Written by **Joe Wolverton, II, J.D.** on September 9, 2018

NYPD Surveillance Software Sorts Images by Skin Color

New York City police have given facial recognition software developers access to surveillance footage including the faces of millions of New Yorkers and vistitors, none of whom had any idea they were being recorded or that those images would be passed on to private corporations for research and development.

An investigative report conducted by The Intercept and The Investigative Fund reveals that the New York City Police Department has been using technology fine tuned by tech giants to sort through the millions of faces collected by the cameras the department has placed all over the Big Apple.

The technology developed by IBM and others enables New York law enforcement to "search camera footage for images of people by hair color, facial hair, and skin tone."

Yep. That's right. The Progressive Capital that is New York City is using ubiquitous surveillance cameras to filter faces based on skin color.

In response to questions asked it by The Intercept, the NYPD issued the following statement via e-mail:

> Video, from time to time, was provided to IBM to ensure that the product they were developing would work in the crowded urban NYC environment and help us protect the City. There is nothing in the NYPD's agreement with IBM that prohibits sharing data with IBM for system development purposes. Further, all vendors who enter into contractual agreements with the NYPD have the absolute requirement to keep all data furnished by the NYPD confidential during the term of the agreement, after the completion of the agreement, and in the event that the agreement is terminated.

Not a single one of the people whose face was recorded and shared by the NYPD was aware he was being watched, much less that his face was being sent to Silicon Valley scientists to be used as R&D data.

When The Intercept asked the NYPD for an explanation of this apparent abuse of the surveillance technology it deploys throughout the nation's largest city, the response was predictably paltry. The Intercept reported last week that NYPD claimed that:

> "various elected leaders and stakeholders" were briefed on the department's efforts "to keep this city safe," adding that sharing camera access with IBM was necessary for the system to work. IBM did not respond to a question about why the company didn't make this collaboration public. [NYPD spokesman Peter] Donald said IBM gave the department licenses to apply the system to 512 cameras, but said the analytics were tested on "fewer than fifty." He added that IBM personnel had access to certain cameras for the sole purpose of configuring NYPD's system, and that the department put safeguards in

> place to protect the data, including "non-disclosure agreements for each individual accessing the system; non-disclosure agreements for the companies the vendors worked for; and background checks."

The IBM software was been deployed by New York City leaders as part of the Domain Awareness System — a technology developed by Microsoft that collected and collated the images recorded by all the surveillance devices in lower and midtown Manhattan. The surveillance data was collected by: "cameras, license plate readers, and radiation detectors." Then, this information was made available to officers in "a unified dashboard."

With the devices deployed throughout the city — the need for the increased surveillance was "an easy selling point" in New York City in the days after the terrorist attacks of September 11, 2001 — the people appearing in the images recorded became nothing more or less than guinea pigs for the scientists at IBM who were working on improving their algorithms. The goal was to expand the capacity of the collection software to a point where they could collect images and "to identify suspicious objects and persons in real time in sensitive areas."

As the technology became increasingly complex and increasingly able to distinguish hair color, facial hair, and gait, some developers at IBM began to wonder to what unintended ends their technology could be put.

The Intercept piece includes a statement from one of the developers who shared this concern.

"We were certainly worried about where the heck this was going," recalled Rick Kjeldsen, a former IBM researcher. "There were a couple of us that were always talking about this, you know, 'If this gets better, this could be an issue.'"

According to the information provided by NYPD insiders to The Intercept, the department refused to accept software that could be used for racial profiling.

> "While tools that featured either racial or skin tone search capabilities were offered to the NYPD, they were explicitly declined by the NYPD," Donald, the NYPD spokesperson, said. "Where such tools came with a test version of the product, the testers were instructed only to test other features (clothing, eyeglasses, etc.), but not to test or use the skin tone feature. That is not because there would have been anything illegal or even improper about testing or using these tools to search in the area of a crime for an image of a suspect that matched a description given by a victim or a witness. It was specifically to avoid even the suggestion or appearance of any kind of technological racial profiling." The NYPD ended its use of IBM's video analytics program in 2016, Donald said.

That's not quite how Kjeldsen remembers the events:

> Kjeldsen, the former IBM researcher who helped develop the company's skin tone analytics with NYPD camera access, said the department's claim that the NYPD simply tested and rejected the bodily search features was misleading. "We would have not explored it had the NYPD told us, 'We don't want to do that,'" he said. "No company is going to spend money where there's not customer interest."
>
> Kjeldsen also added that the NYPD's decision to allow IBM access to their cameras was crucial for the development of the skin tone search features, noting that during that period, New York City served as the company's "primary testing area," providing the company with considerable environmental diversity for software refinement.
>
> "The more different situations you can use to develop your software, the better it's going be,"

> Kjeldsen said. “That obviously pertains to people, skin tones, whatever it is you might be able to classify individuals as, and it also goes for clothing.”

Upon learning of the potential of the NYPD-tested surveillance tech, other places came forward and requested that the software be installed in their cameras. One such prospective client was California State University, Northridge.

Here’s Cal State Northridge’s experience, according to The Intercept’s report:

> “We were able to pick up where they were at different locations from earlier that evening and put a story together, so it saves us a ton of time,” Vanscoy said. “By the time we did the interviews, we already knew the story and they didn’t know we had known.”
>
> Glavin, the chief of the campus police, added that surveillance cameras using IBM’s software had been placed strategically across the campus to capture potential security threats, such as car robberies or student protests. “So we mapped out some CCTV in that area and a path of travel to our main administration building, which is sometimes where people will walk to make their concerns known and they like to stand outside that building,” Glavin said. “Not that we’re a big protest campus, we’re certainly not a Berkeley, but it made sense to start to build the exterior camera system there.”

Some will be question why such information should be made instantly available to law enforcement. Why shouldn’t police have at their command all relevant data about potential perpetrators?

One word: Constitution!

The Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

We must insist that no surveillance be conducted without the consent of those being watched. Furthermore, there can be no sharing of the data with large corporations for use in research and development.

Finally, the knowledge that there are potentially hundreds of law enforcement agencies around the country that can instantly sift through the hours and hours of surveillance images to select only “black” people, “white” people, “Arabic” people, etc., should give pause to those of us still committed to restoring constitutionally protected liberty.

We must not be tricked into laying our liberty on the altar of safety, for we will wind up without either.

Photo: JayLazarin/iStock Unreleased/Getty Images