FACIAL RECOGNITION AI[*]

MARGARET HU[**]

The integration of algorithmic decisionmaking and artificial intelligence ("AI") into facial recognition technology poses new, unprecedented risks to privacy and individual autonomy rights, particularly in urban settings. The murder of Brian Thompson, CEO of UnitedHealthcare, in New York City on December 4, 2024, provides a timely case study to examine the deployment of facial recognition systems by the New York Police Department and other law enforcement agencies to identify the suspect. New York City deploys some of the most sophisticated surveillance architecture in the nation, put into place following the terrorist attacks of September 11, 2001. This Article explores the utilization of facial recognition systems and facial recognition AI in the investigation of Thompson's murder. Ultimately, because of its limitations, facial recognition AI failed to assist law enforcement in identifying the suspect, Luigi Mangione, who was apprehended less than one week later through non-AI identification: a customer at a McDonald's restaurant in Altoona, Pennsylvania, alerted a McDonald's employee, who then reported the suspect to the local police. The benefits of facial recognition AI are uncertain, and its efficacy is largely unproven and untested. Facial recognition technology is largely unregulated and poses significant constitutional concerns. Specifically, this Article contends that the compelled deanonymization of individuals in urban settings results in diminished constitutional protections. It concludes that examining the European Union's approach to AI oversight offers an important comparative perspective on regulatory approaches to facial recognition AI.

[**] Davison M. Douglas Professor of Law, Director, Digital Democracy Lab, William & Mary Law School. Very grateful to Eisha Jain for the opportunity to participate in this Symposium volume, exploring the critically important topic of criminal records in the digital age, and for the dedicated research support of Angelina Han, Courtney Lange, Davi Liang, Xueyan Liu, and Katie Smart. I would like to express my deepest appreciation for the editorial leadership and care of the *North Carolina Law Review*, including Meyke Kang, Samuel Lahne, and Andrew Parco.

INTRODUCTION

Law enforcement increasingly relies upon facial recognition technology to make identity-based assessments and predict threats.[1] The high-profile shooting of Brian Thompson, CEO of UnitedHealthcare, on December 4, 2024, provides a useful case study of the operationalization of facial recognition data collection and other visual data image capture, and the deployment of facial recognition artificial intelligence ("AI") by law enforcement in urban contexts.[2] Thompson

[1] *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1115–26 (2021); KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE 7, 13 (2011); Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1533 tbl.13 (2013) [hereinafter Hu, *Biometric ID*]; Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1, 1 (2020); Shlomit Yanisky-Ravid & Kyle Fleming, *The Tripartite Model of Facial Recognition: Bridging the Gap Between Privacy, Public Safety, Technology and the Fourth and First Amendments*, 37 NOTRE DAME J.L. ETHICS & PUB. POL'Y 159, 159 (2023); Amanda Levendowski, *Resisting Face Surveillance with Copyright Law*, 100 N.C. L. REV. 1015, 1015 (2022); Samuel D. Hodge, Jr., *The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector*, 71 DEPAUL L. REV. 731, 737 (2022); Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33, 35 (2019) [hereinafter Selinger & Hartzog, *Inconsentability of Facial Surveillance*]; Henry H. Perritt, Jr., *Defending Face-Recognition Technology (And Defending Against It)*, 25 J. TECH. L. & POL'Y 41, 55–56 (2020); Woodrow Hartzog, Evan Sellinger & Johanna Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, 101 WASH. U. L. REV. 717, 736–45 (2024); Laura M. Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentification*, 30 WM. & MARY BILL RTS. J. 337, 337 (2021); Jason M. Schultz, *The Right to Publicity: A New Framework for Regulating Facial Recognition*, 88 BROOK. L. REV. 1039, 1041 (2023); Samuel D. Hodge, Jr., *Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century*, 89 U. CIN. L. REV. 30, 30–32 (2020). *See generally* KASHMIR HILL, YOUR FACE BELONGS TO US: A SECRETIVE STARTUP'S QUEST TO END PRIVACY AS WE KNOW IT (2023) (telling a gripping, dystopian story about the rise of Clearview AI and warning about the implications this technological superpower might have on privacy rights); JOY BUOLAMWINI, UNMASKING AI: MY MISSION TO PROTECT WHAT IS HUMAN IN A WORLD OF MACHINES (2023) (recounting Buolamwini's personal experiences in researching and auditing computer vision and facial recognition technology).

[2] Christopher Maag, Ed Shanahan, Andy Newman & Lola Fadulu, *What We Know About the UnitedHealthcare C.E.O.'s Killing and the Suspect*, N.Y. TIMES, https://www.nytimes.com/2024/12/06/nyregion/unitedhealthcare-brian-thompson-shooting.html [https://perma.cc/A7FZ-4M8S (staff-uploaded, dark archive)] (last updated Dec. 20, 2024).

was shot by a gunman in front of the Hilton Midtown Hotel in New York City ("NYC") in the early morning of December 4, 2024, as he was about to enter the hotel to address an annual meeting with UnitedHealthcare shareholders.[3] The suspect, later identified as 26-year-old Luigi Mangione, managed to evade capture for several days, even as the New York Police Department ("NYPD") leveraged one of the most sophisticated surveillance networks in the world.[4] With "more than 18,000 interconnected cameras"[5] across NYC, and a myriad of advanced tools like facial recognition technology, the NYPD sought to piece together the moments leading up to and following the shooting.[6]

Facial recognition AI, however, failed to assist law enforcement in identifying the suspect, Mangione, who was apprehended less than one week later through non-AI identification. The suspect was identified on December 9, 2024, by a customer at a McDonald's restaurant in Altoona, Pennsylvania.[7] The customer alerted a McDonald's employee, who then reported the suspect to the local police.[8]

Nonetheless, the vast surveillance infrastructure throughout the city played an important role in the investigation. The NYPD's Domain Awareness System is one of the largest camera networks in the United States. These cameras, including both public and private systems, are used to monitor the city's streets and identify suspects in criminal investigations. The sophisticated camera networks allow authorities to track individuals in real time or review footage after an incident. The NYPD uses its network to gather hundreds of

[3] *Id.*

[4] *See Technology: Applications and Software*, N.Y. POLICE DEP'T (2025), https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/technology.page [https://perma.cc/67C5-73RT]; *see also* Jonathan Chang & Meghna Chakrabarti, *The Limits of the Surveillance State*, WBUR: ON POINT (Dec. 16, 2024), https://www.wbur.org/onpoint/2024/12/16/surveillance-state-united-health-care-luigi-mangione [https://perma.cc/AL2E-FEXU].

[5] Sydny Shepard, *New Surveillance Cameras to Bolster Security in NYC*, SEC. TODAY (Oct. 29, 2018), https://securitytoday.com/articles/2018/10/29/new-surveillance-cameras-to-bolster-security-in-nyc.aspx [https://perma.cc/V95G-5WC6].

[6] *Surveillance City: NYPD Can Use More than 15,000 Cameras to Track People Using Facial Recognition in Manhattan, Bronx and Brooklyn*, AMNESTY INT'L (June 3, 2021), https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/ [https://perma.cc/6C4Q-N46J] [hereinafter *Surveillance City*]; *see also* Holly Yan, *Why Finding the Suspected CEO Killer Is Harder than You Might Think*, CNN, https://www.cnn.com/2024/12/07/us/suspect-search-unitedhealthcare-ceo [https://perma.cc/WM8K-FJU5] [hereinafter Yan, *CEO Killer*] (last updated Dec. 7, 2024, 7:49 AM); Emily Mae Czachor, *What's the Evidence Against Luigi Mangione in the UnitedHealthCare CEO Shooting, According to Authorities?*, CBS NEWS, https://www.cbsnews.com/news/evidence-luigi-mangione-unitedhealthcare-ceo-shooting/ [https://perma.cc/R2PK-85N3] (last updated Dec. 13, 2024, 4:34 PM).

[7] Holly Yan, *The Suspected UnitedHealthcare CEO Killer Planned His Attack Well – But Made Crucial Mistakes, Experts Say*, CNN, https://www.cnn.com/2024/12/10/us/luigi-mangione-shooter-unitedhealthcare-ceo/index.html [https://perma.cc/EEU7-7MWT] (last updated Dec. 10, 2024, 12:19 PM).

[8] *Id.*

hours of video footage across multiple locations. As the suspect of Thompson's murder carried out his attack and fled the crime scene, he appeared on multiple surveillance cameras positioned throughout NYC.[9]

Facial recognition technology describes a subfield of biometric identification and verification systems that utilize algorithmic and machine learning to match digital images to an individual's identity. "Biometric technologies provide a means to establish or verify the identity of humans based upon one or more physical or behavioral characteristics. Examples of physical characteristics include face, fingerprint, and iris images."[10]

Facial recognition technology is currently largely unregulated and poses significant constitutional concerns. New challenges posed by cybersurveillance systems operating in urban areas, such as the integration of facial recognition AI into law enforcement and other surveillance technologies, require a reexamination of constitutional protections and how they will likely fail to protect the citizenry against abuses.

This Article proceeds in three parts. Part I explains recent innovations in the adoption of facial recognition AI by law enforcement agencies. The investigation surrounding Thompson's murder provides an opportunity to examine the facial recognition AI systems and other surveillance infrastructure that were deployed by the NYPD. This case study illustrates the military-grade surveillance capacities of the NYPD that were adopted after the terrorist attacks of September 11, 2001. Yet, the failure of the facial recognition AI systems to capture Mangione demonstrates the limitations of the technological capacities of AI surveillance.

Part II focuses on the risks of forced urban deanonymization and radical transparency, as increased by innovations in identity management technologies, such as facial recognition technology and sensors that are integrated into city surveillance architectures. This part will explore, in particular, the surveillance capacities of Clearview AI, and how the integration of AI into facial recognition technology serves law enforcement investigations, such as that of the murder of Thompson in NYC.[11]

[9] *Surveillance City*, *supra* note 6.

[10] *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 42 (2020) (statement of Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce).

[11] *See, e.g.*, Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1738 n.2 (2015) [hereinafter Hu, *Blacklisting*]; Glyn Moody, *Details Emerge of World's Biggest Facial Recognition Surveillance System, Aiming to Identify Any Chinese Citizen in Three Seconds*, TECHDIRT (Oct. 18, 2017, 3:30 AM), https://www.techdirt.com/articles/20171017/07423938416/details-emerge-worlds-biggest-facial-recognition-surveillance-system-aiming-to-identify-any-chinese-citizen-three-seconds.shtml [https://perma.cc/6W9J-JXTB (staff-uploaded archive)] (describing a new facial recognition program in China with the goal of identifying any citizen within three seconds); Shai Oster, *China Tries Its Hand at Pre-Crime*, BLOOMBERG (Mar. 3, 2016, 4:24 PM), https://www.bloomberg.com/news/articles/2016-

Part III discusses why this technology is largely unregulated and poses significant constitutional concerns, including new risks to criminal procedure protections under the Fourth, Fifth, and Sixth Amendments. The integration of facial recognition AI into law enforcement systems requires a reexamination of how criminal procedure protections, as currently understood, may not offer adequate safeguards. Urban populations are particularly at risk of diminished constitutional protections. This part examines the Supreme Court's decision in *Carpenter v. United States*[12] to analyze whether the Fourth Amendment's reasonable expectation of privacy test borrows doctrinal elements of First Amendment protections inclusive of anonymity rights, as well as substantive due process rights protected under the Fifth and Fourteenth Amendments.[13]

Despite the significant constitutional risks posed by biometric cybersurveillance systems, currently, facial recognition AI systems such as Clearview AI are only challenged under a combination of consumer privacy and data privacy laws, mostly under state statutes.[14] Increasingly, they are also challenged under data protection and AI regulations enacted by the European Union ("EU").[15] The Article concludes that examining the European Union's approach to AI oversight offers an important comparative perspective on regulatory approaches to facial recognition AI.[16]

I. FACIAL RECOGNITION AI IN URBAN SPACES: A CASE STUDY

To better understand the risks and potential failures of facial recognition AI, it is instructive to examine the investigation of the murder of CEO Brian Thompson within the context of a post-9/11 NYPD and the installation of urban

03-03/china-tries-its-hand-at-pre-crime [https://perma.cc/H8BW-ZH6J (staff-uploaded, dark archive)] (explaining a new data collection program implemented in China); Simon Denyer, *Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/ [https://perma.cc/R76Z-E7BF (staff-uploaded, dark archive)] (describing a new facial recognition program in Chongqing, China and contextualizing it within a global trend toward surveillance); John R. Quain, *Crime-Predicting A.I. Isn't Science Fiction. It's About to Roll Out in India*, DIGIT. TRENDS (June 22, 2018), https://www.digitaltrends.com/cool-tech/could-ai-based-surveillance-predict-crime-before-it-happens/ [https://perma.cc/9697-5JA2] (outlining crime-predicting software to be introduced in India); Yi Shu Ng, *China Is Using AI to Predict Who Will Commit Crime Next*, MASHABLE (July 24, 2017), https://mashable.com/2017/07/24/china-ai-crime-minority-report/ [https://perma.cc/W2YL-PPUA] (describing China's implementation of facial recognition to predict crimes); Justin Lee, *Chinese Facial Recognition Firm Developing AI to Predict Crimes*, BIOMETRICUPDATE.COM (July 25, 2017, 3:36 PM), https://www.biometricupdate.com/201707/chinese-facial-recognition-firm-developing-ai-to-predict-crimes [https://perma.cc/AN3Y-7T3S] (explaining new facial recognition programs to be used by the Chinese government).

[12] 138 S. Ct. 2206 (2018).

[13] *See infra* Part III.

[14] *Id.*

[15] *Id.*

[16] *Id.*

surveillance architecture and AI infrastructure. This case study also demonstrates the lack of anonymization in urban settings that can lead to lesser constitutional protections. Additionally, the inability of facial recognition AI to capture the suspect, Luigi Mangione, raises important constitutional questions regarding the inherent tradeoffs involved in sacrificing data privacy in urban settings when the efficacy of facial recognition AI systems remain largely untested and unproven.

A. *Introduction to Thompson Murder Investigation*

In the immediate aftermath of Thompson's murder, surveillance footage from multiple locations in NYC painted a clear picture of the suspect's movements. Hotel security cameras captured the gunman waiting for Thompson outside the New York Hilton Midtown.[17] He approached the CEO from behind, shooting him twice before fleeing the scene, riding an electric bike into Central Park.[18] Surveillance footage continued to track the suspect through the park and beyond, where he was seen discarding his backpack, taking a taxi, and entering train station, with these and other movements all tracked through the pervasive presence of cameras throughout NYC.[19] Surveillance footage of the suspect captured him in several locations around NYC wearing a hoodie and mask, making it difficult for facial recognition systems to identify him with certainty.[20]

The first images of Mangione emerged from cameras around the scene.[21] Hotel surveillance cameras captured the gunman waiting near the New York Hilton Midtown hotel before approaching Thompson from behind and shooting him at close range.[22] The gunman was seen calmly leaving the scene,[23] blending into the surroundings before riding away on an electric bike,[24] a notable clue that would later help law enforcement track him.[25] As the investigation progressed, the NYPD continued to sift through hours of video footage. Among the most useful images were those captured at the HI New

[17] Maag et al., *supra* note 2.

[18] *Id.*

[19] Deborah Mary Sophia, *Internet Sleuths Hunt for Clues on Murder of UnitedHealth's Brian Thompson*, REUTERS, https://www.reuters.com/world/us/internet-sleuths-hunt-clues-murder-unitedhealths-brian-thompson-2024-12-05/ [https://perma.cc/5SBT-ZKPR (staff-uploaded, dark archive)] (last updated Dec. 5, 2024, 5:01 PM).

[20] *See, e.g.*, Yan, *CEO Killer*, *supra* note 6.

[21] *Id.*

[22] Maag et al., *supra* note 2.

[23] *Id.*

[24] Jeff Capellini, *UnitedHealthcare CEO Murder Suspect Luigi Mangione Indicted by Manhattan District Attorney*, CBS NEWS, https://www.cbsnews.com/newyork/news/unitedhealthcare-ceo-murder-luigi-mangione-court-appearance-brian-thompson/ [https://perma.cc/2JDG-XXQB] (last updated Dec. 18, 2024, 3:31 PM).

[25] *See* Capellini, *supra* note 24.

York City Hostel on Amsterdam Avenue, where Mangione stayed before the killing. Surveillance cameras inside the hostel recorded a moment when the suspect lowered his balaclava, revealing his face to a hostel employee in a seemingly casual moment.[26] This image, despite being taken from an angle and still partially obscured by his hood, was a key breakthrough. It provided authorities with a much-needed lead in identifying the gunman.[27]

In addition to the hostel footage, other cameras showed the suspect in a Starbucks near the crime scene just minutes before the shooting. These cameras provided glimpses of Mangione, but his face was again obscured by his mask. It was not until the images from the hostel were analyzed that the suspect's face became clearly visible. The NYPD released these images to the public, which prompted numerous tips, including a crucial sighting in Altoona, Pennsylvania, where a McDonald's employee recognized Mangione.[28]

Despite his attempt to avoid detection, Mangione's exposure to various cameras, including in the hostel and public spaces, ultimately led to his identification. The NYPD's ability to access and analyze these images quickly played an important role in the investigation but facial recognition technologies did not result in the suspect's eventual capture in Pennsylvania.[29]

B. *Rise of Facial Recognition AI in Post-9/11 NYC*

Facial recognition technology is a form of biometric identification technology.[30] Today, advanced facial recognition technology utilizes AI. Thus, facial recognition technology is now "facial recognition AI."

[26] Rebekah Riess, *What We Know About the Suspect's Movements Before, During and After the Shooting of UnitedHealthcare CEO Brian Thompson*, CNN, https://www.cnn.com/2024/12/07/us/timeline-luigi-magione-ceo-shooting/index.html [https://perma.cc/C4HT-6LCF] (last updated Dec. 11, 2024, 1:12 PM).

[27] *See id.*

[28] *Id.*; Phil Helsel, Tom Winter, Jonathan Dienst & David K. Li, *Timeline: UnitedHealthcare CEO Shooting Suspect Luigi Mangione's Movements Before and After Arrest*, NBC NEWS, https://www.nbcnews.com/news/us-news/timeline-suspect-luigi-mangione-unitedhealthcare-ceo-shooting-rcna183682 [https://perma.cc/9NDS-S7M9 (staff-uploaded archive)] (last updated Dec. 12, 2024, 8:46 AM); Costas Pitas, *Images of Unmasked Suspect in UnitedHealth Executive Shooting Key to Arrest*, REUTERS, https://www.reuters.com/world/us/images-unmasked-suspect-unitedhealth-executive-shooting-key-arrest-2024-12-09 [https://perma.cc/ZE2G-H4AR (staff-uploaded archive)] (last updated Dec. 9, 2024, 6:51 PM).

[29] Pitas, *supra* note 28.

[30] JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007); *see, e.g.*, Koichiro Niinuma, Unsang Park & Anil K. Jain, *Soft Biometric Traits for Continuous Use Authentication*, 5 INST. ELEC. ELECS. ENG'R TRANSACTIONS ON INFO. FORENSICS & SEC. 771, 772 (2010) (defining the characteristics of both "soft" and "hard" biometrics); Margaret Hu, *Bulk Biometric Metadata Collection*, 96 N.C. L. REV. 1425, 1440 (2018) [hereinafter Hu, *Bulk Biometric*] (quoting ENCYCLOPEDIA OF BIOMETRICS 1235 (Stan Z. Li & Anil Kumar Jain eds., 2009)); *id.* at 1441 (quoting VACCA, *supra*, at 3); VACCA, *supra*, at 57.

Biometric-based identification systems, or identity verification systems, essentially use an individual's unique physical or behavioral characteristics to identify or verify the identity of that individual.[31] These systems can collect and analyze both "hard" or "primary biometrics,"[32] as well as "soft" or "secondary" biometrics.[33] Hard biometrics are traditional biometric identifiers, such as scanned fingerprints, facial recognition technology (for example, digital photos and videos), iris scans, and DNA database screening."[34]

Whereas, "soft biometrics," are essentially "anatomical or behavioral characteristic[s] that provide some information about the identity of a person, but [do] not provide sufficient evidence to precisely determine the [individual's] identity."[35] Soft biometric identification systems analyze or determine individual characteristics such as weight, race, skin color, height, age, hair color, or identification of birthmarks, scars, and tattoos. They can verify and analyze behavioral "characteristics [or traits] that are learned or acquired."[36] Such identifiers may also include voice identification or so-called "gait analysis"—analysis of an individual's walking pattern or style.[37]

The public and private sectors often utilize hard and soft biometric data systems as "secure identification and personal verification solutions."[38] Biometric tracking systems can be combined with biographic monitoring systems to surveil individuals and populations. Integrating AI capacities into biometric-biographic systems can facilitate predictive policing. This is because these systems purport not only to verify an individual's identity (*is this person who they claim to be?*), but also to help determine an individual's identity (*who is this person?*), as well as make assessments about that individual's intent (*what are the motivations and predispositions of this person?*).[39] Furthermore, once biometric-biographic data profiles are collected, AI assessments can be shared across

[31] VACCA, *supra* note 30, at 589.

[32] *Id.*

[33] *See, e.g.*, Niinuma et al., *supra* note 30, at 772 (defining the characteristics of both "soft" and "hard" biometrics).

[34] *Id.*

[35] *See* Hu, *Bulk Biometric*, *supra* note 30, at 1440 (quoting ENCYCLOPEDIA OF BIOMETRICS, *supra* note 30, at 1235).

[36] *Id.* at 1441 (quoting VACCA, *supra* note 30, at 3).

[37] *Id.*

[38] VACCA, *supra* note 30, at 57. Vacca does not define hard or primary biometric data; however, he provides a background on biometric technology and verification system standards. Other scholars have noted the experimental nature of soft or secondary biometric characteristics as a way to supplement hard or primary biometric characteristics. Hu, *Bulk Biometric*, *supra* note 30, at 1440 n.58; *see, e.g.*, Balkin, *The Constitution in National Surveillance State*, 93 MINN. 1, 3 (2008).

[39] *See, e.g.*, Toshimaru Ogura, *Electronic Government and Surveillance-Oriented Society* in THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND 270, 270 (David Lyon ed., 2006); Hu, *Biometric ID*, *supra* note 1, at 1491.

entities.[40] This means that data can be shared at the discretion of private or public entities, amongst themselves or other actors.[41]

Over two decades after the 2001 terrorist attacks, the NYPD now relies heavily upon a complex urban surveillance architecture that includes up to 18,000 cameras in NYC, and the deployment of multiple sophisticated facial recognition AI systems, either that it pilots or that it relies upon through its cooperative relationship with federal law enforcement and other state law enforcement agencies.[42] The sophisticated and extensive nature of surveillance infrastructure in NYC is, in part, an outgrowth of a significant investment in facial recognition technologies and surveillance sensors that were put in place as a result of the 2001 terrorist attacks in NYC and in Washington, D.C. After the terrorist attacks of September 11, 2001, the NYPD and other law enforcement agencies across the United States acquired military-grade surveillance technologies.[43] Facial recognition technology was among these military-grade surveillance technologies and, increasingly, facial recognition AI has been adopted by the private sector as well as the public sector for a wide range of policing functions.[44]

In the eyes of many policymakers, AI and the Internet of Things ("IoT") are transformative technologies that can be harnessed to make the nation, states, cities, workplaces, homes, and individual citizens "smarter" and, thus, safer.[45] IoT technologies demonstrate the ubiquity of data generation. By 2020, the number of connected devices in use globally was estimated to be over thirteen billion and is estimated to exceed thirty billion by 2025.[46] The digital economy

[40] *See* Hu, *Bulk Biometric*, *supra* note 30, at 1444.

[41] *See, e.g.*, Margaret Hu, *Biometric Cyberintelligence and the Posse Comitatus Act*, 66 EMORY L.J. 697, 706 (2017) [hereinafter Hu, *Biometric Cyberintelligence*].

[42] Anthony Kimery, *Limitations of FRT Apparent in Search for United Healthcare CEO's Killer*, BIOMETRICUPDATE.COM (Dec. 10, 2024, 5:10 PM), https://www.biometricupdate.com/202412/limitations-of-frt-apparent-in-search-for-united-healthcare-ceos-killer [https://perma.cc/R9G2-C58D] ("Officially, the NYPD says its primary facial recognition tool is provided by DataWorks Plus. However, the department acknowledges the use of other tools for specific purposes . . . .").

[43] *See* Margaret Hu, *Militarized Biometric Data Colonialism* in RACE AND NATIONAL SECURITY 130, 132 (Matiangai V.S. Sirleaf ed., 2023); Hu, *Biometric Cyberintelligence*, *supra* note 41, at 731.

[44] In addition to law enforcement purposes, the founders of Clearview AI speculated that "it could be used to vet babysitters or as an add-on feature for surveillance cameras . . . [or] a tool for security guards in the lobbies of buildings or to help hotels greet guests by name[.]" Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/GSU4-MFGN (staff-uploaded, dark archive)] (last updated Nov. 2, 2021) [hereinafter Hill, *Secretive Company*].

[45] *See* Ryan Budish, *Helping Global Policymakers Navigate AI's Challenges and Opportunities*, MEDIUM (Aug. 13, 2018), https://medium.com/berkman-klein-center/helping-global-policymakers-navigate-ais-challenges-and-opportunities-11b128687cad [https://perma.cc/Y6EE-YGUX (staff-uploaded archive)] (describing how global policymakers can use AI to their benefit but also describing the challenges associated with AI use).

[46] *See* Lionel Sujay Vailshery, *Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide from 2010 to 2025 (in Billions)*, STATISTA (Sept. 6, 2022), https://www.statista.com/statistics/

and IoT facilitate endless data creation, collection, and analysis opportunities through AI and algorithmic-based data analytics.[47] This vast interconnectedness of devices is also ripe with opportunities for data tracking and surveillance.[48] Complex urban environments are often susceptible to complex challenges: higher crime rates, greater burdens on infrastructure, more poverty and greater needs for public assistance, heightened demands for health services, and a need to regulate employment and labor flows, to name a few.[49] These unique challenges mean that urban governments are especially incentivized to embrace surveillance and more efficient algorithmic-driven systems in order to provide services, analyze infrastructure, and stimulate development in the urban communities they regulate.

After the terrorist attacks of September 11, 2001, federal, state, and local law enforcement agencies began utilizing facial recognition technology more frequently.[50] For example, post-September 11, 2001, the U.S. Department of

1101442/iot-number-of-connected-devices-worldwide/ [https://perma.cc/D4NL-J92X (staff-uploaded, dark archive)].

[47] *See, e.g.*, CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 12–13 (2016); Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/H4TH-YZM3]; Julia Angwin & Jeff Larson, *Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say*, PROPUBLICA (Dec. 30, 2016, 4:44 PM), https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say [https://perma.cc/JY2B-CXKY (staff-uploaded archive)]; Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 639–40 (2017).

[48] *See* Uri Gal, *Data Surveillance Is All Around Us, and It's Going to Change Our Behaviour*, CONVERSATION (Oct. 10, 2016, 6:50 PM), https://theconversation.com/data-surveillance-is-all-around-us-and-its-going-to-change-our-behaviour-65323 [https://perma.cc/37LR-T9RY] (describing the expanding world of data surveillance).

[49] *See, e.g.*, Leo Carroll & Pamela Irving Jackson, *Inequality, Opportunity, and Crime Rates in Central Cities*, 21 CRIMINOLOGY 178, 186–88 (1983); Stephen Graham, *Introduction: Cities and Infrastructure Networks*, 24 INT'L J. URB. & REG'L RSCH. 114, 114 (2008); Peter Dreier, *America's Urban Crisis: Symptoms, Causes, and Solutions*, *in* RACE, POVERTY, AND AMERICAN CITIES 79, 80 (John Charles Boger & Judith Wegner eds., 1996); Sandro Galea, Nicholas Freudenberg & David Vlahov, *Cities and Population Health*, 60 SOC. SCI. & MED. 1017, 1017 (2005); ANNETTE BERNHARDT, RUTH MILKMAN, NIK THEODORE, DOUGLAS HECKATHORN, MIRABAI AUER, JAMES DEFILIPPIS, ANA LUZ GONZÁLEZ, VICTOR NARRO, JASON PERELSHTEYN, DIANA POLSON & MICHAEL SPILLER, BROKEN LAWS, UNPROTECTED WORKERS: VIOLATIONS OF EMPLOYMENT AND LABOR LAWS IN AMERICA'S CITIES 2–5 (2009), https://www.nelp.org/app/uploads/2015/03/BrokenLawsReport2009.pdf [https://perma.cc/UBG5-LHZW].

[50] *See* Douglas Ernst, *U.S. Army Breakthrough: Facial Recognition Technology Now Works in the Dark*, WASH. TIMES (Apr. 16, 2018), https://www.washingtontimes.com/news/2018/apr/16/army-breakthrough-facial-recognition-technology-no/ [https://perma.cc/FH74-RQRY (staff-uploaded archive)] (explaining that the Army can now use facial recognition programs in the dark which allows "humans to visually compare visible and thermal facial imagery through thermal-to-visible face synthesis." (quoting Dr. Benjamin S. Riggan on Association of Research Libraries Public Affairs)). Law enforcement provides the facial recognition software "with an image of an individual they'd like to identify." Dakin Andone, *Police Used Facial Recognition to Identify the Capital Gazette Shooter. Here's How It Works*, CNN (June 29, 2018, 6:22 PM), https://www.cnn.com/2018/06/29/us/facial-recognition-technology-law-enforcement/index.html [https://perma.cc/WN3H-7QPL]. "The

Homeland Security ("DHS") implemented programs whereby state and local law enforcement agencies are required to share data gathered by their biometric identification systems, such as fingerprints, with DHS.[51] This data is specifically screened through DHS and U.S. Federal Bureau of Investigation ("FBI") databases to identify potentially undocumented or watchlist individuals.[52] DHS, the U.S. Department of Justice, and other federal agencies promote biometric tracking programs to support their immigration enforcement and counterterrorism efforts simultaneously.[53]

Surveillance programs included the NYPD post-9/11 program that significantly expanded its facial recognition technologies.[54] Two decades after the 9/11 terrorist attacks, the facial recognition surveillance continues to be used in ordinary policing functions.[55] Facial recognition AI significantly expands cybersurveillance capabilities. Initially, facial recognition technology was "[t]he process of algorithmically cross-referencing two facial images to determine a 'match' [and] is 'not a match between two [biometric] templates, only a degree of statistical closeness.'"[56] The replacement of facial recognition technology

system . . . then checks that image against those uploaded to the system from the state's Motor Vehicle Administration records" and other state records such as inmate records and mugshots. *Id.*; *see also* Katelyn Ringrose & Divya Ramjee, *Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy*, 11 CALIF. L. REV. ONLINE 349, 350–63 (2020) (describing devices used by police, including body-worn cameras, license plate readers, cell-location information, drones, and additional facial recognition technologies and how they are used by law enforcement).

[51] *See, e.g.*, Thomas J. Miles & Adam B. Cox, *Does Immigration Enforcement Reduce Crime? Evidence from Secure Communities*, 57 J.L. & ECON. 937, 938–39 (2014); Adam B. Cox & Thomas J. Miles, *Policing Immigration*, 80 U. CHI. L. REV. 87, 110–34 (2013); Christopher N. Lasch, *Rendition Resistance*, 92 N.C. L. REV. 149, 209–16 (2013).

[52] Department of Homeland Security ("DHS") explains that Secure Communities is justified by a combination of authorities. *See* Memorandum from Riah Ramlogan, Deputy Principal Legal Advisor to Beth N. Gibson, Assistant Deputy Director., U.S. Dep't of Homeland Sec., U.S. Immigr. & Customs Enf't (Oct. 2, 2010), https://uncoverthetruth.org/wp-content/uploads/2012/01/Mandatory-in-2013-Memo.pdf [https://perma.cc/2FFQ-GBGW (staff-uploaded archive)]. DHS relied upon the following: (1) that 28 U.S.C. § 534(a)(1) and 28 U.S.C. § 534(a)(4) together provide the FBI with authority to share fingerprint data with ICE/DHS; (2) that 8 U.S.C.A. § 1722 mandates the development of a data sharing system that "enable[s] intelligence and law enforcement agencies to determine the inadmissibility or deportability of an [undocumented immigrant]"; and (3) that 42 U.S.C. § 14616 ratifies information or database sharing between federal and state agencies. *Id.* at 4.

[53] OFF. OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., DEP'T OF JUST., REVIEW OF DOMESTIC SHARING OF COUNTERTERRORISM INFORMATION 6 (2017), https://oig.justice.gov/reports/2017/a1721.pdf [https://perma.cc/85NV-SUR2].

[54] Ali Watkins, *How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers*, N.Y. TIMES, https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html [https://perma.cc/UU5J-CP9T (staff-uploaded, dark archive)] (last updated June 22, 2023).

[55] *See id.*

[56] *See* Hu, *Bulk Biometric*, *supra* note 30, at 1438 (quoting Marc Valliant, Vice President & Chief Tech. Officer, Animetrics, Presentation Before the NTIA Multi-Stakeholder Process to Develop Consumer Data Privacy Code of Conduct Concerning Facial Recognition Technology: Face Recognition Technology Today (Feb. 25, 2014), https://www.ntia.doc.gov/files/ntia/publications/ntia_feb252014_marcvaillant.pdf [https://perma.cc/3RCB-DYGK (staff-uploaded archive)]).

with facial recognition AI is motivated by precrime ambitions: to assess threat risk and to preempt crime and terrorism.[57] For example, machine learning, a subset of artificial intelligence, is currently being used "to [develop] an array of classifiers."[58] Classifiers "represent a certain persona, with a unique personality type, a collection of personality traits or behaviors. [These] algorithms can score an individual according to their fit to these classifiers."[59] An example of a classifier is simply, "terrorist."[60] Beyond machine learning AI, there is also "multi-modal" emotion AI.[61] Multi-modal emotion AI aggregates both facial recognition technology and speech analysis to collect expressions of human emotion.[62]

C. *Clearview AI and the NYPD*

Clearview AI provides one example of the type of surveillance capacities that are available to law enforcement, such as the NYPD. Specifically, Clearview AI is an integration of AI into facial recognition technology. The failure of the facial recognition systems to capture Luigi Mangione demonstrates the limitations of the technological capacities of AI surveillance. Clearview AI, a controversial facial recognition tool that the NYPD had adopted on a trial basis in the past,[63] most likely[64] was deployed in identifying the suspect in Thompson's murder. The FBI confirmed that it had cooperated with the NYPD in the database screening to identify the suspect through analysis of the digital images collected from the scene of the crime and the suspect's whereabouts in NYC.[65]

Clearview AI matches faces in photographs by scanning an enormous database of images.[66] This database was amassed using "screen scraping" technology. This process involves automated systems, often referred to as "spiders" or "crawlers," to collect photographs from across millions of websites, including social media platforms. Clearview's core service allows users, primarily law enforcement, to upload a photo and instantly identify individuals

[57] *See, e.g.*, Hu, *Blacklisting*, *supra* note 11, at 1758–59.

[58] *Our Technology*, FACEPTION, https://www.faception.com/our-technology [https://perma.cc/FN6R-9LKT].

[59] *Id.*

[60] *Id.*

[61] *The Science Behind Emotion AI: How it Works*, AFFECTIVA, https://www.affectiva.com/science-overview/ [https://perma.cc/7MJS-KWEB].

[62] *Id.*

[63] Tate Ryan-Mosley, *The NYPD Used a Controversial Facial Recognition Tool. Here's What You Need to Know.*, MIT TECH. REV. (Apr. 9, 2021), https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails/ [https://perma.cc/6T24-C6VY].

[64] Kimery, *supra* note 42.

[65] *Id.*

[66] *See* State v. Clearview AI, Inc., No. 226-3-20 Cncv, 2023 WL 7548710, at *1 (Vt. Super. Ct. Oct. 26, 2023).

by matching the image to the vast database.[67] While Clearview AI had claimed its app is "not available to the public" and that it exists solely to aid law enforcement with "strict guidelines and safeguards," this statement was contradicted by reports that Clearview AI allegedly provided access to its app to for-profit companies like Best Buy, Macy's, and several telecommunications giants, as well as governments and businesses in up to twenty-seven countries, including the United Arab Emirates and Saudi Arabia.[68] This has raised concerns about the broad, unregulated use of the technology.[69]

Clearview AI's vast database, which includes images scraped from social media sites like Facebook, Instagram, and others, likely provided the NYPD with a powerful tool for running facial recognition on the images captured by security cameras.[70] Clearview AI's database, which boasts over fifty billion images scraped from the web without consent, includes photos from social media, allowing police to match faces from surveillance footage to a vast online database.[71]

Although the NYPD had previously downplayed its use of Clearview AI, internal emails released through Freedom of Information Act requests have revealed a much deeper involvement. These emails show that the NYPD had been using Clearview AI for years, including running thousands of searches during live investigations.[72] According to the documents, the department made extensive use of the system, with officers outside the facial recognition unit using it freely, even on their personal devices, circumventing policies meant to regulate its use.[73] The NYPD ran over 5,100 searches with Clearview AI, and many officers reported positive results, claiming that the tool had helped in making arrests.[74] These revelations contradict the NYPD's public stance that its use of Clearview AI was limited to trial periods and did not constitute an ongoing relationship with the company.[75]

[67] *Id.*

[68] *Clearview Is Not a Consumer Application*, CLEARVIEW AI (Jan. 23, 2020), https://web.archive.org/web/20200228035358/https://blog.clearview.ai/post/2020-01-23-clearview-is-not-public/ [https://perma.cc/36B5-8Z4C]; Complaint at 8–9, *Clearview AI, Inc.*, 2023 WL 7548710 (No. 226-3-20 Cncv) [hereinafter Complaint, *State v. Clearview AI*].

[69] *See id.*

[70] Creede Newton, *Hard Right-Linked Clearview AI Asked NYPD to Woo Non-Profit*, S. POVERTY L. CTR. (Feb. 22, 2022), https://www.splcenter.org/hatewatch/2022/02/22/hard-right-linked-clearview-ai-asked-nypd-woo-non-profit [https://perma.cc/5X7X-5A7X].

[71] *Id.*

[72] Caroline Haskins, Ryan Mac, Logan McDonald & Brianna Sacks, *Surveillance Nation*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [https://perma.cc/9YQD-85F9] (last updated Apr. 9, 2021, 7:52 PM).

[73] *Id.*

[74] *Id.*

[75] *Id.*

Because the NYPD publicly denies that it uses Clearview AI, presumably, Clearview AI was not directly used by the NYPD in the investigation of Thompson's murder.[76] Clearview AI access, however, could have been obtained by the NYPD through law enforcement partnerships.[77] The NYPD sought assistance from the FBI and other law enforcement agencies throughout the United States in the Thompson murder investigation. The FBI's facial recognition tools are part of a broader network, which includes access to databases containing millions of images, such as mugshots and other photos.[78] Although the FBI's database is not as extensive as Clearview AI's, with 640 million images compared to Clearview's fifty billion, it provides a critical resource for matching faces in investigations. In this case, the NYPD could have turned to the FBI to run the suspect's images through FBI's databases, in an attempt to identify Thompson's gunman.

Both the FBI and the NYPD have an established history with Clearview AI. Given that approximately 3,000 law enforcement agencies currently use Clearview AI and the FBI was involved in the investigation, it is likely that Clearview AI was used in the Thompson murder investigation.[79] In other words, because the FBI has a longstanding relationship with Clearview AI and is known to have contracted with Clearview AI, the NYPD likely accessed Clearview AI's technology and database via the FBI.[80]

Databases to identify suspects have limitations. "[I]t isn't known whether any of the numerous photos of Mangione found on social media and other online public sources after he was identified are included in [Clearview AI's] database[.]"[81] "[C]ontrary to popular belief, facial recognition software doesn't always link a suspect's face and identity . . . . 'Most Americans may believe that law enforcement has images on everybody in the United States. That's very much not true.'"[82] The types of databases that would have been used to screen the suspect's digital images would have included, for example, the New York Department of Motor Vehicles' biometric database; the FBI's Next Generation Identification database; the DHS's Automated Biometric Identification System; and the Department of Defense's Defense Biometric Identification System.[83]

[76] *Id.*; *see also* Chang & Chakrabarti, *supra* note 4.

[77] Haskins et al., *supra* note 72.

[78] Khari Johnson, *FBI Agents Are Using Face Recognition Without Proper Training*, WIRED (Sept. 25, 2023, 5:07 PM), https://www.wired.com/story/fbi-agents-face-recognition-without-proper-training/ [https://perma.cc/P665-PLZ6].

[79] *See* Kimery, *supra* note 42; Chang & Chakrabarti, *supra* note 4.

[80] Kimery, *supra* note 42; Chang & Chakrabarti, *supra* note 4.

[81] Kimery, *supra* note 42.

[82] Yan, *CEO Killer*, *supra* note 6.

[83] *Id.*

If a suspect had not been previously arrested or documented in government databases, the system may not have a record to engage a facial recognition match in any given facial recognition AI system. As one expert explains:

> If [a suspect] happens to not be a resident of New York [or] happens to not have been arrested before, odds are he's not going to be in their criminal database or their mugshot repository . . . . Some believe police can just cross-check a suspect's face with driver's license photos from the Department of Motor Vehicles . . . . [But] [t]he state of New York does not have access to the DMV database for law enforcement purposes by statute . . . . It requires cooperation and information sharing and a reason and willingness by the respective agencies to be allowed to share that by law.[84]

Further, most facial recognition systems require not a side view or partial view, but a "full face" that represents "image quality good enough to be able to match with the database or the library. . . . And if [a suspect] hasn't been arrested in New York, and he hasn't been on parole, it's not going to have that photo, so they're not going to get a match."[85] Clearview AI's expansive database of images from social media, where individuals post pictures freely, may have been relied upon by criminal investigators to fill the gap.[86] "[E]ven if the NYPD had had a clear facial image of the suspect, it would only have been useful if the suspect's face was in its criminal database."[87]

One of the purported benefits of Clearview AI is that it deploys AI models, referred to as convolutional neural networks ("CNNs"), to identify individuals even where digital images of the face may be partially obscured.[88] The AI "models are designed to focus on specific facial features that remain visible, such as the eyes, eyebrows, and forehead. They can also use contextual clues and patterns from datasets trained on partially masked faces."[89] Clearview AI, Amazon Rekognition, and other facial recognition systems are widely used by law enforcement.[90] Even if Clearview AI was used in the investigation, "it isn't known whether any of the numerous photos of Mangione found on social media and other online public sources after he was identified are included in [Clearview AI's] database, or whether its CNN would have been able to identify

[84] *Id.* (providing quotes from Donnie Scott, CEO of IDEAMIA Group, a facial recognition technology company).

[85] Chang & Chakrabarti, *supra* note 4.

[86] *See* Haskins et al., *supra* note 72.

[87] Kimery, *supra* note 42.

[88] *Id.*

[89] *Id.*

[90] *Id.*

him as a possible match."[91] AI can also facilitate facial recognition technology through the utilization of generative adversarial networks ("GANs").[92] GANs can infer portions of a face that may be absent from the digital image by reconstructing and analyzing facial representations.[93]

The NYPD investigation of Thompson's murder, which included access to both public and private cameras, involved a review of hundreds, if not thousands, of captured images of the suspect wearing a mask and hood, but these images failed to identify the suspect. Facial recognition technology often faces challenges when identifying individuals from blurry or low-quality images, such as those captured on street-level cameras.[94] Furthermore, mask wearing can "hinder facial recognition software because it recognizes points in the face and measures the distance between them" and is "less effective on footage shot on a street in low light or bad weather."[95] The technology's biases, especially its higher error rates when identifying people of color, have led to accusations of racial discrimination in its use.[96]

This case study highlights the complexities and limitations of facial recognition AI surveillance technology. While NYC's cameras and facial recognition tools may have been deployed together with other facial recognition AI systems, the technology's effectiveness was not immediate, and human intervention was still required. The suspect was not identified by technology alone, but by a customer and McDonald's employee in Altoona, Pennsylvania, who recognized the suspect from the images circulating in the media. The employee alerted authorities, leading to Mangione's arrest five days after the murder.[97] While the NYPD's camera network and facial recognition technology helped track the suspect's movements, it was the public's vigilant eye that ultimately led to the suspect's identification and arrest.[98]

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] Chang & Chakrabarti, *supra* note 4.

[95] Megan Palin, *How NYPD Is Using AI, Drones, DNA and Cutting-Edge Tech in the Manhunt for United Healthcare CEO Brian Thompson's Assassin*, N.Y. POST (Dec. 6, 2024, 4:40 PM), https://nypost.com/2024/12/06/us-news/the-next-frontier-for-catching-a-killer-prevalent-surveillance-ai-drones [https://perma.cc/AU5J-U2YL].

[96] Thaddeus L. Johnson & Natasha N. Johnson, *Police Facial Recognition Technology Can't Tell Black People Apart*, SCI. AM. (May 18, 2023), https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/ [https://perma.cc/XH5W-GAYL]; Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022, 7:00 AM), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ [https://perma.cc/9YEU-6XNZ (staff-uploaded, dark archive)]; *see also Surveillance City*, *supra* note 6.

[97] Ray Sanchez & John Miller, *How Suspect on the Run in CEO's Killing Was Recognized at a Pennsylvania McDonald's, Hash Brown in Hand, and Finally Captured*, CNN, https://www.cnn.com/2024/12/11/us/luigi-mangione-unitedhealthcare-arrest-explained/index.html [https://perma.cc/3AHE-FELB] (last updated Dec. 11, 2024, 9:34 AM; Helsel et al., *supra* note 28.

[98] *See* Sanchez & Miller, *supra* note 97; Helsel et al., *supra* note 28.

II. RISKS AND RESPONSES TO FACIAL RECOGNITION AI

Clearview AI's technology has sparked significant legal issues, particularly around privacy and the misuse of biometric data. The core of the controversy lies in Clearview's method of gathering images. The company scrapes publicly available photographs from social media platforms, like Facebook, Instagram, and Twitter (now X), without consent from the users or the platforms themselves.[99] These images are then processed and used for facial recognition matching, which violates the terms of service of most social media platforms, such as Facebook's prohibition against screen scraping.[100] This practice has led to significant legal challenges, with companies like Google, Facebook, and Twitter (now X) sending cease-and-desist letters.[101]

Clearview AI has been legally challenged because many of the images collected were not intentionally made public by the individuals pictured. For instance, people might unknowingly have their private photos posted online due to website coding errors, or photographs taken at private events could end up in the database.[102] Moreover, images that were originally meant for private

[99] Will Knight, *Clearview AI Has New Tools to Identify You in Photos*, WIRED (Oct. 4, 2021, 7:00 AM), https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/ [https://perma.cc/B9GL-59UB (dark archive)]; Miriam Kohn, Comment, *Clearview AI, TikTok, and the Collection of Facial Imagines in International Law*, 23 CHI. J. INT'L L. 195, 199–200 (2022).

[100] *See* Terence Liu, *How We Store and Search 30 Billion Faces*, CLEARVIEW AI: BLOG (Apr. 18, 2023), https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces [https://perma.cc/9NB7-6ZZW] (describing the "complex process" of "identifying an individual or verifying their identity" through Clearview AI's facial recognition algorithm); Kohn, *supra* note 99, at 199 ("[Clearview AI] collects these images despite sources' policies prohibiting 'photo scrapping.'"); *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms/previous [https://perma.cc/E63G-SK2N (staff-uploaded archive)] (last updated Jan. 30, 2015) ("You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.").

[101] *See Google, YouTube, Venmo, and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App That Helps Law Enforcement*, CBS NEWS, https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/ [https://perma.cc/2FGD-PCX8] (last updated Feb. 5, 2020, 6:52 PM); Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html [https://perma.cc/WEF6-Y266 (staff-uploaded, dark archive)].

[102] *See* Katherine Tangalakis-Lippert, *Clearview AI Scraped 30 Billion Images from Facebook and Other Social Media Sites and Gave Them to Cops: It Puts Everyone into 'Perpetual Police Line-Up*,*'* BUS. INSIDER (Apr. 2, 2023, 10:18 PM), https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4 [https://perma.cc/CY87-44P4 (staff-uploaded, dark archive)] ("[I]f you are in the background of a wedding photo, or a friend of yours posts a picture of you together at high school, once Clearview has snapped a picture of your face, it will create a permanent biometric print of your face to be included in the database."); Complaint, *State v. Clearview AI*, *supra* note 68, at 14–15 (asserting that "[i]t is not uncommon for website coding errors to make photographs available to the public accidentally . . . for Clearview's spiders to capture them" and describing how "one website (Classsmates.com) has scanned hundreds of thousands of school yearbooks dating back over a century and has posted those photographs online," which makes them available to Clearview).

use, such as those from yearbooks or social events, have been included in the database without the knowledge or consent of the individuals involved.[103]

One of the main concerns is its "intrusion upon privacy," as the company uses screen scraping technology to amass a database of "three billion photographs" from millions of websites without consent from the individuals pictured.[104] The use of "screen scraping" involves sending "automated scripts or other processes, sometimes called 'spiders,'" to collect photographs from the web, which raises concerns about the violation of "property rights" and the "reasonable expectations of the photographer and the individual in the image."[105] The company scrapes "images of people's faces from across the internet, such as employment sites, news sites, educational sites, and social networks including Facebook, YouTube, Twitter, Instagram and even Venmo."[106]

Clearview AI collects these photos "for a clearly commercial, for-profit use" by creating a service that allows customers to upload photos to "instantly identify the individual through facial recognition matching."[107] This practice is controversial because "when an individual uploads a photograph to Facebook for 'public' viewing, they consent to a human being looking at the photograph on *Facebook*" but not to its mass collection for a facial recognition database.[108] Furthermore, Clearview AI's claim that it only collected "publicly available" photographs has been contested, as "public availability" does not necessarily imply permission for mass collection or commercial use.[109] Indeed, many images "were not acceded to by the individual pictured" and were obtained without consent, raising serious privacy concerns.[110]

Moreover, Clearview AI makes its app available to numerous businesses and governments, violating privacy expectations. The company provided access to its app to "for-profit corporations including Best Buy, Macy's, Kohl's, Walmart, Albertsons, Rite Aid, AT&T, Verizon, T-Mobile, Wells Fargo, Bank of America, the Las Vegas Sands Casino, Madison Square Garden, the NBA, Equinox Fitness, and more than fifty universities, among others."[111] This broad access was not limited to law enforcement agencies, and even within law enforcement, "Clearview had granted access to additional individuals through 'an email regarding an invitation, user referral or free trial from the

[103] Tangalakis-Lippert, *supra* note 102; Complaint, *State v. Clearview AI*, *supra* note 68, at 14–15.

[104] Complaint, *State v. Clearview AI*, *supra* note 68, at 7.

[105] *Id.* at 11.

[106] Hill, *Secretive Company*, *supra* note 44.

[107] Complaint, *State v. Clearview AI*, *supra* note 68, at 7, 14.

[108] *Id.* at 12.

[109] *Id.*

[110] *Id.* at 14.

[111] *Id.* at 8.

company.'"[112] Despite Clearview's claims, its app was made available to a range of unauthorized users.[113]

A. *Clearview AI Litigation*

Several legal battles surrounding Clearview AI focus on alleged violations of state law. For example, in *ACLU v. Clearview AI*,[114] the complaint alleges that the company violated the Illinois Biometric Information Privacy Act ("BIPA"),[115] which mandates "written release" from individuals before their biometric data is collected.[116] In *State of Vermont v. Clearview AI, Inc.*,[117] Vermont alleges the company's web scraping "resulted in the collection of billions of photographs, without the permission of their owners, for a clearly commercial for-profit use."[118] In the legal proceedings, Clearview AI filed a motion to dismiss, arguing that the photographs it collected were public and, therefore, did not violate privacy expectations.[119] However, the court denied the motion, emphasizing that the standard for surviving dismissal is that the state must sufficiently allege that the company's conduct "'imposes a lack of meaningful choice'" or "'involves a lack of consent[,]'" and "Clearview's alleged collection of and application of facial recognition technology to Vermonters' photographs without their consent plainly falls within this standard."[120] The Vermont Superior Court reasoned that it was up to a jury to decide how to resolve the allegation of unfairness to the consumer that could result from the mass data collection of digital photos of Vermont citizens by the company for its facial recognition database and facial recognition AI system. "While it remains to be seen whether the State can prove unfairness at trial, the allegations in the

[112] *Id.* at 9 (quoting Joedy McCreary, *Raleigh Police: Face ID Company Offered Free Trials to Unauthorized Employees*, CBS 17, https://www.cbs17.com/news/digital-investigations/raleigh-police-face-id-company-offered-free-trials-to-unauthorized-employees/ [https://perma.cc/2UBW-KUU7 (staff-uploaded archive)] (last updated Feb. 25, 2020, 6:48 PM)).

[113] *See id.*

[114] 2021 Ill. Cir. LEXIS 292 (2021).

[115] Biometric Information Privacy Act of 2008, Pub. Act 95-0994, 740 Ill. Comp. Stat. 14/1 (2008).

[116] *Id.* at 14/15(b)(3). The statute defines "written release" as "informed written consent, electronic signature, or, in the context of employment, a release executed by an employee as a condition of employment." *Id.* 14/10; Complaint at 3, 27, 32, *ACLU v. Clearview AI*, No. 2020-CH-04353 (Ill. Cir. Ct. May 11, 2022) [hereinafter Complaint, *ACLU v. Clearview*]. For a summary of litigation against Clearview AI under this act, see *ACLU v. Clearview AI*, ACLU, https://www.aclu.org/cases/aclu-v-clearview-ai [https://perma.cc/BZ5M-937L] (last updated May 11, 2022).

[117] No. 226-3-20 Cncv, 2023 WL 7548710, at *1 (Vt. Super. Ct. Oct. 26, 2023).

[118] Complaint, *State v. Clearview AI*, *supra* note 68, at 14.

[119] Ruling on Defendant's Motion to Dismiss at 16, *Clearview AI, Inc.*, No. 226-3-20 Cncv (Vt. Super. Ct. Sept. 10, 2020) ("Clearview also advances slightly different First Amendment theory—that this action violates its right to access public data on the web." (citation omitted)).

[120] *Id.* at 24 (citations omitted).

complaint are sufficient to survive motion to dismiss."[121] Vermont had argued in the complaint that when a Vermont citizen publicly posts photos on Facebook, "[t]hey are not consenting to the mass collection of those photographs by an automated process that will then put those photographs in to a facial recognition database. Such a use violates the terms under which the consumer uploaded the photograph, which the consumer reasonably expects will be enforced."[122]

Vermont later filed a motion for partial summary judgment, which was denied, in part because the Vermont Superior Court concluded that it was a matter for the jury to decide whether the facial recognition AI system used by law enforcement in Vermont was reasonable. "The court cannot say that any reasonable Vermonter would find that the privacy violations ensuing from Clearview's product outweigh the benefits," and "[f]ew Vermonters would argue that [Clearview AI] uses by law enforcement are not beneficial to society."[123] Clearview AI had asserted to the court "that its product has been used by law enforcement to identify child abusers, January 6 rioters at the Capitol, assisting Ukrainians in their fight with Russia, and exonerating an innocent person."[124]

Further, in *American Civil Liberties Union v. Clearview AI*, *Inc*., the ACLU filed a complaint against the facial recognition AI company, alleging violations of the BIPA.[125] The plaintiffs focused explicitly on the harm caused by facial recognition AI on communities of color and other *vulnerable* communities, including survivors of domestic violence and sexual assault, undocumented immigrants, and other targeted communities, and sought multiple remedies, including deletion of all faceprints gathered without consent from Illinois residents.[126]

In 2022, plaintiff and Clearview AI reached a settlement agreement, which included a permanent injunction prohibiting Clearview AI from releasing its faceprint database to most businesses and private entities nationwide and also barred it from selling access to entities within Illinois for five years.[127]

[121] *Id.*

[122] Complaint, *State v. Clearview AI*, *supra* note 68, at 12.

[123] Ruling on Motion for Partial Summary Judgement at 7, 8, *Clearwater AI, Inc.*, No. 226-3-20 Cncv (Vt. Super. Ct. Dec. 18, 2023).

[124] *Id.*

[125] Biometric Information Privacy Act of 2008, Pub. Act 95-0994, 2008 ILL. L. 3693 (codified as amended at 70 ILL. COMP. STAT. 14/1 to 14/99); Complaint, *ACLU v. Clearview*, *supra* note 115, at 27, 32.

[126] Complaint, *ACLU v. Clearview*, *supra* note 115, at 5–7, 11, 32.

[127] Settlement Agreement & Release at 1, 2, Am. C.L. Union v. Clearview AI, 2020 CH 04353 (Cir. Ct. Cook Cnty, Ill.); *see also* Isra Ahmed, Case Brief, ACLU v. Clearview AI, Inc., *2021 Ill. Cir. LEXIS 292*, 33 DEPAUL J. ART, TECH. & INTELL. PROP. L. 66, 66 (2023).

Concurrently with the *American Civil Liberties Union v. Clearview AI, Inc.* litigation that was proceeding in state court in Illinois, a class action lawsuit that represented the consolidation of federal multidistrict litigation was proceeding in a federal district court in Illinois.[128] In 2025, the resolution to the class action lawsuit was announced, and it was considered especially novel given that, instead of establishing a fund for the settlement, the consumers who were potentially harmed may be able to exercise a stake in Clearview AI, holding up to twenty-three percent in the tech startup.[129] The court estimated that the settlement stake could be valued at approximately $51.75 million, based on January 2024 valuation estimates.[130] The settlement explained that the monetary relief would be triggered by the occurrence of several events, including an initial public offering or "liquidation event, such as a merger or consolidation or sale of all or substantially all of Clearview's assets."[131]

The litigation developments surrounding Clearview AI demonstrate how contested facial recognition AI technologies are, including competing theories on how best to regulate these technologies. The *State of Vermont v. Clearview AI, Inc.* case relied on a combination of consumer protection and consumer privacy theories.[132] However, in reviewing the motion for partial summary judgment filed by Vermont, the Superior Court of Vermont denied the motion in part because it found persuasive Clearview AI's arguments that facial recognition AI could be considered reasonable and beneficial for law enforcement purposes.[133] The court concluded: "The world of technology is changing too quickly, and with it the norms of society are changing. The determination of what is 'unfair' in this realm, and how to weigh the risks and benefits of technology such as Clearview's, is one that requires a jury."[134]

Similarly, the settlement agreements in both *American Civil Liberties Union v. Clearview AI, Inc.* in Illinois and the class action lawsuit *In re Clearview AI, Inc., Consumer Privacy Litigation* show that the litigation theories are still

[128] *See* Mike Scarcella, *US Judge Approves 'Novel' Clearview AI Class Action Settlement*, REUTERS, https://www.reuters.com/legal/litigation/us-judge-approves-novel-clearview-ai-class-action-settlement-2025-03-21/ [https://perma.cc/Y6DG-MZAE (staff-uploaded, dark archive)] (last updated Mar. 21, 2025, 2:40 PM); *In re* Clearview AI, Inc., Consumer Privacy Litigation, No. 21-cv-00135, 2025 WL 875162, at *1 (N.D. Ill. Mar. 20, 2025).

[129] Scarcella, *supra* note 128; *In re Clearview AI, Inc.*, 2025 WL 875162, at *9 ("After over six months of negotiations, the parties landed on a settlement agreement providing the Settlement Class with payout from a 23% equity stake in Clearview.") (citation omitted)).

[130] *In re Clearview AI, Inc.*, 2025 WL 875162, at *11.

[131] *Id.*

[132] Complaint, *State v. Clearview AI*, *supra* note 68, at 23–26 (alleging violations of: "Unfair Acts and Practices in Violation of 9 V.S.A. § 2453," "Deceptive Acts and Practices in Violation of 9 V.S.A. § 2453," and "Acquisition and Uses of Brokered Personal Information in Violation of 9 V.S.A. § 2431").

[133] Ruling on Motion for Partial Summary Judgment, *supra* note 123, at 4, 7, 10.

[134] *Id.* at 8.

evolving on how to properly assert oversight over facial recognition AI.[135] Both lawsuits asserted violations of BIPA, the Illinois law that specifically provides data privacy protections for biometric information.[136] The class action lawsuit further alleged violations of various consumer protection and data privacy laws in the jurisdictions of California, Virginia, and New York.[137]

All of the litigation matters involving Clearview AI thus far illustrate the complexity of balancing individual privacy rights with the potential law enforcement benefits that have been asserted but, in the earliest stages of this nascent technology, have not been definitively proven. The battleground for challenging facial recognition AI is currently on consumer protection grounds. Thus, the issues are framed as statutory in nature. Understanding the constitutionality of facial recognition AI will likely demand an interstitial approach that combines statutory and constitutional arguments, as well as a comparative approach that assesses international regulatory regimes that are intended to preempt AI harm and recognizes the need to protect fundamental rights.

B. *Legislative Response*

Presently, when this biometric data is gathered, and then collected in facial recognition AI systems, many public and private actors generally see the data gathering as benign.[138] However, in the age of AI, where database screening, and predictive analysis are rapidly becoming the new norm, biometric data is increasingly used to advance public and private cybersurveillance programs.[139] Thus, these biometric data systems are not benign, but are pervasively transforming the nature of cybersurveillance from simple identity verification to automatic and pervasive monitoring of individuals and their behaviors.[140]

[135] *See In re Clearview AI, Inc.*, 2025 WL 875162, at *9–14.

[136] *Id.* at *3–4; Complaint, *State v. Clearview AI*, *supra* note 68, at 2–3.

[137] *In re Clearview AI, Inc.*, 2025 WL 875162, at *4 (alleging violations of: "(1) BIPA, 740 ILCS § 14/15(b) (c) (d) and (e); (2) Viginia statutes addressing the unauthorized use of names or pictures, Va. CODE §§ 8.01-40, and the Virginia Computer Crimes Act, Va. CODE § 18.2-152.1, *et seq*.; (3) California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq*., California's Commercial Misappropriation statute, Cal. Civ. Code § 3344(A), California common law protections for the right of publicity, and the California state constitution's protections against invasion of privacy; and (4) New York's civil rights protections against invasion of privacy, N.Y. CIV. RIGHTS LAW §§ 50–51; and (5) brought an unjust enrichment claim and sought judgment under the federal Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*.") (citation omitted)).

[138] *See, e.g.*, Hu, *Biometric ID*, *supra* note 1, at 1481, 1529.

[139] *See id.* at 1500, 1521.

[140] *See, e.g.*, Hu, *Blacklisting*, *supra* note 11, at 1756; Biometric Information Privacy Act of 2008, Pub. Act 95-0994, 740 Ill. Comp. Stat. 14/1 (2008). BIPA includes a written release requirement for consent by a data subject to authorize an entity's ability to "capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information." *Id.* at 14/15(b).

Racial justice protests in recent years further demonstrate that technological advances in biometric and facial recognition software are expanding significantly. It was revealed shortly after the 2014 riots in Ferguson, Missouri, and the 2015 Baltimore riots following the deaths of Michael Brown and Freddie Gray, that the local law enforcement deployed facial recognition technology to identify individuals in the crowds of protesters.[141] Through a contractor, local police used Facebook, Twitter (now X), and Instagram feeds to track and arrest several minority protesters who were wanted by law enforcement.[142] Similarly, in May 2020, following the death of George Floyd, it was "reported that the Minneapolis Police had contracted with Clearview [AI] to employ the use of facial recognition technology" during the riots in Minneapolis.[143] Further, "various city police departments and the Federal Bureau of Investigation . . . openly requested that the public share images and videos of protesters . . . with the intention of applying facial recognition algorithms for comparison to footage from body-worn cameras, as well as image identification in various databases."[144] Following the January 6, 2021, riots at the U.S. Capitol, federal officials used facial recognition technology to identify and then prosecute rioters.[145] Clearview AI specifically was relied upon by law enforcement to apprehend the perpetrators of the Capitol attack.[146]

Recognizing the unique challenges to data privacy rights posed by biometric identification data collection and use, multiple states, including Illinois, Texas, and Washington, have introduced or passed laws restricting

[141] *See* Craig Timberg & Elizabeth Dwoskin, *Facebook, Twitter and Instagram Sent Feeds That Helped Police Track Minorities in Ferguson and Baltimore, Report Says*, WASH. POST (Oct. 11, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/11/facebook-twitter-and-instagram-sent-feeds-that-helped-police-track-minorities-in-ferguson-and-baltimore-aclu-says/ [https://perma.cc/QPK2-HPJ2 (staff-uploaded, dark archive)]; *see also* Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/ [https://perma.cc/CX2H-Q6W6] (explaining how the Baltimore Police Department "used geo-based social media tracking and facial recognition technology on protesters following the death of Freddie Gray"); Nathan Freed Wessler & Naomi Dwork, *FBI Releases Secret Spy Plane Footage from Freddie Gray Protests*, ACLU (Aug. 4, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-releases-secret-spy-plane-footage-freddie-gray [https://perma.cc/38S6-CAH7].

[142] *See* Timberg & Dwoskin, *supra* note 141.

[143] Matthew E. Cavanaugh, Note, *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 MINN. L. REV. 2443, 2454 (2021).

[144] Ringrose & Ramjee, *supra* note 50, at 359.

[145] Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ [https://perma.cc/YM3X-FJ2N (staff-uploaded, dark archive)].

[146] Kashmir Hill, *The Facial-Recognition App Clearview Sees a Spike in Use After Capitol Attack*, N.Y. TIMES, https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html [https://perma.cc/WNB8-5LAV (staff-uploaded, dark archive)] (last updated Jan. 31, 2021).

biometric data use and protecting biometric privacy.[147] A proposed House Joint Resolution of the Virginia Assembly called for a report on "the proliferation and implementation of facial recognition and artificial technology within [Virginia]."[148] Although it has not yet passed,[149] the resolution recognizes that "facial recognition implicates constitutional concerns related to unreasonable searches and seizures [under the Fourth Amendment] as well as individual privacy."[150]

In April 2025, a state bill that required human oversight over AI technologies that impacted criminal procedure, H.B. 1642, was passed by the House and Senate in the Virginia Assembly.[151] According to a study by the National Institute of Standards and Technology, Black and Asian faces are 10 to 100 times more likely to be misidentified as false positives by AI facial recognition technologies than white faces.[152] Consequently, some states have enacted a "prohibition against reliance on facial recognition matches as the 'sole basis' for an arrest."[153] Several states have adopted bans against facial recognition technology use as the "sole basis" for an arrest: Alabama, Colorado, Maine, Virginia, and Washington.[154]

[147] *See* Biometric Information Privacy Act of 2008, Pub. Act 95-0994, 740 Ill. Comp. Stat. 14/1 (2008); TEX. BUS. & COM. CODE § 503.001 (regulating "Capture or Use of Biometric Identifier"); WASH. REV. CODE § 19.375.020 (2017) (regulating "[e]nrollment, disclosure, and retention of biometric identifiers"); *see also, e.g.*, JAMES A LEWIS & WILLIAM CRUMPLER, CTR. STRATEGIC & INT'L STUDS., FACIAL RECOGNITION TECHNOLOGY: RESPONSIBLE USE PRINCIPLES AND THE LEGISLATIVE LANDSCAPE 5–6, 11, 19 (2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf [https://perma.cc/2YEH-V2ZM]; *Is Biometric Information Protected by Privacy Laws*, BLOOMBERG L. (June 20, 2024), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/ [https://perma.cc/U5ZF-Z7F8]. Other state laws such as the California Consumer Privacy Act of 2018 (codified as amended at CAL. CIV. CODE § 1798.100 (2023)) and the California Privacy Rights Act of 2020, A.B. 1490 (2021) (codified as amended at CAL. CIV. CODE § 1798.100 (2023)) are not solely biometric privacy laws, but they also encompass biometric data protections.

[148] H.R.J. Res. 59, 2020 Gen. Assemb., Reg. Sess. (Va. 2020).

[149] *Legislation Related to Artificial Intelligence*, NAT'L CONF. STATE LEGISLATURES, https://www.ncsl.org/technology-and-communication/legislation-related-to-artificial-intelligence [https://perma.cc/V4JD-TJRK (staff-uploaded archive)] (last updated Jan. 31, 2023).

[150] H.R.J. Res. 59, 2020 Gen. Assemb., Reg. Sess. (Va. 2020).

[151] H.B. 1642, 2025 Gen. Assemb., Reg. Sess. (Va. 2025).

[152] PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. STANDARDS & TECH., U.S. DEP'T OF COM., FACE RECOGNITION VENDOR TEST (FRVT), PART 3: DEMOGRAPHIC EFFECTS 2 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf [https://perma.cc/JV93-W5RS].

[153] Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, TECH POL'Y PRESS (Jan. 6, 2025), https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ [https://perma.cc/9XJ2-PFZC] [hereinafter Laperruque, *Status of State Laws*].

[154] Jake Laperruque, *Limiting Face Recognition Surveillance: Progress and Paths Forward*, CTR. DEMOCRACY & TECH. (Aug. 23, 2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/ [https://perma.cc/GW7A-JR7J].

III. CONSTITUTIONAL IMPACT OF FACIAL RECOGNITION AI

Governmental reliance on facial recognition technology poses unique challenges to constitutional rights in the United States and to fundamental rights in the European Union (EU). Criminal procedure protections under the Bill of Rights have been particularly challenged. Facial recognition AI especially places stress tests on protections against warrantless unreasonable searches and seizures under the Fourth Amendment, protections against due process violations and self-incrimination under the Fifth Amendment, and protections to confront witnesses under the Sixth Amendment.[155] The EU AI Act presents a comparative perspective that can be useful in understanding regulatory options for placing guardrails around facial recognition AI systems.[156]

A. *Warrantless Searches and Seizures*

Facial recognition technologies present a slew of unique legal challenges. For one, the blending of private and public databases for law enforcement and national security purposes presents issues of ownership, access, and control. As information is shared across government agencies, it becomes more difficult to discover abuses of privacy and other individual rights. Further, exploiting publicly presented data, such as scanning someone's face on the street, and web-based images, like capturing someone's face on social media sites, presents challenges to personal privacy and autonomy. This poses challenges to our current privacy laws, which are ill suited to regulate privacy violations resulting from algorithm-based social media platforms.

Facial recognition AI concerns encompass the collection, use, and storage of biometric data, such as digital images of faces captured through both public and private cameras and live-feed videos. As seen from the case study of the investigation surrounding the murder of CEO Brian Thompson and the eventual capture of suspect Luigi Mangione, public view of one's face or image can be captured in a digital image and then processed by facial recognition technology such as Clearview AI. Companies such as Clearview AI can argue that this falls outside the protections of the Fourth Amendment, contending that the public presentment of one's face and capture of public images falls

[155] U.S. CONST. amends. IV, VI; *see also* Margaret Hu, *Biometrics and an AI Bill of Rights*, 60 DUQUESNE L. REV. 283, 285 (2022) [hereinafter Hu, *Biometrics and AI*] (first citing Ferguson, *supra* note 1, at 1126; then citing Eldar Haber, *Racial Recognition*, 43 CARDOZO L. REV. 71, 101 n.165 (2021) (citing State v. Loomis, 881 N.W.2d 749 (Wis. 2016)); then citing Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, N.Y. TIMES (May 1, 2017), https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html [https://perma.cc/6P8X-9SA3 (staff-uploaded, dark archive)]; then citing Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1983 (2017); and then citing Joseph Clarke Celentino, Note, *Face-to-Face with Facial Recognition Evidence: Admissibility Under the Post-*Crawford *Confrontation Clause*, 114 MICH. L. REV. 1317, 1318 (2016)).

[156] *See infra* Section III.D.

outside the scope of the Fourth Amendment's proscription of warrantless searches and seizures. Asserting protections under the Fourth Amendment is especially challenging when the facial recognition images are digitally collected administratively in a broad surveillance effort and not in the service of a specific law enforcement investigation, falling outside of the warrant requirement of the Fourth Amendment.[157]

When law enforcement agencies outsource the cyber searches and data seizures to private companies such as Clearview AI, facial recognition AI can result in Fourth Amendment harms through the services of web scraping, mass digital image aggregation, and AI analytics. Further, investigatory analysis that stems from services provided by companies such as Clearview AI to law enforcement can lead to AI-driven surveillance tools that erode or infringe upon the Fourth Amendment's reasonable expectation of privacy protections, such as those asserting privacy to facial recognition technologies under the Fourth Amendment.[158]

Integrating AI tools with facial recognition technology in order to make predictive judgments based upon someone's digital image also presents significant challenges to personal privacy and autonomy. Such a system may result in a dystopian future in which a person could potentially be punished for the possibility of a future act as determined by an algorithm. "[I]n 2011, Google's chairman at the time said it was the one technology the company had held back because it could be used 'in a very bad way.'"[159] Moreover, several cities have banned police from using facial recognition technology.[160] Finally, new facial recognition software aggregates identifying data with real-time social media analysis and live-streaming video. This combination of technologies may have a multiplicative effect on privacy violations, which privacy laws are ill suited to handle. These are only some of the legal challenges that we will inevitably have to contend with as facial recognition technologies become more sophisticated and prevalent. It is imperative, therefore, to begin to examine these technologies closely.

AI and cybersurveillance often rely on information made public, such as social media posts, blogs, or other public expressions by individuals.[161] Law

[157] *See, e.g.*, Margaret Hu, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1824 (2017).

[158] *See generally* Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016) (analyzing the inadequacies of existing Fourth Amendment doctrine for handling novel technologies such as the Automated Suspicion Algorithms ("ASAs"), and proposing extrajudicial means to ensure that ASAs are accurate and effective).

[159] Hill, *Secretive Company*, *supra* note 44.

[160] *Id.*

[161] *See, e.g.*, *Social Radar Technologies*, MITRE, https://www.mitre.org/our-impact/intellectual-property/social-radar-technologies [https://perma.cc/957T-QD6T]; FAIZA PATEL, RACHEL LEVINSON-WALDMAN, SOPHIA DENUYL & RAYA KOREH, BRENNAN CTR. FOR JUST., SOCIAL

enforcement may view the use of facial recognition technology not as a search and seizure issue under the Fourth Amendment, but as a database search of images that are often publicly available. Doctrinally speaking, under the third party doctrine, individuals do not retain an expectation of privacy in information they voluntarily share with others.[162] But this approach is increasingly problematic in the digital age.[163] Data gathered for facial recognition tools and other urban surveillance technologies would not be considered private under the third-party doctrine because they have been shared with others.[164] But, as this Article demonstrates, these technologies are ubiquitous and inescapable—if information gathered this way is not private, what sense of privacy remains? It is imperative to locate individual privacy and liberty in the face of evolving facial recognition AI technologies.

The question posed by cybersurveillance technologies, such as facial recognition AI in urban surveillance infrastructures, is whether and to what extent suspicionless mass surveillance can ever be considered reasonable or consistent with constitutional values.[165] The Fourth Amendment is currently interpreted as restricting policing tactics that are unreasonable against a particular individual who has been harmed.[166] Courts use the two-part test developed in *Katz v. United States*,[167] which includes both a subjective and an objective inquiry, to determine if a policing tactic is in fact unreasonable.[168] The subjective portion of the test focuses on whether the government's actions

MEDIA MONITORING 3 (2019), https://www.brennancenter.org/media/212/download [https://perma.cc/ZTP4-L327]; Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 VA. L. REV. 1351, 1351, 1365 (2024).

[162] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301, 100 Stat. 1848, 1868 (codified as amended at 18 U.S.C. § 3121) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[163] *See* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring); *see also* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 985–86 (2016) (discussing the expansion of third party doctrine and constitutional implications of the expansion); Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After* Carpenter*?*, 26 B.U. J. SCI. & TECH. L. 286, 310–23 (2020).

[164] *See Smith*, 442 U.S. at 743–44.

[165] *See generally* U.S. CONST. amend. IV (prohibiting unreasonable searches and seizures). For a discussion of the possibility of using notice and comment practices in surveillance, see Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 137–40 (2016).

[166] *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 134 (1978), *abrogated in part by* Minnesota v. Carter, 525 U.S. 83 (1998) (explaining that Fourth Amendment rights are personal, and therefore "only defendants whose Fourth Amendment rights have been violated" may "benefit from [those] protections").

[167] 389 U.S. 347 (1967).

[168] *Id.* at 361 (Harlan, J., concurring), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 101–11, 100 Stat. 1848, 1848–58 (codified as amended at 18 U.S.C. §§ 2510–20), *as recognized in* United States v. Koyomejian, 946 F.2d 1450, 1455 (9th Cir. 1991).

violate an individual's expectation of privacy.[169] This is an inquiry into the individual circumstances of a specific encounter with the particular technology or conduct that was the source of the intrusion. The objective portion of the test considers whether the individual's expectation of privacy is one that society at large would consider reasonable.[170] This two-part analysis illustrates the current understanding of the Fourth Amendment as providing protections to the *individual*, and not to the community at large.

Yet modern surveillance practices do not appear to fall into traditional definitions of search and seizure. These practices focus on mass data collection, storage, and analysis, rather than tangible objects that may be confiscated and examined.[171] Modern surveillance is virtual, automated, and conducted remotely.[172] Further, data presents unique issues,[173] particularly because creating and collecting data is frequently mandated simply by being a part of the Information Society.[174] A population that is aware that their information, expressions, thoughts, and ideas are constantly being watched, collected, and shared is a population that is gradually surrendering an objective expectation of privacy.[175]

A push for a more open, digitally connected society also carries with it the potential for a society without privacy.[176] This change requires a fundamental

[169] *Id.* (explaining the first requirement is "that a person have exhibited an actual (subjective) expectation of privacy").

[170] *Id.* (explaining the second requirement is "that the expectation [of privacy] be one that society is prepared to recognize as 'reasonable'").

[171] *See, e.g.*, Margaret Hu, *Horizontal Cybersurveillance Through Sentiment Analysis*, 26 WM. & MARY BILL RTS. J. 361, 361 (2017) [hereinafter Hu, *Horizontal Cybersurveillance*]; Randy Barnett, *Why the NSA Data Seizures Are Unconstitutional*, 38 HARV. J.L. & PUB. POL'Y 3, 3–5 (2015).

[172] *See id.*; *see also* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 409 (2012).

[173] *In re* Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 200–01 (2d Cir. 2016); *see also* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 326 (2015); Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473, 473–75 (2016).

[174] United States v. Jones, 565 U.S. 400, 415–18 (2012) (Sotomayor, J., concurring) (explaining that the "digital age" requires disclosure of significant amounts of information for routine activities); *see also* Margaret Hu, *Biometric Surveillance and Big Data Governance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 121, 135 (David Gray & Stephen E. Henderson eds., 2017).

[175] *See Jones*, 565 U.S. at 427 (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

[176] *Id.* at 415–16 (Sotomayor, J., concurring); *see also* A WORLD WITHOUT PRIVACY: WHAT LAW CAN & SHOULD DO? 1 (Austin Sarat ed., 2015); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1310 (2012); Dave Lee, *Apple v FBI: US Debates a World Without Privacy*, BBC NEWS (Mar. 2, 2016), http://www.bbc.com/news/technology-35704103 [https://perma.cc/U389-G3Z3].

rethinking of the Fourth Amendment, lest it become virtually meaningless. As David Gray points out, the language of the Fourth Amendment protects the right of the *people* to be free from unreasonable surveillance and tracking.[177] The federal government has already argued against this conceptualization of the Fourth Amendment when the scope of its surveillance was challenged—the government maintained that the Fourth Amendment is not an antisurveillance amendment.[178] This constitutional matter presents an ongoing issue for the federal judiciary.

The Supreme Court has struggled with the impact of developing technology on the Fourth Amendment for decades, since before *Katz* was decided in 1967.[179] As technology continuously changes, the Court continuously struggles with how to fit these developments into existing Fourth Amendment jurisprudence.[180] With the increase in modern, automated surveillance, and the daily reality that people must surrender vast amounts of personal information to access the basic conveniences of life,[181] it is difficult to conclude that the Fourth Amendment as it is currently applied can provide robust privacy protections. Privacy is likely to continue to be undermined absent a statutory solution, a significant transformation in Fourth Amendment doctrine, or a change in constitutional interpretation to recognize the importance of freedom from surveillance in a democratic society.

B. *Anonymity, Expressive, and Associational Protections*

One route to establishing greater constitutional protections against facial recognition AI harms is by arguing that the First Amendment and Fourth Amendment, read together, protect individual freedoms to associate and to share expressions and ideas without surveillance and tracking.[182] Horizontal cybersurveillance—made possible by the integration of facial recognition AI into surveillance infrastructures, which can track not only identity, but also sentiment, emotion, expression, association, and ideas—implicates a

[177] *See, e.g.*, DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 251–54 (2017); David Gray, *A Collective Right to be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189, 191 (2015).

[178] *See, e.g.*, Transcript of Oral Argument at 3–5, *Jones*, 565 U.S. 400 (No. 10-1259).

[179] *See* Silverman v. United States, 365 U.S. 505, 508–11 (1961).

[180] *See, e.g.*, Riley v. California, 573 U.S. 373, 385 (2014); *Jones*, 565 U.S. at 402, 404–08.

[181] *See Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring) (explaining that persons using a GPS system are unwittingly giving up vast amounts of personal information about their habits and whereabouts); Smith v. Maryland, 442 U.S. 735, 748–49 (1979) (Marshall, J., dissenting) (describing how the Court determined that telephone subscribers have "no subjective expectations of privacy concerning the numbers they dial").

[182] *See, e.g.*, NAACP v. Alabama, 357 U.S. 449, 466 (1958) (holding an organization had immunity from disclosing its membership lists to the State because nondisclosure was necessary to protect members' freedom of association).

combination of Fourth Amendment and First Amendment values.[183] These issues are not without judicial precedent; for example, as early as 1958, the Supreme Court held that the First Amendment can include anonymity within its protections.[184]

Though anonymity protections have been affirmed under the First Amendment,[185] and anonymity is often considered to be a characteristic and incidental privilege of urban life,[186] the use of surveillance technologies has resulted in forced urban deanonymization. This has been justified by emphasizing transparent identities to promote safety and public benefit concerns. This Article contends that urban populations are especially vulnerable to weakened constitutional protections.[187] Constitutional protections may be uniquely at risk due to the forced deanonymization that will result from cybersurveillance, and the ambitions of both the public and private sectors to implement technologies that make identity more transparent.[188]

C. *Due Process and Self-Incrimination Risks*

Another avenue for securing greater constitutional protection from facial recognition AI and biometric cybersurveillance harms is through substantive

[183] *See, e.g.*, Hu, *Horizontal Cybersurveillance*, *supra* note 171, at 379–82 (citing Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1723 (2014)); ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE: A CONVERSATION (2013) (probing the historical and western origins of the modern surveillance systems and raising ethical and political questions about its expansion); Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) ("The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity . . . this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights.").

[184] *NAACP*, 357 U.S. at 462.

[185] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 336–57 (1995) (holding that an Ohio statute which prohibited the distribution of anonymous "campaign literature" violated the First Amendment); *see also* Talley v. California, 362 U.S. 60, 66 (1960) (holding that a city ordinance which required the disclosure of identifying information on distributed handbills was unconstitutional and violated First Amendment protections); Signature Mgmt. Team v. Doe, 876 F.3d 831, 839 (6th Cir. 2017) (holding that an anonymous blogger may stay anonymous, upon the resolution of an infringement case against him, because to compel him to reveal his identity would violate his First Amendment protections and "might hinder his ability to engage in anonymous speech in the future").

[186] *See, e.g.*, LAUREN ELKIN, FLÂNEUSE: WOMEN WALK THE CITY IN PARIS, NEW YORK, TOKYO, VENICE AND LONDON 1–23 (2016); JANE JACOBS, THE DEATH AND LIFE OF GREAT AMERICAN CITIES 55–65 (50th anniversary ed. 2011); Susan Buck-Morss, *The Flâneur, the Sandwichman and the Whore: The Politics of Loitering*, *in* WALTER BENJAMIN AND THE ARCADES PROJECT 33, 35–38 (Beatrice Hanssen ed., 2006); Judith A. Garber, *'Not Named or Identified': Politics and the Search for Anonymity in the City*, *in* GENDERING THE CITY: WOMEN, BOUNDARIES AND VISIONS OF URBAN LIFE (Kristine B. Miranne & Alma H. Young eds., 2000).

[187] *See supra* Section I.B.

[188] *See supra* Part II.

due process under the Fifth and Fourteenth Amendments.[189] Facial recognition AI can also pose risks of procedural due process deprivations[190] under the Fifth and Fourteenth Amendments, and self-incrimination concerns under the Fifth Amendment.[191]

Louis Brandeis and Samuel Warren proposed this theory on privacy protection through the Fifth and Fourteenth Amendments in 1890. Brandeis and Warren acknowledged that, under the common law, individuals retain the right to determine to what extent their "thoughts, sentiments, and emotions shall be communicated to others," and that individuals "generally retain[] the power to fix the limits of the publicity which shall be given them." Although Brandeis and Warren were discussing this in the context of copyright law and the publication of private facts, the principles they advocated for as the basis for the right to privacy—"the right to one's personality"—may form a basis for protections against broader surveillance regimes based on "collect-it-all" surveillance.

The Supreme Court recognized the potential impact that cybersurveillance and inference-based reasoning may have upon individuals in *Carpenter v. United States*.[192] The majority opinion, authored by Chief Justice Roberts, is worthy of careful consideration.[193] In *Carpenter*, the Court considered the constitutionality of warrantless collection of cell site tower geolocational data.[194] The Court concluded that accessing such data required a warrant in part because it could create a "comprehensive chronicle" of an individual's life. Previously, in *United States v. Jones*,[195] the Court considered the warrantless collection of GPS geolocational data.[196] In her concurrence in *Jones*, Justice Sotomayor reasoned that in the digital age, when information can be gathered, stored, and analyzed cheaply, location data is not just about location anymore.[197] It is transformed through inference-making into other, more historically sensitive information: "familial, political, professional, religious,

[189] *See, e.g.*, Ian Kerr, *Prediction, Pre-emption, Presumption: The Path of Law After the Computational Turn*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN: THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY 91, 92–93 (Mireille Hildebrandt & Katja de Vries eds., 2013); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1249–50 (2008); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 1 (2014); Hu, *Blacklisting*, *supra* note 11, at 1735.

[190] Brandon Garrett, *Artificial Intelligence and Procedural Due Process*, J. CONST. L. 2 (forthcoming 2025).

[191] *See, e.g.*, Citron, *supra* note 189, at 1281; Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 1957, 1989 (2021).

[192] 585 U.S. 296, 310–11 (2018).

[193] *Id.* at 300.

[194] *Id.* at 303.

[195] 565 U.S. 400 (2012).

[196] *Id.* at 402–04.

[197] *Id.* at 415–16.

and sexual associations."[198] In *Carpenter*, Chief Justice Roberts explicitly adopted Justice Sotomayor's reasoning from *Jones*.[199]

The Court's approach in *Carpenter* edged closer to a substantive due process approach to privacy, and potentially recognizes how limited traditional Fourth Amendment jurisprudence fails to protect against cybersurveillance harms. The Court previously suggested that substantive due process might be invoked to protect against informational privacy violations by the government.

The Court has also relied on substantive due process to protect liberty and privacy in personal settings, such as education and other parenting decisions. In *Griswold v. Connecticut*,[200] the Court suggested that personal privacy was protected by the Constitution, without necessarily clarifying where those privacy protections originated.[201] As the Court pointed out in *Griswold*, freedom of association is not spelled out directly in the Constitution or the Bill of Rights, and yet the Court recognized that this right is protected by the First Amendment.[202] The Court concluded that there is a right to privacy in making fundamental personal decisions in the interest of autonomy and dignity.[203]

Several prominent companies, such as Apple and Google, have adopted facial recognition technology. For example, Apple implemented a Face ID feature on their iPhone X which can unlock an iPhone with a simple look, rather than a fingerprint.[204] In 2015, Google followed with "Trusted Face" as part of the Android 5.0 Lollipop update.[205] Although most iPhone and Android users do not see the technology as anything other than something that unlocks their phones, the data gathered from the daily use of this technology can have far-reaching effects: "There's a whole lot of data carried in your face: your age, your gender, even your emotional state at the time. And, those are things that could be useful outside of simply authentication."[206]

[198] *Id.* at 415.

[199] *Carpenter*, 585 U.S. at 307.

[200] 381 U.S. 479 (1965).

[201] *See id.* at 483–85.

[202] *Id.* at 483.

[203] *Id.* at 485–86.

[204] *See* Arielle Pardes, *Facial Recognition Tech Is Ready for Its Post-Phone Future*, WIRED (Sept. 10, 2018, 7:00 AM), https://www.wired.com/story/future-of-facial-recognition-technology/ [https://perma.cc/5SFS-XKW7 (staff-uploaded archive)] (explaining the advent of facial recognition technology in iPhones and where facial recognition technology is expanding beyond phones).

[205] Lucas Mearian, *Facial Recognition Tech Moves from Smartphones to the Boardroom*, COMPUTERWORLD (Mar. 30, 2018), https://www.computerworld.com/article/3267488/facial-recognition-tech-moves-from-smartphones-to-the-boardroom.html [https://perma.cc/XC3V-GAMK].

[206] *Id.*; *see also* Adrienne LaFrance, *Who Owns Your Face?*, ATLANTIC (Mar. 24, 2017), https://www.theatlantic.com/technology/archive/2017/03/who-owns-your-face/520731/ [https://perma.cc/J7S3-AL43 (dark archive)].

Because one cannot hide one's face easily, and one regularly presents one's face in public, facial recognition AI can undermine rights to protect against self-incrimination. This is particularly the case when biometric security systems, such as Face ID on iPhones, can be used by law enforcement to unlock phone access through the presentment of a criminal defendant's face.[207] In *United States v. Michalski*,[208] for example, the police secured a warrant in 2018 to investigate a child pornography matter, and searched the defendant's smart phone by compelling the defendant to unlock the iPhone's Face ID with his face.[209] Media reports state this was the first instance where facial data was demanded pursuant to a criminal investigation to open access to phone information, including accessing documents and conversations that were stored on the iPhone.[210] The defendant later pleaded guilty to the charges, and the court did not hear a Fifth Amendment defense.[211] In contrast, another court denied an application for a search warrant that would have compelled unlocking digital devices through biometric identification such as facial recognition,[212] on the grounds that compelling the production of biometric data would violate the Fifth Amendment privilege against self-incrimination.[213]

D. *Right to Confrontation and Identifying Unacceptable and High-Risk Biometric AI Systems in the EU*

Facial recognition AI raises questions as to whether criminal procedure protections under the Fourth, Fifth, and Sixth Amendments can be assured when the utilization and application of the facial recognition AI itself is difficult to detect, assess, and analyze.[214] It specifically demands considering greater transparency and contestability for understanding "the source of the data collected and used, the nature of the algorithm, and the interpreter of the AI-enabled outcome" to conform to the Sixth Amendment protections, as required by the Confrontation Clause.[215] The Sixth Amendment mandates that a

[207] *See* Lily Hay Newman, *Why Cops Can Force You to Unlock Your Phone with Your Face*, WIRED (Oct. 1, 2018, 4:52 PM), https://www.wired.com/story/police-unlock-iphone-face-id-legal-rights/ [https://perma.cc/7SQP-B9QP] (documenting one of the first publicly known examples of law enforcement using a suspect's face to unlock a phone during an investigation).

[208] No. 2:18-cr-00230 (S.D. Ohio Apr. 08, 2019).

[209] Newman, *supra* note 207; Erin Corbett, *FBI Uses Suspect's Facial Data to Unlock iPhone*, FORTUNE (Oct. 1, 2018, 2:35 PM), https://fortune.com/2018/10/01/fbi-uses-suspects-facial-data-to-unlock-iphone/ [https://perma.cc/MG9X-8WMK]; Search and Seizure Warrant, United States v. Michalski, 2:18-mj-00707 (S.D. Ohio Sept. 19, 2018).

[210] Newman, *supra* note 207; Corbett, *supra* note 209.

[211] *See* Sentencing Memorandum at 2, 11, United States v. Michalski, 2:18-cr-00230 (S.D. Ohio Apr. 08, 2019).

[212] *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019).

[213] *Id.* at 1013, 1016.

[214] Hu, *Biometrics and AI*, *supra* note 155, at 294 (citing Roth, *supra* note 155, at 2048–50).

[215] *Id.* at 294, 298.

defendant be "informed of the nature and cause of the accusation" and the Confrontation Clause guarantees a right to know one's accusers.[216]

Confronting facial recognition AI that may be presented in a criminal case to establish the defendant's identity is complicated because the opportunity to confront AI witnesses is obscured by the AI "black box."[217] When AI informs evidence in criminal law processes, such as through reliance on facial recognition AI, it raises "black box" concerns whereby the Confrontation Clause is rendered largely ineffective.[218] The inscrutability of predictive analytics and correlative determinations through big data assessments has led to concerns of whether AI harms in a criminal proceeding can be adequately protected by the Sixth Amendment with an appropriate "confrontation" when the AI itself has little explanatory power.[219] "[I]n criminal cases, machine sources of accusation—particularly proprietary software created for litigation—might be 'witnesses against' a defendant under the Confrontation Clause."[220]

Recent developments in AI regulation, particularly in the EU, provide a potential pathway for considering the expansion of Sixth Amendment protections in light of facial recognition AI harms. The European Union ("EU") AI Act, for example, recognizes the need to regulate biometric identification technologies that have been integrated within AI systems.[221] The EU AI Act divides biometric AI systems such as facial recognition AI systems into multiple categories, including general-purpose AI models, high-risk AI systems, and unacceptable risk AI systems.[222]

In the category of high-risk AI systems, the EU identifies biometric identification deployed during the course of criminal investigations as systems that required pretesting, transparency, explainability, and human oversight.[223] Biometric identification systems that pose unacceptable risks in AI systems include "'real-time' remote biometric identification."[224] These systems include cognitive and behavioral manipulation, predictive policing and social scoring,

[216] U.S. CONST. amend. VI.

[217] Hu, *Biometrics and AI*, *supra* note 155, at 293–94; Roth, *supra* note 155, at 1978, 1983.

[218] Hu, *Biometrics and AI*, *supra* note 155, at 294 (citing Roth, *supra* note 155, at 1978).

[219] Roth, *supra* note 155, at 2048–50.

[220] *Id.* at 1983 (citing *contra* Brian Sites, *Rise of the Machines: Machine-Generated Data and the Confrontation Clause*, 16 COLUM. SCI. & TECH. L. REV. 36, 99–100 (2014)).

[221] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) arts. 5–7, 2024 O.J. (L 1689), https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [https://perma.cc/QX9V-ABJT].

[222] *Id.* art. 1(1), art. 6(1)–(2), annex III; art. 5(1)(e)–(h), (2)–(7).

[223] *Id.* art. 26(1)-(2), art. 13(1)-(3), art. (14)(1), art. (15)(1), art. 6(1)–(2), annex III.

[224] *Id.* art. 5(1)(e)–(h), (2)–(7).

and inferring emotion recognition.[225] In instances where the systems are deemed as threats to safety, fundamental rights, and the right to earn a livelihood, the systems are banned from use in the EU.[226] Generally, these systems are banned from public spaces.[227] However, they can be used by law enforcement authorities and for national security purposes in limited circumstances.[228]

Other EU and UK data privacy laws also allow for the challenge of facial recognition AI systems on a federalized scale. In the U.S., if the state offers biometric data privacy or facial recognition technology protection laws, the challenges must proceed on a state level until federal legislation is enacted.[229] Contrast this to the UK, where Clearview AI was alleged to violate multiple articles of the UK General Data Protection Regulation and other authorities in 2022 and was fined 7.5 million pounds, approximately $9 million.[230] The penalty was successfully appealed and overturned in 2023, as it was determined that the UK Information Commissioner did not have the jurisdiction to assess the penalty against Clearview AI.[231]

Additionally, the EU's General Data Protection Regulation ("GDPR")[232] has been relied upon to challenge the lawfulness of Clearview AI's operations in multiple EU nations.[233] Under article 6 of the GDPR, Clearview AI has been

[225] *Id.* (31)-(39), art. 5(1)(e)–(h).

[226] *Id.*

[227] *Id.* (38)-(39), art. 5(2).

[228] *Id.*

[229] *See* U.S. COMM'N ON C.R., 2024 STATUTORY ENFORCEMENT REPORT, THE CIVIL RIGHTS IMPLICATIONS OF THE FEDERAL USE OF FACIAL RECOGNITION TECHNOLOGY 2 (2024), https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf [https://perma.cc/3SLS-BS6N]; Laperruque, *Status of State Laws*, *supra* note 153; *Data Privacy and Biometric Technology Use*, THOMPSON REUTERS (July 22, 2024), https://www.thomsonreuters.com/en-us/posts/corporates/biometric-tech-use [https://perma.cc/43E3-846M].

[230] Chris Vallance, *Face Search Company Clearview AI Overturns UK Privacy Fine*, BBC (Oct. 18, 2023), https://www.bbc.com/news/technology-67133157 [https://perma.cc/Z9P7-BA34].

[231] Clearview AI, Inc. v. Info. Comm'r, [2023] UKFTT 00819 (GRC) (2023), https://www.bailii.org/uk/cases/UKFTT/GRC/2023/819.html [https://perma.cc/GEH2-XNW4]; Kashmir Hill, *Clearview AI Successfully Appeals $9 Million Fine in the U.K.*, N.Y. TIMES (Oct. 18, 2023), https://www.nytimes.com/2023/10/18/technology/clearview-ai-privacy-fine-britain.html [https://perma.cc/5K8J-MLPT (staff-uploaded, dark archive)] (last updated Oct. 19, 2023).

[232] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (119/1) [hereinafter EU 2016/679 GDPR]

[233] *See, e.g.*, *Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million*, EUR. DATA PROT. BD. (Mar. 10, 2022), https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en [https://perma.cc/29FU-Q2YU] [hereinafter *Italian SA Fines Clearview AI*]; *Hellenic DPA Fines Clearview AI 20 Million Euros*, EUR. DATA PROT. BD. (July 20, 2022), https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en [https://perma.cc/TS4L-NKNF] [hereinafter *Hellenic DPA Fines Clearview AI*]; *The French SA Fines Clearview AI EUR 20 Million*, EUR. DATA PROT. BD. (Oct. 20, 2022),

alleged to have violated the GDPR requirements for personal data processing.[234] The Clearview AI facial recognition AI system was also challenged as violating articles 12, 13, 14, 15, and 17 of the GDPR for violating the data rights of individuals.[235] In 2022, Italy, Greece, and France each imposed a €20 million fine on Clearview AI for violating the GDPR.[236] In 2023, Austria found that Clearview AI violated articles 5, 6, and 9 of the GDPR for data processing violations.[237] Most recently, in 2024, the Dutch Supervisory Authority for GDPR imposed a €30.5 million on Clearview AI in violation of articles 5, 6, and 9 for data processing infringements; article 12 in conjunction with article 14 for data transparency infringements; article 12 in conjunction with article 15 for denial of the right to data access; and article 27 for failure to designate a representative in the EU.[238]

In short, facial recognition AI systems are placing strains on criminal procedure protections under the Fourth, Fifth, and Sixth Amendments. It is critical, therefore, to look to the EU for greater guidance in how to construct AI protections. It is also important to view, as reflected in the EU's AI Act, the integrated impact of private facial recognition AI systems on both the private sector and law enforcement.

CONCLUSION

This Article aims to describe the unfolding trajectory from one-dimensional identification in urban settings—for example, law enforcement requesting to review someone's driver's license during a traffic stop—to multidimensional identification systems facilitated by algorithmic-driven AI embedded within urban settings—for example, scanning crowds or city streets with facial recognition technology then algorithmically assessing the individuals for threat risk. The investigation of the murder of Thompson utilized the most sophisticated surveillance technologies and facial recognition AI systems available to the NYPD. In the end, the suspect, Mangione, was not captured

https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en [https://perma.cc/XC8C-92JF].

[234] EU 2016/679 GDPR art. 6; *Italian SA Fines Clearview AI*, *supra* note 233; *Hellenic DPA Fines Clearview AI*, *supra* note 233; *French DPA Fines Clearview AI*, *supra* note 233.

[235] EU 2016/679 arts. 12, 15, 17; *Italian SA Fines Clearview AI*, *supra* note 233; *Hellenic DPA Fines Clearview AI*, *supra* note 233; *French DPA Fines Clearview AI*, *supra* note 233.

[236] *Italian SA Fines Clearview AI*, *supra* note 233; *Hellenic DPA Fines Clearview AI*, *supra* note 233; *French DPA Fines Clearview AI*, *supra* note 233.

[237] *Decision by the Austrian SA Against Clearview AI Infringements of Articles 5, 6, 9, 27 GDPR*, EUR. DATA PROT. BD. (May 12, 2023), https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en [https://perma.cc/3YMP-75CB].

[238] *Dutch Supervisory Authority Imposes a Fine on Clearview Because of Illegal Data Collection for Facial Recognition*, EUR. DATA PROT. BD. (Sept. 3, 2024), https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en [https://perma.cc/8G8J-ACFT].

through facial recognition AI. Instead, the suspect was identified through visual identification by a human witness. This case study underscores how sacrifices to digital privacy do not necessarily translate into the efficient identification and apprehension of suspects by law enforcement.

Further, although facial recognition AI risks extend beyond consumer protection harms and data privacy violations in civil law, currently, no omnibus AI law exists in the United States to comprehensively regulate these risks. This means that, in the absence of a comprehensive regulatory regime, facial recognition AI systems will be challenged under consumer protection and data privacy laws.

For instance, the Federal Trade Commission ("FTC") recently resolved a matter, *Federal Trade Commission v. Rite Aid Corp.*,[239] that involved algorithmic determinations that were part of a facial recognition AI system that demonstrates the blending of the private sector use of AI systems that then implicate criminal consequences.[240] In the matter, the FTC alleged that from 2012 until 2020, Rite Aid utilized facial recognition technology to detect criminal activity generally and shoplifting in particular.[241] Through its system, notification alerts were sent to Rite Aid employees' emails and phones, indicating that certain individuals who had entered the store were potential criminal matches.[242] Rite Aid employees would then take action against "match alert" individuals, such as increased surveillance, keeping patrons from making purchases, and banning the shoppers from the Rite Aid location.[243] It was alleged that the shoppers would be publicly shamed for past criminal activity, and detained or subjected to searches, while employees called the police to notify them that the shoppers may be potential criminals.[244]

As *FTC v. Rite Aid* demonstrates, the facial recognition AI system can have spillover effects, both implicating criminal and civil law. The criminal databases and facial recognition databases were aggregated to predict potential criminal activity. The Rite Aid "match alert" feature of the facial recognition AI system, that led to allegations of consumer discrimination and harassment, was treated as a consumer protection issue.[245] However, the system had been informed by criminal records and would lead to Rite Aid employees contacting law enforcement when the "match alert" was triggered.[246] This underscores the need for a federal omnibus AI law that extends protections in a way that recognize

[239] No. 2:23-cv-5023 (E.D. Pa. 2023).

[240] Complaint at 1–2, *Fed. Trade Comm'n v. Rite Aid Corp.*, No. 2:23-cv-5023 (E.D. Pa. 2023), [hereinafter Complaint, *Fed Trade Comm'n v. Rite Aid*].

[241] *Id.*

[242] *Id.* at 2.

[243] *Id.*

[244] *Id.*

[245] *See id.* at 7–10.

[246] *See id.*

that AI system risks might necessitate both criminal and civil protections simultaneously.

At present, facial recognition AI harms in the United States are largely challenged under consumer privacy and consumer protection laws, like the Clearview AI cases and the *FTC v. Rite Aid* case. As this Article explores, however, facial recognition AI implicates a range of constitutional protections and, in particular, anonymization protections under the First Amendment, due process protections, and criminal procedure protections. Forced urban deanonymization, through forced transparency of the identities of those who reside and travel in crowds and other dense populations, exacerbates these constitutional challenges.[247] The EU AI Act, by offering a horizontal regulatory regime that provides oversight of AI systems based on their anticipated impact on fundamental rights, does not divide the AI system regulation into either criminal procedure protections or civil consumer protections like the United States. Rather, the AI system is examined for its potential harms, which may span both criminal and civil contexts

The integration of algorithmic decision-making and AI into facial recognition technology poses new, unprecedented risks to privacy and individual autonomy rights, particularly in urban settings. The benefits of facial recognition AI are uncertain, and its efficacy is largely unproven and untested. Facial recognition technology is largely unregulated and poses significant constitutional concerns. EU's approach to AI oversight offers an important comparative perspective on regulatory approaches to facial recognition AI.

[247] *See, e.g.*, Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1363 (2015); Selinger & Hartzog, *Inconsentability of Facial Surveillance*, *supra* note 1, at 37–38.