DOMAIN AWARENESS SYSTEM

AYYAN ZUBAIR

SEPTEMBER 26, 2019

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

Domain Awareness System

Ayyan Zubair

Background

Imagine the government tracking your license plate throughout the city while you run errands. During your morning run around the neighborhood, facial recognition cameras scan your face at every street corner. Now, picture all that information constantly updated into a city-wide database accessible to the police, immigration enforcement, and even private corporations.

Thanks to the NYPD's Domain Awareness System (DAS), formed through a public-private partnership with Microsoft, what was once the subject of dystopian imagination is now an everyday reality for New Yorkers. DAS uses cameras, license plate readers, and radiological sensors to create a real-time surveillance map of New York City.[1] This system partners with privately-owned CCTV cameras throughout New York City, and instantly compares data with multiple non-NYPD intelligence databases.[2] DAS video files are stored for at least one month, and metadata and license plate data are stored for at least five years—possibly indefinitely.[3]

New York blurs the lines of accountability by staffing its DAS headquarters in lower Manhattan with both police and employees of what it refers to as "private stakeholders"; Goldman Sachs, Pfizer, and Citigroup representatives all frequent the command center as part of their business continuity planning.[4]

Racial Bias

DAS is particularly concerning considering given the NYPD's history of discrimination. Three notorious killings of unarmed Black men have come to symbolize the NYPD's record of discriminatory policing. In 1999, four NYPD officers shot Amadou Diallo, an unarmed Guinean immigrant, 41 times in his apartment building.[5] In 2006, NYPD officers shot Sean Bell 50 times,

---

[1] *See* ADAM MARTIN, *NYPD, Microsoft Hope to Make a Mint off New Surveillance System*, THE ATLANTIC, Aug. 8, 2012, https://www.theatlantic.com/national/archive/2012/08/nypd-microsoft-hope-make-mint-new-surveillance-system/324924/.

[2] *See* NEAL UNGERLEIDER, *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" With Real-Time CCTV, License Plate Monitoring*, FAST COMPANY, Aug. 8, 2012, https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito.

[3] See NYPD, NYPD Public Security Privacy Guidelines, http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf.

[4] *See id.*

[5] *See* JANE FRISCH, *The Diallo Verdict: The Overview; 4 Officers In Diallo Shooting Are Acquitted of All Charges*, N.Y. TIMES, Feb. 26, 2000, https://www.nytimes.com/2000/02/26/nyregion/diallo-verdict-overview-4-officers-diallo-shooting-are-acquitted-all-charges.html.

killing him just hours before his wedding.[6] In 2014, an NYPD officer placed Eric Garner in an apparent "choke hold," ignoring his 11 pleas for air—"I can't breathe."[7] Beyond its use of deadly force, the NYPD implemented a discriminatory "stop-and-frisk" program throughout the 2000s that increased stops by more than five-fold and almost exclusively targeted New Yorkers of color.[8]

In 2011, a bombshell AP report found significant evidence[9] that the NYPD conducted widespread religious profiling of Muslim New Yorkers.[10] For example, the NYPD deployed informants and undercover personnel without warrants to investigate Muslims in mosques, coffee shops, and even their homes for merely practicing their faith.[11] Over 95% of NYPD intelligence investigations targeted Muslim New Yorkers and associated entities.[12] Furthermore, the NYPD routinely surveils Black Lives Matter protestors and other civil rights activists.[13] This pattern of discriminatory surveillance chills New Yorkers' constitutional rights, A system as powerful and invasive as DAS can only magnify the impact of inequalities in policing like those that have plagued the NYPD.

Immigration Enforcement

DAS's dystopian surveillance tools serve as a boon to immigration enforcement agencies. Newly released documents reveal that ICE creates watchlists using DAS data to track undocumented immigrants.[14] The NYPD has contracted for years with the private firm Vigilant Solutions to record over one million license plates per day. Vigilant Solutions doesn't just contract with local police departments—it also shares its nationwide database of over two million data points with ICE. U.S. Customs and Border Protection (CBP) contracts with another private firm, Perceptics, to purportedly photograph millions of vehicles annually at border crossings.[15] In a reminder of how easily private data ostensibly collected for law-enforcement purposes can fall into other hands, CBP

---

[6] *See* MICHAEL WILSON, *Judge Acquits Detectives in 50-Shot Killing of Bell*, N.Y. TIMES, April 26, 2008, https://www.nytimes.com/2008/04/26/nyregion/26bell.html?rref=collection%2Ftimestopic%2FBell%2C%20Sean&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=40&pgtype=collection.

[7] *See* AL BAKER, *BEYOND THE CHOKEHOLD: THE PATH TO ERIC GARNER'S DEATH*, N.Y. TIMES, JUNE 13, 2015, https://www.nytimes.com/2015/06/14/nyregion/eric-garner-police-chokehold-staten-island.html.

[8] N.Y.C. Local Law No. 71 § 1 (2013), https://www1.nyc.gov/assets/cchr/downloads/pdf/amendments/Int_1080_2013_bias_profiling.pdf; in 2013, a federal judge held that NYPD's policies and practices on "stop, question, and frisk" violated the Fourth and Fourteenth Amendments, primarily because the Court found that those policies and practices resulted in the disproportionate and discriminatory stopping of hundreds of thousands of Black and Latino people. The Court issued an order specifying remedies and appointed a federal monitor to oversee implementation of the Court orders and the parties' agreements. The Court also required that NYPD "begin tracking and investigating civilian complaints related to racial profiling and other allegations of bias" committed by officers. *See generally Floyd v. City of N.Y.*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013)..

[9] For an in-depth review of Muslim surveillance by the NYPD, *see Raza v. City of New York*, 998 F. Supp. 2d 70 (E.D.N.Y. 2013).

[10] *See Handschu v. Police Dep't of N.Y.*, 219 F. Supp. 3d 388 (S.D.N.Y, 2016).

[11] *See id.*

[12] *Id.* at 1.

[13] *See, e.g.*, MARK MORALES & LAURA LY, *Released NYPD Emails Show Extensive Surveillance of Black Lives Matter Protesters* , CNN, https://www.cnn.com/2019/01/18/us/nypd-black-lives-matter-surveillance/index.html.

[14] *See* ZACH WHITTAKER, *ICE Has a Huge License Plate Database Targetting Immigrants, Documents Reveal*, TECH CRUNCH, March 13, 2019, https://techcrunch.com/2019/03/13/ice-license-plates-immigrants/.

[15] *See Colleen Long, Customs Says Hack Exposed Traveler, License Plate Images, Associated Press, June 10, 2019, https://www.nytimes.com/aponline/2019/06/10/us/politics/ap-us-customs-traveler-data-breach.html.*

revealed in June 2019 that a cyberattack on Perceptics had compromised almost 100,000 of those border-crossing license plate photos.[16]

Constitutional Concerns

DAS infringes on New Yorkers' right to be free from warrantless surveillance. The NYPD's partnership with Microsoft erodes the most powerful check against law enforcement overreach: limited police resources.[17] In decades past, police departments simply could not track every single New Yorker since it took dozens of officers and several thousand dollars to keep tabs on a single suspect.[18] DAS's relative affordability—and real-time ability to share millions of data points—has allowed the NYPD to treat every resident of the city as a perpetual suspect.

The Supreme Court has weighed in twice in recent years on the warrantless use of tracking technology by law-enforcement agencies. In the 2012 case of *U.S. v. Jones*, the court unanimously struck down warrantless GPS tracking of vehicles.[19] In a concurrence, Justice Sotomayor went so far as to say that location tracking by the government could be "inimical to democratic society."[20] Notably, the GPS technology at issue in Jones was used for only 4 weeks, in contrast to DAS's perpetual tracking of millions of residents.

In 2018, in *Carpenter v. U.S.*, the court struck down extended warrantless searches of cell phone location logs.[21] Just as in *Jones*, the Court spoke to the constitutional right to location privacy,[22] even when that data is collected by a phone company or other "third party."[23][24] Even Chief Justice Roberts felt it went too far to allow the government to track every single American's movements without a warrant.[25] But this is *exactly* what DAS does.

Legislative Action

Local and state lawmakers have proposed legislation to provide safeguards against DAS. In 2018, New York City Council Member Vanessa L. Gibson introduced "The Public Oversight of Surveillance Technology" (POST) Act, which would require the NYPD to disclose how it uses

---

[16] Id.
[17] *Illinois v. Lidster*, 540 U.S. 419, 426(2004)
[18] DAS represents artificial surveillance without limitation—far from the limited police trailing available when the Supreme Court held over 50 years ago in *Katz v. U.S.* that there is no reasonable expectation of privacy on a public road. *See Katz v. U.S.*, 389 U.S. 347, 353 (1967).
[19] *See generally U.S. v. Jones*, 565 U.S. 400 (2012).
[20] *See id.* at 416 (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (CA 2011)).
[21] *See Carpenter v. U.S.*, 138 S.Ct. 2206 (2018).
[22] *See id.* at 2216 (finding that "much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled").
[23] According to the third party doctrine, personal information loses all protection when exposed to any third party, such as a bank or phone company. *See Katz*, *supra* note 25 at 351 (holding that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection").
[24] *Id.* at 2217 (holding that "[g]iven the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection").
[25] *Id.* at 2218 (noting that "because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when").

electronic surveillance tools.[26] While the POST Act does not mandate City Council approval for new surveillance technology, its passage will require the NYPD to at least disclose basic information about how the technology will be deployed.

In June 2019, New York State Senator Andrew Gounardes introduced S6428, which would create a statewide task force on the role of artificial intelligence in New York State Government.[27] If enacted, S6428's 15-member task force would review how state agencies use artificial intelligence tools to make decisions about policing, education, state hiring, and other areas of government operations.

Meanwhile, legislatures across the country have created protocols to ensure that automated license plate readers (ALPRs)—an integral DAS tool—and other surveillance technologies are not misused. In 2015, California passed S.B. 34, requiring agencies that use ALPRs to protect data, maintain access logs, and implement a usage and privacy policy.[28] This law also prohibits public agencies from selling, sharing, or transferring ALPR data to private companies.[29] Also in 2015, Minnesota placed strict limits on license plate readers, including limits on who can be tracked using ALPRs and which entities the data may be shared with.[30] Minnesota also bars law-enforcement agencies from capturing images of a vehicle's occupants, a practice that has become increasingly common in New York and other jurisdictions.[31]

Conclusion

DAS is an unparalleled invasion of New Yorkers' privacy rights. It operates like Big Brother—tracking New Yorkers' every movement throughout the five boroughs. Through its partnership with Microsoft, the NYPD has acquired a hitherto unimaginable ability to surveil New Yorkers anytime, anyplace. Local, state, and federal legislatures must act swiftly to curb this Orwellian surveillance tool.

[26] *See* NEW YORK CITY COUNCIL, *Int. No. 487*, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0&Options=ID%7cText%7c&Search=The+Public+Oversight+of+Surveillance+Technology.
[27] *See* NEW YORK STATE SENATE, *S6428*, https://www.nysenate.gov/legislation/bills/2019/s6428.
[28] See California State Senate, SB34, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB34.
[29] See id.
[30] See Minnesota State Senate, SB86, https://legiscan.com/MN/bill/SF86/2015.
[31] See id.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT