OPINION

GUEST ESSAY

# The N.Y.P.D. Is Teaching America How to Track Everyone Every Day Forever

**By Elizabeth Daniel Vasquez**
**Illustrations by Wesley Allsbrook**
Ms. Daniel Vasquez was a public defender in Brooklyn and Washington, D.C. She now runs the Forensic Evidence Table, a nonprofit focusing on the intersection of criminal law, technology and science.

Sept. 15, 2025

I ran a practice inside Brooklyn's public defense office focused on the police department's use of science and technology, so I am well accustomed to the department's collection of personal information on people being investigated for crimes. But more than a decade of observing traditional police work did not prepare me for what the department is doing today: building vast, hidden repositories of data it collects on everyone in the city, with no clear boundaries on how it can be used. As cities across the country follow New York's lead, I am gravely worried about what this system enables, and the effect on what the Supreme Court justice Louis Brandeis termed our most valued right: the "right to be let alone."

The city's police force has spent more than $3 billion amassing information that reveals where you have been, whom you have interacted with and what you have said, thought and believed. Unlike previous surveillance methods, new digital tools allow law enforcement agencies to conduct surveillance persistently, universally, at an unimaginable scale. They can do so with no special permission, no oversight and no advance planning. The

results amount to a digital time machine that not only makes our past constantly available to law enforcement officers but also can provide them with predictions about our futures.

Traces of this system have surfaced regularly in news reports for years. Journalists at multiple outlets have reported the N.Y.P.D.'s intrusive surveillance on peaceful protests, popular hip-hop shows and kids across the city, all in the name of fighting crime before it occurs. If you commute by car, police algorithms can predict what time you'll likely head home on any given Wednesday and what roads you'll take to get there. The city's computers are constantly passively compiling this information in case it is of use to them later, a version of the film "Minority Report" made real.

The surveillance has reached such a scale that it has begun to erode a large number of people's basic civil rights.

New Yorkers who merely fit certain demographic categories or public profiles may be subjected to a higher number of police interactions, which can result in the loss of their property and peace of mind and endanger them physically. They may lose housing and job or educational opportunities. They may have to curtail the way they move through the city, express themselves and interact with others.

Take a teenager living in the Marcy Houses, a public housing complex in Brooklyn. Simply because of where he lives, if he posts photos with certain classmates or if he tries out certain hashtags, he might be added to the N.Y.P.D.'s gang database, which contains active entries for more than 13,000 people, 99 percent of whom are people of color. If he is active on social media — as almost every teenager is — the N.Y.P.D.'s social media analysis and research team may track him, analyzing and collecting his online activity

and networks. He could be among those who are periodically contacted on social media by undercover detectives impersonating other teenagers.

Even if there is no suspicion that this particular young man has engaged in any crime, his presence on that database exposes him to a level of monitoring previously reserved for intensive undercover operations targeting organized crime.

Once targeted, as Jumaane Williams, New York City's public advocate, has warned, someone in this situation might experience repeated and regular police stops. A minor infraction that would normally be ignored, or at worst result in a ticket or summons, could turn into hours of questioning about his social networks and his neighborhood and communities. Being taken to the station for questioning also often means having his cellphone seized. The N.Y.P.D. disclosed that in 2024 alone, it seized and kept more than 24,000 cellphones.

If you knew that your son actively risked being labeled a gang member because of his proximity to certain kids in his class, would you want to move him to a different school? If you anticipated that police officers could track your presence at a rally in Washington Square Park — and then open their phones to find your address in Brooklyn — would you think twice about attending?

Think of the effect on kids of being randomly approached by officers outside their houses, addressed by name and asked knowing questions about their family members, schools and jobs. Too many of our city's children are left looking over their shoulders and wondering who has been talking about them. Paranoia spreads like a contagion.

Information obtained in these interactions — from the seized cellphones and the seized children — gets added to the N.Y.P.D.'s databases, feeding the system of surveillance all over again.


EXH-1222


Even if you regard widespread surveillance as a reasonable precaution against crime, there is no way to be sure how this data could be used in the future, and no system in place to protect or regulate it.

To consider but one possible scenario, today, abortion is legal in New York. But in many states it is not, and some of them are actively considering whether to criminalize out-of-state travel for abortion-related care. No current laws would prevent the federal government from demanding access to the N.Y.P.D.'s data or stop the department from granting it. The system could quickly identify out-of-state cars and people who visit or have visited Planned

Parenthood. Dossiers could easily be generated for each person and then expanded to include information about their travel, social networks, habits and beliefs. From there, it would be easy to create a watch list targeting suspects for further monitoring, stops, questioning and property seizures.

That may seem improbable today. Will it seem that way tomorrow?

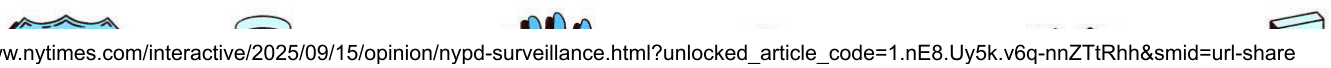
We have all gotten used to advising our children that their actions online leave a permanent trail, and that they should be aware of how their current-day escapades may look to future employers or schools. The threat from a unified repository of our physical and digital lives — maintained by an institution with the power to arrest, jail, banish and even kill — is vastly greater.

We need to talk about our data. Most of all, we need legislation that prohibits law enforcement from pre-emptively collecting and keeping this kind of information in the first place.

Here in New York, the N.Y.P.D. has publicly disclosed using dozens of data collection systems. Once collected, the department says, the data is funneled into a storage and analysis hub called the Domain Awareness System that can retain the information for years, and use it to predict things like where we'll travel or whom we'll be in contact with.

Most of this material — gathered by social media analysis, drone surveillance and more — will never be reviewed by any court and will be entirely inaccessible to anyone outside of law enforcement. For almost 90 percent of the technologies it deploys, the department has stated that it has no obligation to obtain a warrant.

**How the N.Y.P.D. tracks people**




Source: New York City Police Department • Note: List is not exhaustive. • Illustrations by Josie Norton.

Over the past decade, similar approaches to collecting and fusing data have been adopted by police forces around the country, from large jurisdictions such as New Orleans and San Francisco all the way down to Austell, Ga. (population: about 8,000), which maintains a unified database linking surveillance cameras, license plate readers and police files.

The beginning of President Trump's second term, however, has taken this strategy to new levels for the nation as a whole. Early this year, the Department of Government Efficiency started working to break down walls between federal data collections maintained by the Internal Revenue Service, the Social Security Administration, the Centers for Medicare and Medicaid Services and the Department of Veterans Affairs. Aggregating these intentionally separated data sources not only reduces their security but also allows for the instant reconstruction of the sum of

our private lives, with few or no rules on who will have access to it or how it will be used. In March, Mr. Trump issued an executive order explicitly directing all federal agencies to follow suit by eliminating boundaries between the systems they use to collect data on the populations they serve.

The early indications are not good. The federal government has significantly expanded contracts with Palantir, the powerful and secretive surveillance technology company co-founded by Peter Thiel. The U.S. Postal Service has reportedly started cooperating with the Department of Homeland Security to track undocumented immigrants. State and local police officers are collaborating as well.

After reading headlines about DOGE's access to I.R.S. data, my 73-year-old mother asked me if she should get a virtual private network to shield her from this kind of surveillance. It's a reasonable question. But individual actions like deploying a V.P.N., changing your phone's privacy settings or using encrypted messaging apps won't protect you. And they certainly won't empty the data warehouses where your records are already stored.

The only way we can protect ourselves from this extraordinarily intrusive and dangerous practice is by getting our legislators to ban it.

Nearly half of U.S. states have data privacy laws, but all of them contain carve-outs for law enforcement and national security. We urgently need to create guardrails for when and how government agents like the N.Y.P.D. are allowed to collect our data, who in government can have it, what they can use it for and how long they can keep it. For a culture that values personal freedom and private ownership, nothing would be more American than a law that confirms that we each own our own information.

Should our legislatures continue to fail to act, the only barrier to weaponizing these unconscionably powerful tools of surveillance will be our leaders' respect for our shared values of liberty and

democracy. The second Trump administration has shown us how frail that bulwark is.

Additional production by Shoshana Schultz, Gus Wezerek, Michelle Pera-McGhee and Matt Daniels.