Who Owns Your Face? New York Joins Rising Efforts to Protect Biometric Privacy

By Alana Galloway

Imagine you're taking your annual winter holiday trip to New York City with 16 family members—your spouse, children, grandchildren, parents-in-law, and even your brother-in-law from Florida. You and your group visit Rockefeller Center to see the tree before heading to Radio City Music Hall to watch the Rockettes perform in the 2022 Christmas Spectacular. Once in the door, you hurry to stock up on snacks and sodas before the show begins. Everything seems fine, until you're approached by two men in the lobby, neither of whom identify themselves. They ask you if you're Johnathan D'Agostino, the lawyer. You are. But you also run a music publishing company. You confirm your name, say you work with a music publishing company and show them your ID in confusion. They walk off. But when you get to your seat—popcorn in hand and grandkids in tow—security is waiting, ready to escort you out. This is exactly what happened to Jonathan D'Agostino of D'Agostino & Associates Dec. 2, 2022.

D'Agostino is a personal injury attorney in Staten Island, Brooklyn, New York City, and New Jersey. He is currently working on a case for a client who fell and injured themself at Radio City. D'Agostino was identified and escorted out of Radio City on this basis.

According to D'Agostino, he was unaware he wasn't allowed at Radio City. He says security responded that this is standard policy and that they are not allowing anyone from his organization on properties until the litigation is resolved. By law, D'Agostino has a right to go to the area where his client fell, take photos, and speak to witnesses. Attending the Rockettes performance at Radio City wouldn't have provided D'Agostino any benefit he wouldn't otherwise have.

"It denied me a memory with my family," D'Agostino said. "It created confusion for my grandchildren who are 7, 4, and 2 who wanted to know why I wasn't with them and why I was escorted to the sidewalk. It was embarrassing."

When D'Agostino asked security how they identified him, they said they used facial recognition software. A sign at Radio City indicates the venue's use of such software, but D'Agostino did not see it. Parent company MSG Entertainment began using facial recognition software in 2018 but use of the technology to identify lawyers and restrict their access did not begin until 2021.

This case and others like it have raised questions that are being asked throughout New York and across the country. When is facial recognition technology (FRT) use acceptable, and by who? And, should citizens be entitled to a private right of action, meaning the right to file personal lawsuits against companies that violate their privacy rights, when biometrics are concerned?

The earliest pioneers of FRT began using computers to identify the human face in 1964. However, FRT did not truly advance until 2010—the epoch of technology categorized as Web 2.5, the era of social media growth and the mobile web. In 2010, Facebook incorporated facial recognition functionality into its platform to help users tag friends in photos. This feature was immediately controversial, triggering an onslaught of articles grappling with privacy concerns. But use of the technology continued. In 2017 Apple's iPhone incorporated FaceID software, an

option users can use to unlock their phones. Today, this technology is used from border patrol and police to airports and stadiums.

However, all facial recognition firms are not cohesively restricted in regard to product-development. There is no bigger example than Clearview AI. Founded in 2017, the U.S.-based facial recognition firm began scraping over 20 billion photographs from the Internet and social media sites, which it then compiled into a database. Clearview AI then built out an algorithm which it utilized to match faces to the database. The company remained largely unknown until late-2019, when it began selling its database to corporations, law enforcement, universities, and private citizens.

In the US, there is no federal biometric privacy law. And, only three states—Illinois, Texas, and Washington—have enacted biometric laws. Of these states, only the Illinois Biometric Information Privacy Act (BIPA), an initiative led by the ACLU of Illinois and passed unanimously by the Illinois legislature in 2008, ensures individuals a private right of action. Under BIPA, individuals are legally entitled to control their biometric information. Private companies are not allowed to acquire it without first notifying the person involved in writing. This notification must provide clear information about the type of data being collected or stored (e.g. a fingerprint for a bank account app on a phone), specify the purpose of the data collection and the length of time it will be used (e.g. the fingerprint will be kept for six months to make logging into the app easier), and must obtain the individual's written consent (e.g. the user must sign their name before giving their fingerprint).

On May 28, 2020, the American Civil Liberties Union (ACLU), the ACLU of Illinois, and the legal firm Edelson PC sued Clearview AI, alleging a breach of Illinois residents' privacy rights under BIPA in its means of obtaining biometric information without subjects' consent. The ACLU argued this case under BIPA as it is the only biometric law in the United States that includes a private right of action.

Subsequent to the settlement agreement and release resulting from *ACLU v. Clearview AI, Inc.*, in 2022, widespread use of Clearview technology has changed. Clearview AI is no longer permitted to sell access to its faceprint database to private enterprises and other entities anywhere in the country under the terms of the deal. Furthermore, the corporation is prohibited from working with any government or law enforcement agency in Illinois for the next five years. Clearview has agreed that it will no longer provide free trial memberships to individual police officers unless their employer agency expressly authorizes it.

Nathan Freed Wessler, Deputy Director of the ACLU Speech, Privacy, and Technology Project, said while the ACLU is pleased with the outcome of the settlement, “It does not answer every question about Clearview’s business model, use and collection of peoples’ unique biometric identifiers but it puts meaningful restraints on the company.”

However, he said, “continued police use of this technology outside of Illinois raises really serious privacy concerns.”

Indeed, even with this lawsuit won, FRT remains in use throughout the US. And, other companies like PimEyes, a comparable face search engine based in Seychelles, are compiling and selling similar databases. PimEyes does not have controls in place to restrict searches and users can run any photo they would like through the system for a match. To test the server, I ran four images of myself through the server, and PimEyes retrieved 25 images of me on the web. I would have had to pay $14.99 to “Unlock full access to the current search results,” meaning the photos’ sources and original websites of the search. However, I recognized them as images of me online—my LinkedIn profile picture, old Facebook profile photos, a few press images, two images only featured on my Private Instagram, and one image of a woman who is certainly not me. Twenty-four of 25 photos were me.

Wessler believes that PimEyes, like Clearview, is “a tremendous threat to privacy. And because it’s based outside of the US it’s a lot harder to get at them under US privacy laws.”

Despite rising concerns, nearly 80 percent of countries “have some government use of facial recognition” and 7 in 10 governments have “growing, widespread, or invasive use of FRT.” according to data compiled by comparitech tech writer, privacy advocate and VPN expert Paul Bischoff.

“Pros are going to maintain [FRT] is unbiased, maintains fast reading of features, can be transparent—used then destroyed–and coupled with heat sensitive finger scanning it can authenticate who people are in a fast manner,” said Sarvesh Ramprakash, Communications Chair of Restore the Fourth, a non-profit organization devoted to restoring the Fourth Amendment to the U.S. Constitution and preventing unlawful mass government surveillance. “The against [argument] is generally saying that this is a dystopian technology and that it's prone to misidentification, it's biased, discriminatory, and leads to loss of privacy.”

Of the arguments against FRT, misidentification is among the most concerning due to its potentially life-changing repercussions.

For instance, imagine you're driving to a belated Thanksgiving dinner with your mom, on your front lawn in the company of your spouse and children, leisurely paused at a traffic stop, or paying a cordial visit to police 30 miles out of town. Abruptly, you're arrested for a crime you didn't commit. You're taken to prison on the basis of false evidence and, just like that, your whole life is derailed by court cases and attorney fees. What's worse? The mistaken identifications are not made by man, but rather by machine. You're fighting with a computer; with an algorithm.

All of the above happened to four men who reside across America, living in diverse circumstances. Despite their similar skin color—black—they had little in common. Until each was wrongly tagged by facial recognition technology (FRT) and accused of crimes they did not commit.

In Jan. 2019, police accused Nijeer Parks, 35, who works at a grocery store in Paterson, New Jersey, of stealing from a Hampton Inn gift shop in Woodbridge, New Jersey. Police reports cite that the shoplifter left a fake ID at the scene, which was run through a facial recognition system to falsely identify Parks as a "high profile" match. Parks was held for ten days, then dismissed due to insufficient evidence after paying about $5,000 to defend himself.

Police issued a warrant for Michael Oliver, 28, four months later and arrested him at a traffic stop in July 2019 in Ferndale, Michigan. He was taken into custody on the basis of allegedly taking a teacher's smartphone to record a fight outside a school, then tossing it on the ground. The teacher in question shared a screenshot from the video, which police used to falsely identify Oliver, who was at work when the crime occurred.

In Jan. 2020, Detroit police handcuffed and arrested Robert Julian-Borchak Williams, 42, who lives in Farmington Hills, Michigan, in front of his wife, Melissa, and their two young daughters, then ages 2 and 5. The cause? A crook—someone, but not Williams—stole five watches at the Detroit Midtown Shinola store in 2018. The Wayne County police detained Williams for 30 hours, then released him on bail until the court hearing, when charges were dropped due, again, to a lack of evidence.

Another mistake occurred nearly three years later in Nov. 2022 with the DeKalb County, Georgia arrest of Randal Reid, 28, a transportation analyst in Atlanta, Georgia.

Reid had never been to Louisiana when facial recognition linked him to $10,000 worth of purse thefts in Jefferson Parish and Baton Rouge, according to Reid's attorney, Tommy Calogero. When Calogero received the police report and the perpetrator's photo they used to identify Reid,

he said the faces were nearly identical. But, “the perpetrator had flabby arms,” Calogero said. “My client was a slim guy and the perp looked like a big guy. And [Reid] didn’t have a mole the way the perpetrator did.”

Police arrested Reid on Nov. 25 and released him Dec. 1 because of a mole it took authorities six days to notice.

“He was very frightened. Very, very upset. He was afraid he was going to lose his job,” Calogero said.

In the case of Williams, Wayne County police used FRT to link surveillance video footage to his old driver’s license photo. The Michigan State Police Investigative Lead Report includes a dark, grainy probe image where the perpetrator’s features are unidentifiable.

In a 2021 interview with the Detroit News, Williams said, "I held that piece of paper up to my face and said, 'I hope you don't think all Black people look alike.'"

The ACLU is particularly outspoken about the danger of face surveillance tools and how this danger is amplified by flawed algorithmic production of biased and inaccurate results, especially skewed by race.

“The technology is racially biased, but even if it were 100% accurate it poses severe civil rights and privacy concerns that it should not be in the hands of police,” NYCLU Senior Privacy & Technology Strategist Daniel Schwarz said, in an interview. “And it's shrouded in secrecy so oftentimes people affected by the systems don’t even know that they were identified with facial recognition.”

Joy Buolamwini, a researcher in the MIT Media Lab’s Civic Media group, created a dataset to calculate errors and disparities among gender and race with the use of FRT. Buolamwini’s findings indicated that gender was far more likely to be misidentified in darker-skinned males and females than in their lighter-skinned counterparts. For instance, algorithms misidentified only about one percent of lighter-skinned males’ gender, whereas they misidentified about 12 percent of darker-skinned males’ gender. For females, gender was misidentified for about seven percent of lighter-skinned females, while it was misidentified in about 35 percent of darker-skinned females.

Facial recognition isn’t only being used to identify potential criminals. It’s being used to identify almost everyone.

In New York City, efforts have been made to limit its use. On July 9, 2021, New York City Council amended its administrative code to regulate business use of biometric identifier information (BII) within the city. This law aims to protect New York City residents and visitors by limiting how commercial establishments may gather, use, share and store biometric identifiers. About two weeks later, on July 29, the council passed the Tenant Data Privacy Act (TDPA) to place additional regulations on "smart access" building owners' use of biometric information.

Still, Radio City acted within the law. The current legal landscape that led to what D'Agostino experienced in the presence of his family could, he said, lead to unexpected or unintended chilling effects.

"When someone calls me and says, 'Hi I was injured at Radio City Music Hall,' I shouldn't have to think twice about whether or not I want to take that case because it's going to subject my lawyers to this sort of penalty," D'Agostino said. "The ones who suffer are the ones who are calling looking for representation. They might be turned down by firms who say, 'It's not worth not being able to go to a Rangers game. Or a Knicks game. Let them call another lawyer.'"

And D'Agostino isn't the only lawyer whose life has been impacted negatively by facial recognition. Kelly Conlon, a senior associate at New Jersey personal injury firm Davis, Saperstein and Salomon, was also planning to see the Christmas Spectacular show at Radio City Music Hall with her daughter, a Girl Scout, and her Girl Scout friends, when security stopped her on the account of facial recognition. Conlon's law firm, like D'Agostino's, represents a client suing a restaurant owned by Madison Square Garden Entertainment Corporation. Security relayed the same message to Conlon as to D'Agostino: that she was not allowed on their property until the lawsuit ended. Conlon waited outside for the girls.

"It illustrates the larger issue of this surveillance industrial complex," Schwarz said, referring to the D'Agostino and Conlon cases. "We need to have meaningful biometric privacy protections that at a minimum require informed obtained consent from people."

On Jan. 24, New York Attorney General Letitia James sent a letter, written by Civil Rights Bureau member Kyle S. Rapiñan, Esq., to MSG to investigate its use of facial recognition software to deny entry to certain ticket holders. In this letter, Rapiñan says The New York State Office of the Attorney General (OAG) reviewed reports revealing MSG's use of FRT to identify lawyers representing litigation against the company and prevent them from entering their venues.

According to the letter, approximately 90 law firms have been affected by the Company's Policy, impacting thousands of lawyers.

James asked MSG to provide evidence of compliance with all applicable federal, state, and local laws prohibiting discrimination and retaliation. James is also requesting that MSG report the measures it is taking to adhere to New York's civil and human rights laws, as well as to ensure that their technology does not result in discriminatory behavior. MSG previously claimed that the policy was necessary to prevent lawyers from gathering evidence inside its venues to support their legal claims, but James warned that it may discourage legitimate cases against the company.

In a Jan. 26 interview on *FOX 5's Good Day New York*, MSG CEO James Dolan defended the company's use of FRT. A press release accompanied this broadcast statement, in which MSG described the attorneys it's refusing entry to as "ambulance chasers and money grabbers whose business is motivated by self-promotion and who capitalize on the misfortune of others."

On Feb. 6, 2023, MSG released another statement regarding its "adverse attorney policy," which bans lawyers involved in lawsuits against the company. MSG published this subsequent to the publicity Conolon's case received. The policy no longer applies to lawyers tied to pending litigation with Tao Group Hospitality, which consists of around three dozen restaurants and clubs in the city, as the company is attempting to sell the bar and restaurant group. This amendment does not apply to other locations, like Radio City or MSG. And the company has not commented on potential flaws in the technology.

D'Agostino said his daughter, Jenna D'Agostino, planned to attend the Jingle Ball at MSG with her sister-in-law on Dec. 9, 2022. But, he said, "they walked through security and immediately someone pointed and said, 'that one with the red hair.' They pulled her aside immediately and said she wouldn't be allowed to see the concert because she's part of D'Agostino." Jenna is a D'Agostino in that she shares her father's surname, but she is not associated with D'Agostino & Associates, as this security guard suggested. In fact, Jenna is licensed in Tennessee, not New York.

FRT worked on Jenna in this instance in that it identified her, yet the technology lacked proper insight into her circumstances.

"We have twin concerns about this technology. It's dangerous when it works and dangerous when it doesn't work," Wessler, of the ACLU, explained.

“Dangerous when it doesn’t work because of the potential for false matches that can lead to false arrests or to someone being ejected from a store when they’re falsely matched to a prior shoplifter that they actually have nothing to do with,” he said. “Dangerous when it does work since there’s potential for pervasive government surveillance—a system that’s able to instantaneously identify anyone and everyone as they’re walking around in public.”

Though it has received considerable publicity and backlash in the past few months, MSG is not alone in its increased use of FRT for event entry. In fact, the use of face recognition technology at sporting events is also on the rise, driven by the need to quickly authenticate ticket holders. In 2018, the same year MSG began using FRT, the New York Mets and New York Yankees were among nine Major League Baseball stadiums that took part in a biometric identification trial with Clear, a company that provides identity verification services at airports in the US and Canada.

The Mets started using the technology with select season ticket holders, and come March 2023, when the season starts, all fans will have access to the face recognition system in order to get into Citi Field. The Mets plan to use the technology for other purposes, such as paying for food and drink, but it is not designed to limit access to any group. Ticketmaster and ASM Global, which operates over 300 stadiums and entertainment venues, have also tested the technology in order to reduce wait times for ticket holders. Although civil rights groups have raised concerns about potential misuse and privacy concerns, stadium and entertainment center operators are using face recognition to reduce wait times, scalping, and the need for physical contact with public surfaces.

“There’s trade associations for high tech companies and legislatures saying these technologies provide a service,” said Adam Schwartz, Senior Staff Attorney and Assistant Director of the Electronic Frontier Foundation, a leading non-profit organization focused on protecting civil rights in the digital sphere. “One big issue that’s in conflict is whether there should be a private right of action.” Schwartz explained that industry hates private rights of action and that there is a big debate at the federal level about whether to enact a comprehensive data privacy law.

At the federal level, FRT is in wide use. According to a 2021 survey conducted by the U.S. Government Accountability Office, an examination of 24 federal agencies about their use of FRT found that 16 agencies use FRT for cybersecurity or digital access purposes, such as enabling staff members to use it to unlock agency devices. Five agencies reported utilizing it for physical security, such as regulating access to a building or facility, six agencies reported using it to produce leads in criminal investigations, and ten agencies said that they expected to increase the use of FRT. Eighteen of the 24 agencies examined responded to GAO's survey FRT activities in fiscal year 2020 and stated that they used an FRT system for cybersecurity, digital access,

national law enforcement, use of commercial systems (like PimEyes) that match against publicly available photographs, and/or for physical protection.

The ACLU has been suing the Department of Homeland Security, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA) for the release of information on FRT use and safeguards, or lack thereof, since 2020. It is additionally in an ongoing Freedom of Information Act lawsuit against the FBI. Documents obtained through this lawsuit reveal how the FBI and the Defense Department have been actively involved in research and development of facial recognition software, despite the fact that three states and more than a dozen cities had passed laws prohibiting or limiting the technology's utilization by law enforcement.

New York State law enforcement, in particular, has been utilizing FRT for years. According to the New York Police Department, its Facial Identification Section received 9,850 requests to identify murder, rape, felony assault, robbery, and grand larceny cases in 2019 and identified 2,510 potential matches. Online, the NYPD states they know of "no case in New York City in which a person was falsely arrested on the basis of a facial recognition match."

Yet that same year, the Georgetown Law Center on Privacy and Technology uncovered that the NYPD was using questionable methods such as substituting images of celebrities for those of suspects, altering the photos of the suspects to the extent that their real appearances were changed, and arresting people solely off of face recognition matches without carrying out any further investigations. And in Aug. 2020, facial recognition software was used to pinpoint Derrick Ingram, a Black Lives Matter activist, through a photo taken from his Instagram account during a protest against police brutality.

Email documents, obtained by Muckrock journalist Rachel Richards and the Legal Aid Society Jan. 2021, reveal a three-year relationship between the NYPD and Clearview AI during which the NYPD ran over 5,100 searches with Clearview AI. This indicates the state's use of FRT not only on a company level, but also on a law enforcement level. Should the police maintain access to FRT? Should Madison Square Garden and similar corporations?

For the purpose of this article, at least three dozen NYPD addresses listed on the Muckrock documents were emailed requesting a statement admitting or denying continued use of Clearview. No one replied.

On Jan. 19, New York State lawmakers in the Senate and the Assembly introduced the "Digital Fairness Act." This bill stipulates that any entity conducting business in New York and managing

the personal information of 500 or more individuals must provide clear and concise notice regarding their use of this information. Additionally, it limits the information that may be collected and requires it to be kept secure and shared only with authorized parties. Furthermore, it prohibits the processing of biometric data, and allows consumers to take private legal action if their rights are violated. The bills remain in committee.

Schwarz and the NYCLU are proponents of the Digital Fairness Act. “It would create comprehensive privacy protection,” Schwarz said. “It would protect our civil rights and civil liberties in the digital age, it would ensure that digital technologies cannot be used to circumvent our civil rights and civil liberties protections.”

New York City's Biometric Information Privacy Law, effective since July 2021, forbids the trading of biometric identifier information (BII) for commercial gain, including the sale, rental, or exchange of biometric data. It establishes a private right of action for parties whose data is illegally sold.

Apart from NYC’s ban aimed at businesses, 17 local bans restrict government use of face recognition. And, since the start of the 2023 legislative session, 11 states have proposed 15 new biometric privacy laws. These bills would necessitate that businesses comply with stricter rules when dealing with biometric data. And many of the proposals have the potential to significantly boost the legal responsibility and risk of companies handling biometric information. States proposing new laws include Arizona, Hawaii, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, New York, Tennessee, Vermont, and Washington.

California, Colorado, Connecticut, Utah, and Virginia have also passed laws that regulate the processing of biometric information and aim to mitigate data breaches.

At the national level, Schwartz is watching the American Data Privacy Protection Act (ADPPA), which is on the House floor in Congress. The proposed bill would create uniform national guidelines and protections for government-issued identification and personal data, including biometric information, collected by businesses. This legislation is seen as a major step forward in the effort to establish federal regulations for data privacy in the US. Several other federal bills have been proposed in recent years to address issues with algorithmic decision-making, though the ADPPA is the first to gain considerable bipartisan backing and to combine provisions regarding algorithmic fairness and data security. Most notably, the ADPPA introduces a private right of action at the national level.

A hurdle for private right of action thus far, Schwartz said, is that industry and Republicans tend to hate it. Yet with so many new bills and laws proposed and cases such as D'Agostino's and false recognition gaining media attention, data privacy proponents remain forward-thinking.

"I hope that with the recent publicized cases it's a wakeup call; that lawmakers realize the urgent need for real protections comprehensively on all privacy issues but specifically on biometric privacy," Schwarz said.