Connecticut Debate Association

October 12, 2019

AITE and Oxford High School

Resolved: The US should significantly limit the use of facial recognition systems.

Study Urges Tougher Oversight for Police Use of Facial Recognition

By Daniel Victor, The New York Times, Oct. 18, 2016

A new report by a think tank at Georgetown University calls for greater oversight in the use of emerging facial recognition software that makes the images of more than 117 million Americans — a disproportionate number of them black — searchable by law enforcement agencies.

While the agencies, including the F.B.I., have historically created fingerprint and DNA databases primarily from criminal investigations, many of the photographs scattered among agencies at all levels of government are of law-abiding Americans, according to the report released Tuesday.

The report found that 16 states allowed law enforcement officials to compare the faces of suspects to photographs on driver's licenses and other forms of identification without a warrant, "creating a virtual lineup."

"This is unprecedented and highly problematic," said the report, by the Center on Privacy and Technology at Georgetown's law school.

Facial recognition technology, long used overseas by the American military and intelligence agencies in Iraq and Afghanistan, is seen by local law enforcement as a tool for identifying criminals, but it has also raised concerns among privacy advocates.

Because African-Americans disproportionately come into contact with, and are arrested by, law enforcement officials, the report said, their police photos will most likely be overrepresented in facial recognition databases.

The authors of the report said the aim was not to stop the use of the software, which they acknowledged had been effective in investigations. Nor did they fault law enforcement officers, who they said "are simply using every tool available to protect the people that they are sworn to serve."

Rather, they called for Congress and state legislatures to pass laws creating stricter regulations on the technology. Researchers found, for instance, that just one agency — the Ohio Bureau of Criminal Investigation — specifically prohibited using the software to track people engaging in political or religious speech. No state has a law regulating use of the software.

"There is a real risk that police face recognition will be used to stifle free speech," the report said.

In a statement, the F.B.I. said it "has made privacy and civil liberties integral to every decision since the inception of its use of facial recognition technology, establishing practices that protect privacy and civil liberties beyond the requirements of the law."

When the algorithms identify a candidate based on matching facial patterns, the results must go through two layers of human review before the person is suggested to an investigator, according to the statement.

"It is crucial that members of the law enforcement community have access to advanced biometric technologies to accurately investigate, identify, apprehend, and prosecute terrorists and criminals," the statement said.

The report found that systems relying on police photographs have a greater effect on African-Americans because they are arrested at higher rates.

But the software may be less accurate with images of black people, and there is no independent testing for racially biased errors, it said.

These were among the steps the authors suggested taking:

■ Databases should rely on police photographs, not driver's licenses and photo IDs.

■ Law enforcement should occasionally eliminate innocent people from any search.

■ Searches of driver's license and ID photos should require a court order and be limited to serious crimes, with the exception of identity theft and fraud cases.

■ An explicit ban should be enacted against tracking people on the basis of political or religious beliefs, race or ethnicity.

The report raised concerns about the increasing use of facial recognition software on live video, letting the police continuously scan faces on surveillance cameras. Several large police departments have looked into or have begun using the technology, the report said.

"If deployed pervasively on surveillance video or police-worn body cameras, real-time face recognition will redefine the nature of public spaces,” the report warned.

How Facial Recognition Makes You Safer

By James O’Neill, The New York Times, June 9, 2019

Mr. O’Neill is the New York police commissioner.

Used properly, the software effectively identifies crime suspects without violating rights.

In 1983, when I was sworn in as a police officer, many of the routine tasks of the trade would have seemed more familiar to a cop from my grandfather’s day than to a new police academy graduate today. I took ink fingerprints on paper cards and used a Polaroid camera for mug shots. Reports were handwritten or typed on carbon triplicates. Biological evidence could be analyzed only in terms of blood type.

Technology has improved the profession beyond what the most imaginative officer could have conceived in those days. These innovations include facial recognition software, which has proved its worth as a crime-fighting resource since we adopted it in 2011. But the technology has also raised concerns about privacy, so the public should know how the New York Police Department uses its system — and the safeguards we have in place.

When detectives obtain useful video in an investigation, they can provide it to the Facial Identification Section, of the Detective Bureau. An algorithm makes a template of the face, measuring the shapes of features and their relative distances from each other. A database consisting solely of arrest photos is then searched as the sole source of potential candidates — not photos from the Department of Motor Vehicles, Facebook, traffic cameras or the myriad streams of close-circuit TV video from around the city. Facial “landmarks” are compared without reference to race, gender or ethnicity.

After the software generates a list of possible matches, an investigator assesses their resemblance to the suspect. If one is selected, a review is conducted by detectives and seasoned supervisors, noting similarities and differences. If they affirm the match, the investigator proceeds with further research, including an examination of social media and other open-source images.

We might find social media images of a person at a birthday party wearing the same clothing as the suspect in a robbery. That person then becomes a lead; the facial identification team will provide only a single such lead to the case detective. Leads provided by the unit are comparable to tips to our Crime Stoppers hotline — no matter how compelling, they must be verified to establish probable cause for an arrest. No one can be arrested on the basis of the computer match alone.

In 2018, detectives made 7,024 requests to the Facial Identification Section, and in 1,851 cases possible matches were returned, leading to 998 arrests. Some investigations are still being conducted and some suspects have not been apprehended.

But in many cases there have been clear results. Recently, the work of the facial identification team led to the arrest of a man accused of raping a worker at a day spa, and another charged with pushing a subway passenger onto the tracks. We have made arrests in murders, robberies and the on-air assault of a TV reporter. A woman whose dismembered body was found in trash bags in two Bronx parks was identified. So was a woman hospitalized with Alzheimer’s, through an old arrest photo for driving without a license.

The software has also cleared suspects. According to the Innocence Project, 71 percent of its documented instances of false convictions are the result of mistaken witness identifications. When facial recognition technology is used as a limited and preliminary step in an investigation — the way our department uses it — these miscarriages of justice are less likely.

We have never put police sketches into the system; they would be of no value. We have used editing software to substitute a generic feature when a suspect is closing his eyes or sticking out his tongue in the submitted photo. The system can also create a mirror image of the right side of a face if we have only the left side, for example, to produce a 3-D model.

We use these methods solely to fill in missing or distorted data. And when we do so, we bring an additional degree of scrutiny to the process. To compare this to filling in a partial fingerprint, as the Georgetown Center for Privacy and Technology did in a recent report, is absurd. It makes sense to create an image of a suspect’s left ear using his right ear as a model. But it is impossible to infer the shape of a nose from the shape of a chin. As the algorithm is constantly improving in its ability to read lower-quality images, the editing software is used less and less frequently.

The department does not conduct civil immigration enforcement, and neither does our Facial Identification Section. But we do work with other police departments when appropriate. A recent request from the F.B.I. led to the identification of a child sex trafficker who advertised his services on social media.

Biometric technology is no longer new. It is routinely used everywhere from shopping malls to doctors’ offices. Its application by the department is carefully controlled and its invaluable contributions to police investigations have been achieved without infringement on the public’s right to privacy. When cases using this technology have been prosecuted, our methods and findings are subject to examination in court.

Facial recognition technology can provide a uniquely powerful tool in our most challenging investigations: when a stranger suddenly commits a violent act on the street. In the days of fingerprint cards and Polaroid mug shots, these crimes defined New

York City, for visitors and residents alike.

Though far rarer now, they remain life-altering, and sometimes life-ending, events. To keep New York City safe requires enormous and relentless effort. It would be an injustice to the people we serve if we policed our 21st-century city without using 21st-century technology.

San Francisco Is Right: Facial Recognition Must Be Put On Hold

By Farhad Manjoo, The New York Times, May 16, 2019

The technology is unregulated and rife with error. We shouldn't deploy it without strong privacy rules.

What are we going to do about all the cameras? The question keeps me up at night, in something like terror.

Cameras are the defining technological advance of our age. They are the keys to our smartphones, the eyes of tomorrow's autonomous drones and the FOMO engines that drive Facebook, Instagram, TikTok, Snapchat and Pornhub. Cheap, ubiquitous, viral photography has fed social movements like Black Lives Matter, but cameras are already prompting more problems than we know what to do with — revenge porn, live-streamed terrorism, YouTube reactionaries and other photographic ills.

And cameras aren't done. They keep getting cheaper and — in ways both amazing and alarming — they are getting smarter. Advances in computer vision are giving machines the ability to distinguish and track faces, to make guesses about people's behaviors and intentions, and to comprehend and navigate threats in the physical environment. In China, smart cameras sit at the foundation of an all-encompassing surveillance totalitarianism unprecedented in human history. In the West, intelligent cameras are now being sold as cheap solutions to nearly every private and public woe, from catching cheating spouses and package thieves to preventing school shootings and immigration violations. I suspect these and more uses will take off, because in my years of covering tech, I've gleaned one ironclad axiom about society: If you put a camera in it, it will sell.

That's why I worry that we're stumbling dumbly into a surveillance state. And it's why I think the only reasonable thing to do about smart cameras now is to put a stop to them.

This week, San Francisco's board of supervisors voted to ban the use of facial-recognition technology by the city's police and other agencies. Oakland and Berkeley are also considering bans, as is the city of Somerville, Mass. I'm hoping for a cascade. States, cities and the federal government should impose an immediate moratorium on facial recognition, especially its use by law-enforcement agencies. We might still decide, at a later time, to give ourselves over to cameras everywhere. But let's not jump into an all-seeing future without understanding the risks at hand.

What are the risks? Two new reports by Clare Garvie, a researcher who studies facial recognition at Georgetown Law, brought the dangers home for me. In one report — written with Laura Moy, executive director of Georgetown Law's Center on Privacy & Technology — Ms. Garvie uncovered municipal contracts indicating that law enforcement agencies in Chicago, Detroit and several other cities are moving quickly, and with little public notice, to install Chinese-style "real time" facial recognition systems.

In Detroit, the researchers discovered that the city signed a $1 million deal with DataWorks Plus, a facial recognition vendor, for software that allows for continuous screening of hundreds of private and public cameras set up around the city — in gas stations, fast-food restaurants, churches, hotels, clinics, addiction treatment centers, affordable-housing apartments and schools. Faces caught by the cameras can be searched against Michigan's driver's license photo database. Researchers also obtained the Detroit Police Department's rules governing how officers can use the system. The rules are broad, allowing police to scan faces "on live or recorded video" for a wide variety of reasons, including to "investigate and/or corroborate tips and leads." In a letter to Ms. Garvie, James E. Craig, Detroit's police chief, disputed any "Orwellian activities," adding that he took "great umbrage" at the suggestion that the police would "violate the rights of law-abiding citizens."

I'm less optimistic, and so is Ms. Garvie. "Face recognition gives law enforcement a unique ability that they've never had before," Ms. Garvie told me. "That's the ability to conduct biometric surveillance — the ability to see not just what is happening on the ground but who is doing it. This has never been possible before. We've never been able to take mass fingerprint scans of a group of people in secret. We've never been able to do that with DNA. Now we can with face scans."

That ability alters how we should think about privacy in public spaces. It has chilling implications for speech and assembly protected by the First Amendment; it means that the police can watch who participates in protests against the police and keep tabs on them afterward.

In fact, this is already happening. In 2015, when protests erupted in Baltimore over the death of Freddie Gray while in police custody, the Baltimore County Police Department used facial recognition software to find people in the crowd who had outstanding warrants — arresting them immediately, in the name of public safety.

But there's another wrinkle in the debate over facial recognition. In a second report, Ms. Garvie found that for all their alleged power, face-scanning systems are being used by the police in a rushed, sloppy way that should call into question their results.

Here's one of the many crazy stories in Ms. Garvie's report: In the spring of 2017, a man was caught on a security camera stealing beer from a CVS store in New York. But the camera didn't get a good shot of the man, and the city's face-scanning system returned no match.

The police, however, were undeterred. A detective in the New York Police Department's facial recognition department thought the man in the pixelated CVS video looked like the actor Woody Harrelson. So the detective went to Google Images, got a picture of the actor and ran his face through the face scanner. That produced a match, and the law made its move. A man was arrested for the crime not because he looked like the guy caught on tape but because Woody Harrelson did.

Devora Kaye, a spokeswoman for the New York Police Department, told me that the department uses facial recognition merely as an investigative lead and that "further investigation is always needed to develop probable cause to arrest." She added that "the N.Y.P.D. constantly reassesses our existing procedures and in line with that are in the process of reviewing our existent facial recognition protocols."…

…In a bizarre twist, some police departments are even pushing the use of facial recognition on forensic sketches: They will search for real people's faces based on artists' renderings of an eyewitness account, a process riddled with the sort of human subjectivity that facial recognition was supposed to obviate.

The most troubling thing about all of this is that there are almost no rules governing its use. "If we were to find out that a fingerprint analyst were drawing in where he thought the missing lines of a fingerprint were, that would be grounds for a mistrial," Ms. Garvie said.

But people are being arrested, charged and convicted based on similar practices in face searches. And because there are no mandates about what defendants and their attorneys must be told about these searches, the police are allowed to act with impunity.

None of this is to say that facial recognition should be banned forever. The technology may have some legitimate uses. But it also poses profound legal and ethical quandaries. What sort of rules should we impose on law enforcement's use of facial recognition? What about on the use of smart cameras by our friends and neighbors, in their cars and doorbells? In short, who has the right to surveil others — and under what circumstances can you object?

It will take time and careful study to answer these questions. But we have time. There's no need to rush into the unknown. Let's stop using facial recognition immediately, at least until we figure out what is going on.

Facial Recognition Tech Comes to Schools and Summer Camps

By Julie Jargon, The Wall Street Journal, Updated July 30, 2019 12:19 pm ET

Facial recognition is no longer just being used to unlock iPhones, tag Facebook friends and scan crowds for security threats. It's moving into summer camps, youth sports tournaments and schools.

Parents at summer camps across the country can opt into facial-recognition services to receive photos of their camper without having to sift through hundreds of group shots for proof that little Susie is having a good time climbing ropes. One facial-recognition software manufacturer has proposals in front of several K-12 public school districts to install the technology to help identify and track potential shooters on campus…

Are You Ready for Facial Recognition at the Airport?

By Scott McCartney, The Wall Street Journal, Updated Aug. 14, 2019 8:58 am ET

Airlines and TSA are starting to scan faces to get people through security and boarding faster, as privacy advocates warn of unintended consequences

Travelers have to face a new reality—their faces are rapidly becoming their IDs and boarding passes at airports.

Facial recognition is rolling out at boarding gates for international flights at big airports in Europe, Asia and the U.S., even as privacy concerns about the technology grow….

Facial Scans at U.S. Airports Violate Americans' Privacy, Report Says

By Ron Nixon, The New York Times, Dec. 21, 2017

WASHINGTON — A new report concludes that a Department of Homeland Security pilot program improperly gathers data on Americans when it requires passengers embarking on foreign flights to undergo facial recognition scans to ensure they haven't overstayed visas.

The report, released on Thursday by researchers at the Center on Privacy and Technology at Georgetown University's law school, called the system an invasive surveillance tool that the department had installed at nearly a dozen airports without going through a required federal rule-making process.

The report's authors examined dozens of Department of Homeland Security documents and raised questions about the accuracy of facial recognition scans. They said the technology had high error rates and were subject to bias, because the scans often fail to properly identify women and African-Americans…

Homeland security officials said the program was necessary and fulfilled a decades-old congressional requirement to prevent foreign visitors from overstaying their visas.

John Wagner, deputy executive assistant commissioner for field operations at Customs and Border Protection, said American travelers could ask to be inspected other than by a facial scan before boarding flights. He said that at least 90 percent of the scans had correctly identified faces, and that the agency had not encountered gender or racial bias problems with the technology…..

A Major Police Body Cam Company Just Banned Facial Recognition

By Charlie Warzel, The New York Times, June 27, 2019

Mr. Warzel is an Opinion writer at large.

Its ethics board says the technology is not reliable enough to justify using.

Axon, the company that supplies 47 out of the 69 largest police agencies in the United States with body cameras and software, announced Thursday that it would ban the use of facial recognition systems on its devices…

In a 28-page report, Axon's ethics board, which was handpicked by members of the Policing Project at New York University School of Law, argued that the technology "does not perform as well on people of color compared to whites, on women compared to men, or young people compared to older people."

The report also cautioned that facial recognition is especially prone to inaccuracy when used with police body cameras, which frequently operate in low-light conditions and produce shaky footage…..

A.I. Experts Question Amazon's Facial-Recognition Technology

By Cade Metz and Natasha Singer, The New York Times, April 3, 2019

SAN FRANCISCO — At least 25 prominent artificial-intelligence researchers, including experts at Google, Facebook, Microsoft and a recent winner of the prestigious Turing Award, have signed a letter calling on Amazon to stop selling its facial-recognition technology to law enforcement agencies because it is biased against women and people of color…

…In January, two researchers at the Massachusetts Institute of Technology published a peer-reviewed study showing that Amazon Rekognition had more trouble identifying the gender of female and darker-skinned faces in photos than similar services from IBM and Microsoft. It mistook women for men 19 percent of the time, the study showed, and misidentified darker-skinned women for men 31 percent of the time.

Before publishing their findings on Amazon Rekognition, the M.I.T. researchers released a similar study examining services from IBM, Microsoft and Megvii, an artificial-intelligence company in China. All three updated their services to address concerns raised by the researchers.

In separate blog posts from the Amazon executives Matthew Wood and Michael Punke, the company disputed the study and a Jan. 24 article in The New York Times describing it.

"The answer to anxieties over new technology is not to run 'tests' inconsistent with how the service is designed to be used, and to amplify the test's false and misleading conclusions through the news media," Dr. Wood wrote. Amazon did not directly engage with the M.I.T. researchers…..

How China Uses High-Tech Surveillance to Subdue Minorities

By Chris Buckley and Paul Mozur, The New York Times, May 22, 2019

KASHGAR, China — A God's-eye view of Kashgar, an ancient city in western China, flashed onto a wall-size screen, with colorful icons marking police stations, checkpoints and the locations of recent security incidents. At the click of a mouse, a technician explained, the police can pull up live video from any surveillance camera or take a closer look at anyone passing through one of the thousands of checkpoints in the city.

To demonstrate, she showed how the system could retrieve the photo, home address and official identification number of a woman who had been stopped at a checkpoint on a major highway. The system sifted through billions of records, then displayed details of her education, family ties, links to an earlier case and recent visits to a hotel and an internet cafe.

The simulation, presented at an industry fair in China, offered a rare look at a system that now peers into nearly every corner of Xinjiang, the troubled region where Kashgar is located.

This is the vision of high-tech surveillance — precise, all-seeing, infallible — that China's leaders are investing billions of dollars in every year, making Xinjiang an incubator for increasingly intrusive policing systems that could spread across the country and beyond.

Have No Fear of Facial Recognition

By Andy Kessler, The Wall Street Journal, Aug. 4, 2019 5:51 pm ET

If it is bound by good legal protections, the technology is a boon, not a tool for tyranny.

Englishman Francis Galton first noted the unique arches, loops and whorls in our fingerprints back in the 1880s. Thirty years later, Clarence Hiller confronted an intruder in his Chicago home and was fatally shot. The culprit fled, but not before leaving a fingerprint in fresh paint on a railing. Thomas Jennings became the first defendant convicted using fingerprints as evidence. This is now routine, but back then there was public hysteria over the fingerprint's invasion of privacy and then questionable accuracy.

Today, with faces matched almost instantly via machine learning and artificial intelligence, fears of Big Brother have created similar hysteria—especially after Georgetown legal scholars discovered last month that Immigration and Customs Enforcement has access to driver's license photos from 21 states.

So much so that the crime-ridden cities of San Francisco and Oakland, Calif., along with Somerville, Mass., have banned the use of facial recognition by law enforcement, even though local businesses can use it to track who enters and leaves their buildings. Pretty crazy.

Paranoid? Is someone watching you? Let's get some constitutional rights out of the way first, especially "unreasonable searches and seizures." In Katz v. U.S. (1967), the Federal Bureau of Investigation used an electronic eavesdropping device, attached to the outside of a phone booth, to record the defendant's gambling transactions. Charles Katz won and the Supreme Court ruled that in a phone booth, "like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy." On the flip side, the justices held that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."

But we are still protected against dragnets (dum du dum dum)—the use of cameras or other surveillance to track collectively where everyone goes and what they do. Even in public, where you have no reasonable expectation of privacy, law enforcement can't record everything in hope that someone commits a crime. The USA Patriot Act weakened some of these protections, but the 2015 USA Freedom Act fixed that.

There's added hysteria around the potential bias in facial recognition's mistakes. About a year ago, the American Civil Liberties Union did a study, using Amazon's Rekognition tool, in which it ran photos of members of Congress against a database of 25,000 arrest mug shots. It falsely matched 28 congressmen, 40% of whom were "people of color." The headlines blared: "Facial recognition's racial bias problem."

But if you read the fine print, the ACLU admits that it "used the default match settings that Amazon sets for Rekognition," which is an 80% confidence level. Amazon reran the study with 30 times as many mug shots and the 99% confidence threshold they recommend for law enforcement use and the "misidentification rate dropped to zero." You probably missed the media's retractions.

To see if this technology is any good, I spoke to someone who actually uses it, Capt. Chuck Cohen of the Indiana State Police. He reminisced about the bad old days of passing around grainy videotapes from security cameras asking if "anyone recognized this guy." He tells me facial recognition is another tool in the forensic shed, along with fingerprints, tire imprints, partial license plates and DNA. He stressed repeatedly that he doesn't consider facial recognition as evidence in court, only as a lead in investigations.

Capt. Cohen says it works. During a physical altercation, someone was shot in the stomach and the victim's friend recorded phone video. Facial recognition identified the shooter, which was the lead police needed to find more evidence to nab the suspect. In another disturbing case, with explicit video, someone sexually harassed and extorted young girls. Police used facial recognition to identify 14 of 22 victims, who were carefully interviewed. They eventually identified the offender.

Hundreds of crimes have been solved. From other sources, I've heard that Alabama security cameras picked up a 90-year-old woman being robbed and beaten by an African-American woman. Police considered lineups, the proverbial usual suspects. Instead they used facial recognition and found the man who did it. You read that right: The culprit was a cross-dressing man, something a lineup would never have found.

The Chinese have powerful facial-recognition tools, SenseTime and Megvii. We know Beijing uses technology for mass surveillance, especially against the Muslim Uighurs. How do we safeguard U.S. citizens against similar abuses? Rather than banning its use, we need strong silos. Such protections exist today. Try getting President Trump's tax returns. Try finding the guy who cut you off with a license-plate number. Cops can't do extended surveillance without a judge's warrant. We can make databases inaccessible except with a judge's consent. Heck, use the judge's face as the ID.

Facial recognition will only get better. But we ought to can the hysteria. So long as the tech is properly limited in use to avoid fishing expeditions, we'll all be safer.