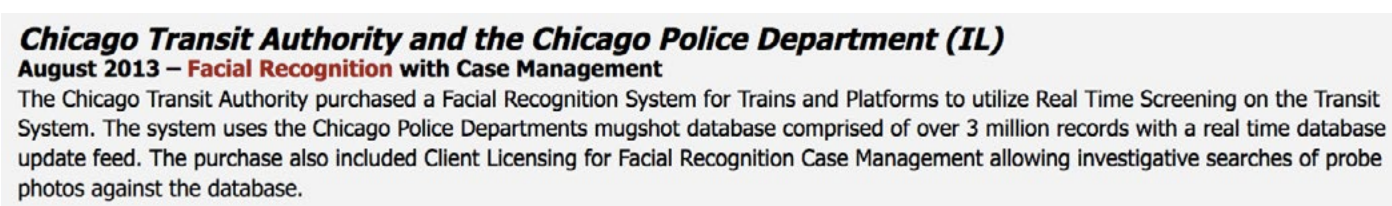
In its final progress report for the FY09 DHS grant in 2013, CPD stated it had developed various video surveillance applications, including software "already able to process and provide notification functionalities such as … face capture and match" and "able to handle multiple concurrent video streams."[42]

A. ANOTHER OPAQUE SURVEILLANCE SYSTEM

Despite its potentially leviathanic size, the face recognition component of Chicago's surveillance system has almost completely evaded public scrutiny. The most complete description of the system, as quoted above, was provided not by a public agency running the program but by the vendor company selling it—in its bid for the contract to provide Detroit with similar capabilities.[43]

Figure 5: A police camera monitors the bridge walkway near Wacker and Lake Streets in Chicago. (Source: Steve Hamann/Shutterstock, all rights reserved.)

Responses from CPD to public records requests provide a conflicting picture of the status of CPD's face surveillance capabilities. In a letter to the ACLU of Illinois on November 10, 2016, CPD stated that it "does not use facial recognition technology in real time-situations [sic]..."[44] despite its report to DHS in 2013 indicating that face surveillance capabilities were in place.[45] That same day, DataWorks Plus entered an agreement to provide maintenance and support for the real-time face surveillance software it had provided to CPD under a previous contract.[46] Continued maintenance and support of the system certainly suggests that it is operational, if not yet in operation.



Chicago Transit Authority and the Chicago Police Department (IL)

August 2013 – Facial Recognition with Case Management

The Chicago Transit Authority purchased a Facial Recognition System for Trains and Platforms to utilize Real Time Screening on the Transit System. The system uses the Chicago Police Departments mugshot database comprised of over 3 million records with a real time database update feed. The purchase also included Client Licensing for Facial Recognition Case Management allowing investigative searches of probe photos against the database.

Figure 6: The DataWorks Plus website states clearly that the vendor built a large real-time face surveillance system for Chicago. (Source: DataWorks Plus website, "Company News Archives.")

Responses from CTA, described by the vendor company as one of the contracting agencies, and the Chicago Department of Procurement Services, the office responsible for the City's contracts, have been less helpful. CTA could find no records responsive to a request for corroborating information; the Department of Procurement Services "neither possesses nor maintains any responsive documents."[47]

These responses make it impossible to know whether Chicago's agencies follow any rules when using—or planning to use—this vast face surveillance capability. No public policies appear to exist. Documents dating back to 2013 that describe CPD's investigative face recognition capabilities state that "[p]olicies, training and protocols *will be* developed and maintained by the Bureau of Detectives."[48] CPD's 2016 letter to the ACLU similarly stated: "…to help the public better understand our use of facial recognition technology, we are in the process of rewriting our directive to reflect how we use this technology."[49] Yet, as of the publication of this report more than two years later, no updates have been provided to fulfill the promise of providing transparency to the public about how CPD does—and does not—use face recognition.[50]

B. AT ODDS WITH THE WILL OF THE PUBLIC

"The technology is here and being used by police departments already. There's an article … from China, just this week at a concert, where a concertgoer went and was arrested within minutes based off of facial recognition data at that concert. It is here. We have to balance public safety versus people's Constitutional rights. That's our job. But our job is to uphold the Constitution, the Constitution of Illinois and the Constitution of the United States. And I'll remind people of the First Amendment of the U.S. Constitution, for the right of people to peaceably assemble."[51]

—Rep. Tim Butler (R)

Chicago's expansive face surveillance capabilities run counter to the strong interest in protecting citizens' biometric data expressed by the state legislature. Illinois passed the first, and the country's most protective, biometric privacy law in 2008. The Biometric Information Privacy Act (BIPA) guards state citizens against the collection, use, and dissemination of their biometric information without their express, written consent—but only by commercial entities.[52]

Public agencies, such as law enforcement, are notably exempt from BIPA's requirements. However, recent debate in the state House over a police drone bill suggests that legislators, and by extension the public, may be similarly uncomfortable with the prospect of biometric surveillance by the police. House members repeatedly voiced alarm at the prospect of the drones being equipped with face recognition capabilities. Members characterized the prospect as "truly terrifying" and "somewhat of an Orwellian reach into

Figure 7: The Illinois State Capitol in Springfield, Illinois. In 2008, Illinois passed the country's first biometric privacy law. (Source: Henryk Sadura/Shutterstock, all rights reserved.)

crowd control"—a capability that may run afoul of the First and Fourth Amendments of the Constitution.[53]

Nonetheless, Chicago authorities appear intent on operating at odds with the concerns that many state lawmakers have expressed regarding biometric privacy. The limited information that is available suggests that Chicago is home to the most widespread face surveillance system in the United States today. An amendment proposed last year to Chicago's Municipal Code additionally attempted to circumvent the protections BIPA afforded to citizens. The amendment would have permitted commercial entities that have signed an agreement with police to be able to use face recognition systems to meet whatever "security needs" they may have.[54]

This proposal—and CPD's secretive face surveillance system—creates a stark divide between the privacy protections for Illinois residents outside Chicago, and those within.

IV. FACE SURVEILLANCE PILOTS IN ORLANDO, WASHINGTON, D.C., AND NEW YORK CITY

Chicago and Detroit are not the only jurisdictions interested in face surveillance, though they seem to be the furthest along in realizing this goal. In our 2016 report, the Center on Privacy & Technology found that at least four additional police departments—the Los Angeles Police Department, West Virginia Intelligence Fusion Center, Seattle South Sound 911, and Dallas Area Rapid Transit—had purchased or had announced plans to purchase face surveillance systems.[55] Since then authorities have begun piloting face surveillance systems in Orlando, Washington, D.C., and New York City as well.

A. DOWNTOWN ORLANDO, FLORIDA

The City of Orlando began testing a face surveillance program with Amazon Web Services in December 2017 in a pilot that is scheduled to run until July 2019.[56] The pilot initially ran on eight cameras, comparing the faces of passersby to a "watch list" database of police employee volunteers.[57] If the Orlando Police Department (OPD) deems it a success, the city will move to make it a more permanent surveillance feature.

"We would never use this technology to track random citizens, immigrants, political activists, or certainly people of color," Orlando Police Chief John Mina stated during a press conference in May 2018, responding to widespread privacy and civil rights concerns about the program's goals.[58] Exactly how OPD plans to ultimately use the technology, however, has not yet been decided—there are no rules yet in place. According to the city's website, OPD will "develop a policy and governance surrounding the technology," but only after the conclusion of the pilot in July of 2019.[59]

B. AROUND THE WHITE HOUSE, WASHINGTON, D.C.

The U.S. Secret Service (USSS) initiated a face surveillance pilot around the White House in November 2018. The goal of the pilot is to determine whether the technology can be used "to identify known individuals and to determine if biometric technology can be incorporated into the continuously evolving security plan at the White House Complex." Like the Orlando pilot, the initial test will attempt to identify volunteer agency employees using live surveillance cameras that currently "capture video from individuals on the sidewalk and street" around the complex.[60]

USSS has issued a Privacy Impact Assessment (PIA) evaluating privacy risks that the limited pilot program raises, but not concerns that may be raised if the program goes live. It contemplates some risk to the public—like the fact that the system will continuously scan the faces of people walking by who do not have the ability to opt-out, or that someone may be mistakenly matched to an identity on the "watch list."

However, it envisions these and other risks to be mitigated primarily by the limits of the pilot program, for example that the watch list database is composed of employee volunteers, and not using the face recognition matches for anything other than testing the system's capabilities.[61] This is less than helpful for evaluating the risks—and steps for mitigating risk—on the ultimate live system. Should the USSS choose to adopt the technology, the watch list database will almost certainly not be composed of Secret Service officers.[62]

C. BRIDGES AND TUNNELS AROUND MANHATTAN, NEW YORK

In late 2016, New York's Governor Andrew Cuomo announced that face surveillance would be part of an overhaul of the security, tolling system, and infrastructure of key bridges and tunnels around New York City.[63] The project, headed by the Metropolitan Transportation Authority (MTA), envisioned the ability to capture and identify drivers' faces, through their windshields, passing by cameras located above the highways leading into and out of Manhattan.[64]

The pilot's initial phase began in mid-2018 and has reportedly been a complete failure, unable to detect a single face.[65] Despite this failure, attributed to the fact that the technology is not yet capable of this task, the pilot continues. Even a spokesperson for IDEMIA, the company providing the technology to MTA, when asked if face surveillance could work through the windshield of a moving car, reportedly stated "I'd like to find a tactful way to say, 'No.'"[66]

The pilot has also moved forward despite widespread privacy concerns, a complete absence of transparency, and no apparent rules governing how the system will be used. It is even unclear what the ultimate goal of the face surveillance program is. Conflicting reports from MTA officials have alternately asserted that the system would be used either to identify toll evaders or to screen for far more serious offenders like potential terrorists.[67] These are manifestly different systems, carrying different risks and requiring vastly different sets of rules. And none have thus far been provided to the public.

V. RECOMMENDATIONS

In 2016, the Center on Privacy & Technology issued a report on police use of face recognition technology in the United States. In that report we recommended that state legislatures adopt common sense legislation to comprehensively regulate law enforcement use of face recognition.

Since then, a dramatic range of abuse and bias has surfaced. Baltimore County Police used the technology to identify and arrest people protesting the death of Freddie Gray.[68] A Brown University student was falsely identified as a possible terrorist suspect responsible for attacks in Sri Lanka.[69] Research by Joy Buolamwini, Timnit Gebru, and the ACLU of Northern California verified that the technology still exhibits race and gender bias.[70]

As a result, we now believe that state, local, and federal government should place a moratorium on police use of face recognition. We also believe that jurisdictions that move to ban the technology outright are amply justified to do so.

Once bans or moratoria are in place, communities can stop to think about whether face surveillance should be allowed in their streets and neighborhoods.

The Center warned two years ago: If deployed pervasively, real-time video surveillance threatens to create a world where, once you set foot outside, the government can track your every move.[71] For the 3.3 million Americans residing in Detroit and Chicago, this may already be a reality.

VI. ACKNOWLEDGEMENTS

Critical guidance and close reading of this report were provided by our team of outside reviewers, who will remain anonymous but who lent us their expertise on Chicago and Detroit policing and community organizing, policy considerations regarding surveillance, and the technical functioning of face recognition systems. This report would not be possible without the entire team at the Center, who helped in countless ways: Alvaro Bedoya, Katie Evans, Harrison Rudolph, Jameson Spivack, Gabrielle Rejouis, and Julia Chrusciel. We are also grateful to the Center's research assistants and summer fellows; our copy editor, Joy Metcalf; our design and web development firm, Rootid; and our cover designer, Eve Tyler.

We also acknowledge, with gratitude, the work of our friends and allies at other organizations also striving to shed light on how face recognition technology is used and to prevent powerful police tools from being used in ways that are harmful to individuals and communities.

The Center on Privacy & Technology at Georgetown Law is supported by the Ford Foundation, the Open Society Foundations, the MacArthur Foundation, Luminate, the Media Democracy Fund, and Georgetown University Law Center.

VII. ENDNOTES

1. On October 18, 2016, the Center on Privacy & Technology released a report on the use of face recognition by police across the country. *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Oct. 16, 2016), https://www.perpetuallineup.org. One of the predictions we made was that in the absence of regulation, face recognition was going to become more advanced and more widespread across the United States.

2. Prod. Joyce Liu, *In Your Face: China's all-seeing state,* BBC News (Dec. 10, 2017), https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state at 1:16.

3. The International Justice and Public Safety Network, *Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* (June 30, 2011), Document p. 016632.

4. Carpenter v. United States, 138 S.Ct. 2206, 2217 (2018).

5. *Id.*, quoting United States v. Jones, 565 U. S. 400, 430 (Alito, J., concurring).

6. *Id.,* quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring), Riley v. California, 134 S. Ct. 2473, 2494–95 (2014).

7. *See The Perpetual Line-Up*, https://www.perpetuallineup.org/findings/racial-bias.

8. *See* Michael King, *Demographic Effects of Race on Face Recognition*, IFPC 2018 (Nov. 27, 2018), *presentation available* at https://nigos.nist.gov/ifpc2018/presentations/15_king_18-11-27_DemographicEffectsFaceRecognitionNIST_Update.pdf. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15 (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

9. Summit Medical Center, a reproductive health center, became a Project Green Light partner in December 2016. *See*Project Green Light Locations Dataset, *available at* https://data.detroitmi.gov/Public-Safety/Project-Green-Light-Locations/vrh6-6pvj (last visited April 15, 2019).

10. As of April 15, 2019, Project Green Light had 527 partner locations. Detroit Police Department, Project Green Light Locations Dataset, *available at* https://data.detroitmi.gov/Public-Safety/Project-Green-Light-Locations/vrh6-6pvj (last viewed April 15, 2019). For a discussion of the deterrence goal of the Project, *see* Juleyka Lantigua-Williams, *Using a Green Light to Bring Crime to a Stop*, The Atlantic (May 19, 2016), https://www.theatlantic.com/politics/archive/2016/05/project-green-light/483300/.

11. For a description of the system's capabilities, *see* Detroit Police Department *Professional Services Contract between City of Detroit, Michigan and DataWorks Plus, Contract No. 6000801*, Document pp. 018434, 018477. The contract term is 7/18/2017–7/17/2020. *See* Procurement Contracts Data, *available at* https://data.detroitmi.gov/Government/Procurement-Contracts/itv9-b6jk/data (last viewed April 15, 2019) (Contract effective date is listed as 7/17/2017; contract expiration date is listed as 7/17/2019).

12. DataWorks Plus Contract at 018461.

13. *Id.* at 018459. DataWorks Plus FACE Watch Plus webpage, *available at* http://www.dataworksplus.com/rts.html (last viewed April 15, 2019).

14. DPD, *DataWorks Plus Contract, City of Detroit Request for Proposal, Facial Recognition Software Solutions* (Nov. 30, 2015), Document p. 018406.

15. *Id.* at 018458 ("To purchase facial recognition licensing, software and equipment for the Detroit Police Department Green Light Locations."). For more information, see the sidebar on Project Green Light Detroit. It is unclear exactly if and when the face surveillance component of Project Green Light became operational, but a DPD official told the press that the vendor's software would be integrated with Project Green Light in November 2017. George Hunter, *Project Green Light to add facial recognition software,* The Detroit News (Oct. 30, 2017), https://www.detroitnews.com/story/news/local/detroit-city/2017/10/30/detroit-police-facial-recognition-software/107166498/. DataWorks Plus has implemented complex face recognition systems in other jurisdictions in as little as two to four months. DataWorks Plus Contract at 018471 ("DataWorks Plus delivered the Michigan State Police Facial Recognition system, which had 33 million photos, in less than 4 months after receiving the Purchase Order. We also delivered the SC DMV Facial Recognition system in 2 months. We converted 7.7 million images in less than 3 weeks and enrolled images in 8 days.").

16. DPD, *Crime Intelligence Unit Standard Operating Procedure for Face Recognition* (July 1, 2018, revised April 1, 2019), Document pp. 023779, 023783 (emphasis added). Prior to July 1, 2018, DPD did not have a policy for its face recognition system. In response to a records request, on May 31, 2018 the City told the Center on Privacy & Technology: "Based on information provided by City of Detroit Police Department personnel, it is our understanding that they are currently in the process of creating the policies and standard operating procedures regarding the facial recognition system. Accordingly, they do not currently possess any

record which corresponds with the description of your request." Detroit Police Department, *Letter from Amanda Rakos, Assistant Corporation Counsel for the City of Detroit Law Department to Clare Garvie re. Freedom of Information Act Request No. A18-02928* (May 31, 2018), Document p. 019108.

17. DPD, *Crime Intelligence Unit Standard Operating Procedure for Face Recognition* (July 1, 2018, revised April 1, 2019), Document p. 023782. DPD, *Letter from Dawn Brinningstaull, Director, Department of State Police Criminal Justice Information Center to Chief James E. Craig, Detroit Police Department* (Sept, 25, 2018) (on file with author).

18. *See* Project Green Light Detroit website, http://www.greenlightdetroit.org.

19. *See id.*; State of Michigan Board of Police Commissioners *Community Meeting* (Jan. 14, 2016), Document p. 019537.

20. City of Detroit Open Data Portal, *Project Green Light Locations*, https://data.detroitmi.gov/Public-Safety/Project-Green-Light-Locations/vrh6-6pvj (Last visited Apr. 15, 2019). As of January 25, 2019, this list included: 15 "community" partners, such as churches and cultural centers; 23 "residential" partners, such as hotels, senior care centers, and apartment buildings; and 91 "services" partners, which include clinics, pharmacies, and addiction treatment centers. *See also* Mark Hicks, *Green Light adds 1st School, sparks criticism,* The Detroit News (Apr. 22, 2018), https://www.detroitnews.com/story/news/local/detroit-city/2018/04/22/project-green-light-randolph-school/34154981/.

21. Project Green Light Detroit Website, http://www.greenlightdetroit.org/ (last visited Apr. 15, 2019).

22. City of Detroit Open Data Portal, *Project Green Light Locations*, https://data.detroitmi.gov/Public-Safety/Project-Green-Light-Locations/vrh6-6pvj (last visited Apr. 15, 2019, at which point the dataset listed 528 individual partner businesses).

23. *See* Mark Hicks, *Green Light adds 1st school, sparks criticism*, The Detroit News (Apr. 22, 2018),https://www.detroitnews.com/story/news/local/detroit-city/2018/04/22/project-green-light-randolph-school/34154981/.

24. *See* Allie Gross, *Controversial surveillance program coming to Detroit public housing,* Detroit Free Press (Nov. 6, 2018), https://www.freep.com/story/news/local/michigan/detroit/2018/11/06/project-green-light-detroit-public-housing/1712494002/.

25. *See* Chad Livengood, *Detroit aims to mandate Project Green Light crime-monitoring surveillance for late-night businesses,* Crain's Detroit Business (Jan 3, 2018), https://www.crainsdetroit.com/article/20180104/news/649206/detroit-aims-to-mandate-project-green-light-crime-monitoring.

26. DPD, *Crime Intelligence Unit Standard Operating Procedure for Face Recognition* (July 1, 2018, revised April 1, 2019), Document p. 023782. DPD recently issued a new directive, made public within the last month, that governs the use of face recognition as an investigative tool, but does not appear to contemplate its use on live video feeds. DPD, *Directive Number 307.5: Facial Recognition* (Dec. 13, 2018), *available at* https://detroitmi.gov/document/facial-recognition.

27. For a complete list of Project Green Light Partners, *see* City of Detroit Open Data Portal, *Project Green Light Locations*, *available at* https://data.detroitmi.gov/Public-Safety/Project-Green-Light-Locations/vrh6-6pvj/data (last viewed Apr. 15, 2019).

28. *Id.*

29. *Id. See Memorandum of Understanding Project Green Light Detroit Agreement,* City of Detroit, *available at* https://detroitmi.gov/departments/police-department/project-green-light-detroit/agreements (last viewed April 8, 2019) ("Cameras positioned outdoors will cover all areas generally accessible by the public on or near the Entity's property. Cameras positioned outdoors will also be positioned such that they will legibly capture the license plates of automobiles passing through the Entity's property…"). A Google Maps survey of Project Green Light Locations suggests that dozens of other community and support centers may be within camera range. *See generally,* City of Detroit Open Data Portal, *Project Green Light Locations*, *available at* https://data.detroitmi.gov/Public-Safety/Project-Green-Light-Locations/vrh6-6pvj/data (last viewed April 15, 2019) (notes on adjacent locations on file with author).

30. DPD, *Crime Intelligence Unit Standard Operating Procedure for Face Recognition* (July 1, 2018, revised April 1, 2019), Document p. 023782.

31. *See* George Hunter, *Project Green Light to add facial recognition software*, The Detroit News (Oct. 30, 2017), http://detne.ws/2yY4HBv. This and a few subsequent articles did raise the issue of face surveillance around the time of purchase, providing valuable coverage and context for the public.

32. Project Green Light Detroit Webpage, https://detroitmi.gov/departments/police-department/project-green-light-detroit (last viewed Apr. 15, 2019).

33. Project Green Light Detroit Partnership Agreement, https://detroitmi.gov/departments/police-department/project-green-light-detroit/agreements#Partnership-Agreement; Project Green Light Corridor Agreement, https://detroitmi.gov/departments/police-department/project-green-light-detroit/agreements/corridor-agreement; Project Green Light Business Application, https://docs.google.com/forms/d/e/1FAIpQLSd8Rl2NBYwA1xwkuXp5B_HRli8opAl-DbsinCzzW0n61WpCeA/viewform. The Center on Privacy & Technology additionally called a number of Project Green Light locations, none of whom reported being informed by DPD that face surveillance or face recognition generally might be used on their cameras pursuant to the partnership. (Notes on file with author.)

34. Interactive Project Green Light Map, https://detroitmi.gov/webapp/project-green-light-map (last viewed Apr. 15, 2019).

35. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Oct. 16, 2016), https://www.perpetuallineup.org/risk-framework.

36. The Illinois legislature passed the Biometric Information

Privacy Act (BIPA) in 2008, to regulate the collection of biometric information, including face data, by commercial entities. Law enforcement entities are not covered by the law.

37. DataWorks Plus Contract at 018489. The DataWorks Plus response to Detroit's RFP for a real-time face surveillance system was submitted January 9, 2017, and describes an already-established real-time system in Chicago.

38. *Id.* In 2014, CPD's camera network included "access to 24,371 video cameras … which include[d] not only CPD's own cameras, but also cameras owned by partner agencies." Document p. 023540. The system is called Omnicast, not Omincast. *See* Genetec, *Security Center Omnicast Solutions*, https://www.genetec.com/solutions/all-products/omnicast (last viewed Apr. 16, 2019).

39. DataWorks Plus Contract at 018489.

40. The total 2009 grant award was for $13.8 million for a period of three years. Department of Homeland Security FEMA Grant Programs Directorate, *Cooperative Agreement FY 2009 Transit Security Grant Program, Grant award 2009-RA-T9-K016* (July 24, 2009), Document pp. 023716–18; DHS, *FEMA Grant Manager's Memorandum , Pt 1: Project Summary*, Document p. 023720.

41. CPD, *TSGP Investment Justification Template* (Jan. 14, 2009), Document pp. 023524–25. The face recognition component was part of "Phase C," to be implemented one to three years after the date of the grant award. Document p. 023531.

42. CPD, *FY09 Transit Security Grant Program Award: 2009-RA-T9-K016, Final Progress report: For the period of January 1 - March 31, 2013*, Document pp. 023709–10.

43. DataWorks Plus Contract at 018489.

44. City of Detroit, *Letter from Charise Valente, CPD General Counsel to Karen Sheley, Director, Police Practices Project, Roger Baldwin Foundation of ACLU, Inc* (Nov. 10, 2016), Document p. 023649.

45. CPD, *FY09 Transit Security Grant Program Award: 2009-RA-T9-K016, Final Progress report: For the period of January 1 - March 31, 2013*, Document pp. 023709–10 ("Applications have also been developed that take advantage of the sophisticated analytical functions in the installed video processing software. The software is already able to process and provide notification functionalities such as intrusion detection, objects left behind, loitering, and face capture and match. It is also able to handle multiple concurrent video streams.").

46. CPD, *Motorola Solutions, Task Order and Statement of Work for Services to be performed by DataWorks Plus, LLC For the Chicago Public Building Commission TO896 2016 DataWorks Software Support* (Nov. 10, 2016), Document pp. 023724–32. This agreement is not pursuant to a contract directly with CPD but states that it is for maintenance and support for "Software purchased for Chicago PD" from DataWorks Plus. The primary contract holder, the Chicago Public Building Commission, has previously been responsible for implementing elements of the CPD and CTA "Transit Terrorism Prevention and Response" project, including "Video Analytics/Facial Recognition hardware and software." *See* Public Building Commission of Chicago, *Quarterly Staff Reports 2012: Third Quarter* (Sept. 21, 2012), p. 52, *available at* https://www.pbcchicago.com/wp-content/uploads/2017/07/2012_Q3Report.pdf.

47. Chicago Transit Authority, *Letter to Clare Garvie from Brigett R. Bevan, Director, Freedom of Information Compliance, Chicago Transit Authority* (May 8, 2018), Document pp. 018615–16 ("In response to your request, CTA performed a reasonable search and found that it does not have any records responsive to this request."); Chicago Dep't of Procurement Services, *Letter to Clare Garvie from Cathy Kwiatkowski, Director of Public Affairs and DPS FOIA Officer, Department of Procurement Services for the City of Chicago* (Apr. 26, 2018), Document p. 018619 ("Please be advised, the Department of Procurement Services neither possesses nor maintains any responsive documents.").

48. CPD, *Notice D13-11: Facial Recognition Technology* (Aug. 23, 2013), Document p. 007686 (emphasis added).

49. CPD, *Letter from Charise Valente, CPD General Counsel to Karen Sheley, Director, Police Practices Project, Roger Baldwin Foundation of ACLU, Inc.* (Nov. 10, 2016), Document p. 023649.

50. The Center's latest FOIA request to CPD, dated August 30, 3018, requested "any manuals, guidelines, policies, and practices the agency follows for using the FRT system." CPD's final response, on April 1, 2019, included no policy beyond the original 2013 directive. CPD, *Letter from K. Washington, CPD FOIA Officer to Clare Garvie re. Notice of Response to FOIA Request* (March 26, 2019), Document pp. 023447–49.

51. Rep. Tim Butler, State of Illinois 100th General Assembly House of Representatives Transcription Debate, 138th Legislative Day (May 25, 2018), p. 43, *available at* http://www.ilga.gov/house/transcripts/htrans100/10000138.pdf.

52. 740 ILCS 14/ http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

53. State of Illinois 100th General Assembly House of Representatives Transcription Debate, 138th Legislative Day (May 25, 2018), pp. 40, 43, *available at* http://www.ilga.gov/house/transcripts/htrans100/10000138.pdf. State of Illinois 100th General Assembly House of Representatives Transcription Debate, 141st Legislative Day (May 30, 2018), pp. 252–53, *available at* http://witnessslips.ilga.gov/house/transcripts/htrans100/10000141.pdf. ("Last week we had a very spirited debate on this Bill. I learned a lot from our debate that we had you guys had a lot of suggestions for us on what we could do to make this Bill better … And we also took out facial and biometric recognition. And I hope that made the Bill a lot better for everybody.").

54. Proposed Municipal Code Chapter 4-4-308 (copy on file with author).

55. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Oct. 16, 2016), https://www.perpetuallineup.org/findings/deployment.

56. Phase I of the pilot program ran from December to June of

2018. *See* AWS Professional Services - Statement of Work (Dec. 19, 2017), Document pp. 023393–99 (detailing that the Statement of Work is effective as of the date signed and automatically terminates six months after that date). Phase II, labeled the "Video Identification Proof of Concept" phase, began in October of 2018 and is scheduled to run for a nine month period. *See* AWS Professional Services - Statement of Work (Oct. 17, 2018), *available at* https://www.orlando.gov/files/sharedassets/public/initiatives/amazon-facial-rekognition/statement-of-work-phase-2.pdf; City of Orlando Memorandum on Amazon Pilot Program (July 6, 2018), *available at* https://www.orlando.gov/files/sharedassets/public/initiatives/amazon-facial-rekognition/amazon-pilot-program-memo.pdf

57. City of Orlando Memorandum on Amazon Pilot Program (July 6, 2018), *available at* https://www.orlando.gov/files/sharedassets/public/initiatives/amazon-facial-rekognition/amazon-pilot-program-memo.pdf.

58. *See* Ryan Gillespie and Gal Tziperman Lotan, *Downtown Orlando has 3 Amazon facial-recognition cameras, police chief says—contrary to earlier claim*, Orlando Sentinel (May 24, 2018), https://www.orlandosentinel.com/news/breaking-news/os-amazon-orlando-police-cameras-downtown-20180524-story.html.

59. City of Orlando, Facial Recognition Pilot Program, *available at* https://www.orlando.gov/Initiatives/Facial-Recognition-Pilot-Program (last viewed April 8, 2019).

60. Department of Homeland Security (DHS), *Privacy Impact Assessment for the Facial Recognition Pilot, DHS/USS/PIA-024* (Nov. 26, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf

61. *See, e.g. id.* at 4 ("Mitigation: ...The USSS volunteer employees participating in the pilot are provided individual notice and have consented to their participation."); *see id.* at 7–8 ("As there is a limited gallery of individuals against whom to match, the false positive rate may be limited as well … Additionally, any images that are a match will only be retained until the conclusion of the pilot and no operational use will be made of any matches.").

62. Fortunately, the PIA states that it "will be updated as USSS' methods and policies for the use of facial recognition technology evolve." *Id.* at 9. This still puts the cart before the horse, however, allowing decisions about the systems deployment to occur before the true risks are evaluated and policies are put in place to mitigate those risks.

63. New York State Website, *Governor Cuomo Announces Transformational Plan to Reimagine New York's Bridges and Tunnels for 21st Century* (Oct, 5, 2016), https://www.governor.ny.gov/news/governor-cuomo-announces-transformational-plan-reimagine-new-york-s-bridges-and-tunnels-21st.

64. *See* Frank Esposito, *Cashless tolling: Facial recognition coming to a bridge or tunnel near you*, USA Today (Sept. 25, 2018), https://www.lohud.com/story/news/investigations/2018/09/25/cashless-tolling-facial-recognition-military-technology-bridges-new-york/1260241002/.

65. *See* Paul Berger, *MTA's Initial Foray Into Facial Recognition at High Speed Is a Bust*, Wall Street Journal (Apr. 7, 2019), https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust-11554642000. The pilot was first reported to have begun in April 2018. *See* Dana Rubinstein, *I Seem to Recognize Your Face*, Politico (July 25, 2018), https://www.politico.com/newsletters/new-york-playbook/2018/07/25/ocasio-cortezs-stealth-dc-visit-speed-cameras-set-to-expire-mta-tests-facial-recognition-technology-but-flightless-fowl-move-faster-than-its-buses-de-blasio-moves-to-restrict-hotel-development-290666.

66. *See id.*

67. *See* Paul Berger, *MTA's Initial Foray Into Facial Recognition at High Speed Is a Bust*, Wall Street Journal (Apr. 7, 2019), https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust-11554642000.

68. *See* Jon Schuppe, *Facial recognition gives police a powerful new tracking tool. It's also raising alarms,* NBC News (July 30, 2018), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936.

69. *See* Owen Daugherty, *Sri Lankan authorities mistakenly include Muslim US college student's face among bombing suspects*, The Hill (Apr. 29, 2019), https://thehill.com/blogs/blog-briefing-room/news/441152-sri-lankan-authorities-mistakenly-include-muslim-us-college.

70. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15 (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

71. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America*, 64 (Oct. 16, 2016), https://www.perpetuallineup.org.

VIII. ABOUT THE AUTHORS

Clare Garvie joined the Center on Privacy & Technology as a Law Fellow after graduating from Georgetown Law in 2015, and now serves as a Senior Associate. In 2016, she was lead author of The Perpetual Line-Up: Unregulated Police Face Recognition in America. Prior to entering law school, she worked in human rights and international criminal law with the International Center for Transitional Justice. She received her B.A. from Barnard College in political science, human rights, and psychology.

Laura Moy is the Executive Director of Georgetown Law's Center on Privacy & Technology. Before joining the Center, Laura was Acting Director of the Communications & Technology Clinic at Georgetown Law's Institute for Public Representation. Prior to that, she worked at New America's Open Technology Institute and Public Knowledge. Laura completed her J.D. at NYU School of Law and her LL.M. at Georgetown. Before law school, Laura analyzed cell site location information for the Manhattan District Attorney's Office.

IX. COPYRIGHT