THE TRIPARTITE MODEL OF FACIAL RECOGNITION: BRIDGING THE GAP BETWEEN PRIVACY, PUBLIC SAFETY, TECHNOLOGY AND THE FOURTH AND FIRST AMENDMENTS

SHLOMIT YANISKY-RAVID AND KYLE FLEMING *

Facial Recognition Technologies (FRT) are being rapidly adopted by federal agencies in the U.S. and across the globe. U.S. law enforcement agencies are increasingly using body-worn cameras, which implicate sensitive human and civil rights issues when paired with FRT. Federal agencies are not only using these technologies, but also investing in their future uses.

As the uses of FRT, in conjunction with massive investments in developing this technology, continue to expand, legislators, policymakers, academics, and others have called to entirely ban the use of FRT by law enforcement. The main reasons behind this resistance movement are the protection of human and civil rights, mainly privacy and equality. FRT opponents also argue that the technology is deemed to be inaccurate, biased and hence, inefficient and malfunctioning. Though much of this criticism is valid, the use of FRT provides many benefits, such as ensuring public safety by preventing crime, terror attacks and fraud, and even beyond law enforcement, among other functions, enabling remote communication, remote medical treatments, and remote transactions.

This article focuses on the tension between violations of privacy by FRT and the priorities of law enforcement to ensure public safety and protect citizens from terror and crime.

The article first delves into the constitutional principles that relate to privacy.

Facing a lacuna in regulating the uses of FRT by law enforcement, along with the lack of comprehensive regulation on data privacy, the article explores the question of whether the Supreme Court's constitutional approach to data privacy can modulate privacy protection in relation to the use of FRT by law enforcement.

---

* Professor of Law, PhD; Visiting Professor, Fordham University School of Law; Head of the IP-AI & Blockchain Research Project, Fordham Law Center on Law and Information Policy (CLIP); Professor Fellow, Yale Law School, Information Society Project (ISP); Professor of Law, Ono Academic College, Law School (OAC), Israel; Chair the Advanced Legal Studies and the Head of the Commercial Law, High-Tech and technology, Graduate School; Founder and Academic Director, the Shalom Comparative Research Institute, Eliyahu Law & Tech Center, OAC, Israel. I would like to thank Dean Matthew Diller, Fordham Law School; the late Professor Joel Reidenberg, the Founder of CLIP; Dean Elad Finkelstein, OAC Law School; Professor Jack Balkin, the Founder of Yale Law School, ISP, Professor Chinmayi Arun and Professor Nikolas Guggenberger, current and former Executive Director of Yale Law School, ISP; and to the entire ISP Resident Fellows for their support and contribution to the paper. Mr. Kyle Fleming, Intellectual Property and Information Law Attorney, Fish and Richardson, P.C.; J.D. Fordham Law School, B.S. Mechanical and Civil Engineering, Columbia University; Research Fellow, the Shalom Comparative Research Institute, Eliyahu Law & Tech Center, OAC. Special thanks to Jonathan Fenster and Gabriela Zashin for their outstanding and devoted work as research assistants and to Joseph Gergel, Laura Mahoney, Brigid O'Keefe and all the excellent editors of Notre Dame Journal of Law, Ethics & Public Policy for their professional comments and terrific editing.

With respect to the Fourth Amendment, the article discusses the progeny of the right to privacy, and how modern sense-enhancing digital technology may or may not fit within the up-to-date Supreme Court approach via tests that were developed in the leading cases of *Katz*, *Carpenter*, and *Jones*, among other cases. The article further explores the right to assembly and the right to anonymity through the lens of the First Amendment and the implications on FRT. We allege that despite a long progeny of cases defining the bounds of privacy and other relevant rights, the Court has struggled to fit cutting-edge technologies into existing legal rules. The article concludes that the use of FRT by law enforcement may not be in conflict with the Fourth Amendment, or with the First Amendment.

Unlike other scholars' and policymakers' suggestions to treat all uses of FRT equally, the article innovatively proposes a Tripartite Model, based on understanding the technology behind FRT and categorizes the various uses of FRT into three groups, according to the level of potential threat to privacy of each category: facial matching, facial recognition, and clustering and indiscriminate facial recognition. Adopting the Tripartite Model and approaching each of the uses differently, uniquely contribute to a better balance between the competing principles of an individual's interest in privacy with the state's (and public's) interest in public safety as well as the state's eminent power to protect the citizens.

Finally, the suggested solution uniquely points out the balance between the risks and the benefits and, more importantly, the need to forge constitutional principles to ensure the ethical and legal use of these systems in accordance with the technology itself.

I. INTRODUCTION

Facial recognition is a type of biometric technology based on artificial intelligence (AI) systems that tries to mimic how humans identify or verify faces by computerizing and analyzing images.[1] Recent advancements in AI systems have increased the accuracy of facial recognition technology (FRT), resulting in its increased use across a broad range of applications, including by private entities, the federal government, and law enforcement.

1. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-526, FACIAL RECOGNITION TECHNOLOGY: CURRENT AND PLANNED USES BY FEDERAL AGENCIES (2021); *see also* JOY BUOLAMWINI ET AL., FACIAL RECOGNITION TECHNOLOGIES: A PRIMER 8–10 (2020), https://global-uploads .webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTs PrimerMay2020.pdf [https://perma.cc/X8CH-JAV3] (explaining how an FRT system uses automated processes to recognize individuals through their unique characteristics and runs a comparison process to confirm identities); Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html (describing a 2017 high-speed chase in which FRT was successfully used. As the Dodge Magnum sped through north Florida, several Orlando police officers punctured its tires and brought the high-speed chase to a stop. The officers arrested the individual, but he had passed out and carried no identification card. Investigators ran a photo of the man through a large database and found a likely match).

As the uses of FRT continue to expand, there is a risk of potential troubling abuse by federal agencies and law enforcement, who use their own FRT or collaborate with private firms, while possibly violating human and civil rights without any regulation, inspection, examination, or certification. It has become increasingly important, as this paper addresses, to explore the technological and legal aspects of FRT, as well as to suggest ethical-legal principles for future regulation that will balance the good and the evil and possibly bridge the gap between the industry, the users, and the policymakers.[2]

Ultimately, facial recognition is a controversial technological tool. A technology that we like to hate. On the one hand, it has become part of many devices we are using (or developing), such as our mobile phones, in which we easily give up our privacy to enjoy its benefits.[3] On the other hand, there are many who oppose the use of this technology, including legislators, scholars, and even those within the industry itself.[4]

For many, the advent of FRT in the 3A Era of Advanced, Automated, and Autonomous AI systems of AI and machine learning brings to the forefront many of the dystopian fears present in George Orwell's novel *Nineteen Eighty-Four*.[5] Recent news of the authoritarian use of FRT in China, as part of the

---

2. *See* Valentino-DeVries, *supra* note 1.

3. *See* CLARE GARVIE ET AL., GEO. L. CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 16–22 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20 Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology% 20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/S48P-PL53] (describing the potential risks of FRT when used by law enforcement focusing on the risks of privacy, civil liberties, and civil rights); *see also* Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html (describing how Facebook, Amazon, Microsoft, and IBM reported plans to reduce the use of FRT for specific purposes, such as to unlock phones, following criticisms regarding accuracy and privacy); Fordham Law, *Conference: Facial Recognition Challenges and Solutions in Memory of Prof. Joel Reidenberg*, YOUTUBE (Mar. 29, 2021), https://www.youtube.com/watch?v=JO0M9ZbNm8U&t=12s (reflecting the different voices in regard to facial recognition systems—the technology that we love to hate and many voices have recently called to ban).

4. *See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206; *see also* Shlomit Yanisky-Ravid, *The EU Proposal on Regulation AI: Pros & Cons and Its Impact on Machine Vision, FR & Biometrics*, YOUTUBE, at 05:00 (June 14, 2021), https://www.youtube.com/watch?v=XIQNN3_U81w&t=1675s (describing and analyzing the EU proposal in general and to ban certain uses of FRT by law enforcement, the benefits, the risks, concerns and the consequences on the day after).

5. *See generally* George Orwell, NINETEEN EIGHTY-FOUR (1949) (describing a dystopian future in which much of the world has fallen victim to extreme government surveillance). *See also* Shlomit Yanisky-Ravid & Xiaoqiong (Jackie) Liu, *When Artificial Intelligence Systems Produce Inventions: The 3A Era and an Alternative Model for Patent Law*, 39 CARDOZO L. REV. 2215 (2018) (formulating the term "3A Era" to symbolize a new era where the traditional law regime is no longer relevant and new tools shall replace the missing legal rules).

social reform, has driven concerns about mass surveillance and a loss of privacy.[6] However, many countries, including the U.S., as a rule of thumb de facto, implement facial recognition software. U.S. federal agencies and law enforcement reported on a massive use of FRT for different purposes, and additionally have invested in the development of FRT systems for future uses.[7] This article focuses on the potential privacy issues that may occur as a result of the use of FRT by federal agencies and law enforcement.

As described in the U.S. Government Accountability Office's GAO report ("U.S. Gov't Accountability Report"), FRT is being used in several distinct manners. First, FRT is used for digital access and cybersecurity, to confirm the identities of individuals accessing government websites and to unlock agency-issued smartphones. Second, FRT is used by domestic law enforcement to enable federal agencies to investigate crimes by identifying people of interest by comparing their images to their mugshots. Additionally, agencies sometimes identify crime victims by comparing images with commercial systems that integrate publicly available images for cross-reference. For example, the Federal Bureau of Investigation was able to generate leads in a criminal investigation by comparing photos of unconfirmed individuals suspected of crimes with confirmed criminals through the Next Generation Identification Interstate Photo System. Third, FRT is used for physical security, in which federal agencies implement it to monitor locations to determine whether an individual, such as someone on a watch list, is present. Agencies can use real-time camera feeds to survey individuals suspected of criminal activity and automatically alert security personnel which allows for a more effective and efficient security network. Additionally, federal agencies reported FRT-related research and development projects, like researching their ability to detect faces under masks during the COVID-19 pandemic. Fourth, FRT systems are used by agencies like the Naval Criminal Investigative Service and Air Force Office of Special Investigations for border and transportation security. FRT is used in this capacity to identify or verify travelers within the United States or those seeking admission into the United States. Additionally, FRT is used to detect non-U.S. citizens already in the United States or seeking admission. One example is the Traveler Verification Service of the Department of Homeland Security's U.S. Customs and Border Protection which uses FRT to compare photos of travelers taken at a port of entry with existing photos in their databases, including U.S. passports, visas, and photographs from other encounters. Fifth, agencies like the Department of Homeland Security, Department of Defense, and Department of Justice use FRT for national security and defense purposes. This is primarily used to identify suspected terrorists and

6. *See* Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html (explaining how in China, millions of closed-circuit TV cameras placed all over the country currently monitor the everyday activities of citizens, around the clock); *see also* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1112 (2021) (describing the manner in which mass identification of individuals using face matching technology is used in China).

7. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 1.

monitor locations to search for a person of interest. The State Department uses the Integrated Biometric System which cross-checks terrorist watchlist photos with visa and passport application photos in an effort to decrease the possibility of a terrorist gaining access to such documents. Lastly, federal agencies like the National Aeronautics and Space Administration and Department of Defense use FRT to confirm employees' identities, to ensure that identification cards are given to the proper individuals, and to ensure that the size of the pictures printed on the cards are consistent.[8]

FRT used by federal agencies are owned either by themselves or by private entities that have access to federal databases and resources or have access to other entities' FRT systems owned by state, local, or commercial vendors. Furthermore, agencies reported plans to expand their investments and their use of FRT through fiscal year 2023.[9]

This new realm, on the one hand, may be beneficial, but, on the other hand, it introduces new profound concerns about potential malicious uses of FRT operated by artificial intelligence. First, many uses of facial recognition increase the risk of artificial decision-making that may be biased based on race and gender and hence are disproportionally discriminative against individuals from minority groups, people of color, and women.[10] Second, FRT may violate people's privacy by making use of photos that are published on the web without prior consent and acknowledgment from the individuals.[11] Third, the technology threatens people's freedom to express themselves by participating in assemblies, demonstrating, and moving freely in public spheres as they are being scanned by constant online surveillance. False alarms can cause people's detention or arrest.[12] Federal agencies and law enforcement have access to databases of millions of photos collected by private companies or federal or state agencies, such as the DMV, without consent, warrant, or reasonable background information to justify these uses.[13] Fourth, an inherent conflict of

8. *Id.* at 12–15.

9. *Id.*

10. Bobby Allyn, *IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance*, NPR (June 9, 2020, 8:04 PM), https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial -recognition-products-condemns-racially-biased-surveillance [https://perma.cc/2TR7-7CP7]; *see also* Paul Ohm, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. ONLINE 339, 340 (2012), https://www.pennlawreview.com/wp-content/uploads/2020/05/161-U-Pa-L-Rev-Online-339.pdf [https://perma.cc/U3FS-B9M8] ("But some Big Data projects will also lead to bad outcomes, like invasion of privacy and hard-to-detect invidious discrimination.").

11. *Half of All American Adults are in a Police Face Recognition Database, New Report Finds*, GEO. L. (Oct. 18, 2016), https://www.law.georgetown.edu/news/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds/.

12. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 747 (2008) ("The potential chilling effect due to relational surveillance poses serious risks not only to individual privacy, but to the First Amendment rights to freedom of association and assembly.").

13. *See* Kim Miller, *Facial Recognition: Current Uses, Concerns, and State Action*, MULTISTATE (Feb. 19, 2020), https://www.multistate.us/insider/2020/2/19/facialrecognition-current-uses-concerns-and-state-action; Zusha Elinson, *Police Use of Facial Recognition With*

interest exists where private companies are actively involved in the government's work and receive access to governmental sources while having their own commercial interests, which may not always align with what is best for public welfare.[14] Fifth, no standard, certification, or proof of FRT performance is requested before using FRT systems by law enforcement or private entities. Sixth, there is limited or no regulation and therefore, little transparency, in regard to the use, data, source, and technology being used.[15] From a broader perspective, the ethical legal challenges in regard to FRT are complex, especially as a result of the challenges of trying to ensure public safety by law enforcement, which is the focus of this paper, while also recognizing facial recognition's many advantageous purposes. For example, the Family Educational Rights and Privacy Act (FERPA) was enacted to protect students' right to privacy. A "record" is defined, under FERPA, as "any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche."[16] "Education records" are defined as those records, files, documents, and other materials that (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution. The restrictions on these records prevent many schools from using FRT or iron and gun detectors that may have prevented school shootings.

FRT holds many benefits for society even beyond security from the public (and the states') perspectives, especially in the realms of business and health. First, FRT manages to reduce time and energy by simplifying the check-in and check-out process.[17] An additional benefit is the capability to diagnose diseases and conditions with the help of a "health mirror." The term "health mirror" refers to a mirror that scans a patient's body and can deduce the current health status.[18] Medical researchers have implemented FRT to identify rare genetic diseases here and abroad.[19] Outside the U.S., the National Australia Bank

License Databases Spur Privacy Concerns, WALL ST. J (June 17, 2018, 7:00 AM), https://www.wsj.com/articles/police-use-of-drivers-license-databases-to-nab-crooks-spurs-privacyconcerns-1529233200; Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV. 552 (2021); William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2175 (2002).

14. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 1.

15. ERIK LEARNED-MILLER ET AL., FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE 3–4 (2020), https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf [https://perma.cc/5BGG -ML6V].

[16] Family Educational Rights and Privacy Act of 1974, 34 C.F.R. § 99.3(g) (2011)

17. Anastasiya Zharovskikh, *Facial Recognition for Healthcare Disruption: Key Use Cases*, INDATA LABS (July 2, 2020), https://indatalabs.com/blog/ai-face-recognition-in-healthcare (describing the benefits of FRT in healthcare, including the simplification of the check-in process, freeing personnel from paperwork, and eliminating wrong procedures and wrong-patient errors).

18. *Id.*

19. *Id.*

designed a program that allows clients to withdraw money from ATMs using facial recognition.[20]

FRT was also helpful when used by state and public agencies for civil purposes. There has also been the use of Facial Recognition software within airports. FRT helps reduce unnecessary traffic and helps quicken the process of boarding flights.[21] The DMV as well as banks use facial recognition nowadays to prevent fraud and identity theft.[22] Historians in the U.S. have used facial recognition to identify portraits of unknown soldiers in Civil War photographs ranging all the way back to the 1860s.[23] Outside the U.S., police in New Delhi recently were able to identify nearly 3,000 missing children in just four days.[24]

Without minimizing the threats and concerns, while also focusing on security and public safety, this article tries to better balance the potential benefits and drawbacks of FRT. According to the U.S. Gov't Accountability Report, the uses of FRT by federal agencies target public safety and prevention of crime.[25] Advanced, accurate, and sophisticated FRT brings to the forefront many advances in safety and security that enable law enforcement to ensure public safety. Currently, as described above, U.S. law enforcement agencies are engaging this new technology in innovative ways that can prevent crime and terror attacks, improving the day-to-day lives of citizens. [26] Officers can immediately identify terrorist threats from suspects who otherwise may have slipped through the cracks because they had authentic papers, but they cannot get past a successful facial recognition system.

At the end of the day, FRTs are likely going to be an inevitable part of our future; and therefore, this paper calls for policymakers to adopt a proactive balance, to ensure both public safety and the privacy of citizens without stifling the growth of this new technology.

Unlike other scholars, this article discusses FRT in terms of constitutional privacy and speech-related issues. Throughout the article, we aim to balance the negative and positive effects of this technology, as opposed to completely

---

20. *NAB and Microsoft Leverage AI Technology to Build Card-Less ATM Concept*, MICROSOFT (Oct. 23, 2018), https://news.microsoft.com/en-au/2018/10/23/nab-and-microsoft-leverage-ai-technology-to-build-card-less-atm-concept/ [hereinafter MICROSOFT] (describing how FRT is used in Australia to access ATMs).

21. Francesca Street, *How Facial Recognition is Taking Over Airports*, CNN (Oct. 8, 2019), https://edition.cnn.com/travel/article/airports-facial-recognition/index.html.

22. MICROSOFT, *supra* note 20.

23. Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.

24. Anuradha Nagaraj, *Indian Police Use Facial Recognition App to Reunite Families with Lost Children*, REUTERS (Feb. 14, 2020, 6:20 AM), https://www.reuters.com/article/us-india-crime-children/indian-police-use-facial-recognition-app-to-reunite-families-with-lost-children-idUSKBN2081CU.

25. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 1.

26. *See* GARVIE ET AL., *supra* note 3, at 1–4.

disregarding or outlawing it.[27] Additionally, the article proposes an alternative model based on understanding, on the one hand, how AI FRT works, and on the other hand, analyzing the current U.S constitutional challenges to void all FRT uses, and therefore, applying certain implications to different types of AI FRT. In this way, the article creates the missing dialogue between industry, users, and policymakers.

We suggest that the balance between the good and the evil aspects of FRT can be unfolded by following three steps: first, understanding the different categories within the technology itself, notably, by differentiating between the technology and the many uses of FRT; second, by understanding constitutional concepts of privacy protection and the limitations of the U.S. constitutional analysis to protect privacy against FRT uses; and third, by suggesting a model that differentiates between the different uses of FRT and accommodates the different uses to the level of privacy protection. Our recommendations target the challenge of protecting privacy when federal agencies and law enforcement use FRT and other biometric tools that may violate privacy.

The article opens with an introduction that examines the massive use of FRT by federal agencies and law enforcement and reviews the pros and cons of these uses. The following part explains how artificial intelligence, the system that FRT is based on, actually works. Then, it further discusses the different types of FRT: face matching, facial identifying, and face clustering. The third part describes the legal landscape, focusing primarily on the Fourth Amendment and the First Amendment. This part addresses the question of whether the U.S. Constitution can invalidate the use of FRT or serve as the people's shield against the violation of rights by FRT. There is uncertainty in relying on Supreme Court decisions in restricting certain uses of FRT. Furthermore, outlawing the entire technology may impair the governmental efforts to ensure public safety. The fourth part of this paper discusses theoretical approaches to the protection of privacy in relation to FRT. The last part of the paper proposes the Tripartite Model that balances the conflicting interests of protecting people's privacy and securing public safety. The model innovatively suggests dividing the legal norm into three categories according to the three types of FRT uses, as described in this article, equating the level of privacy protection to the threats of concern each type of use reveals.

27. *See* Yanisky-Ravid, *supra* note 4; *see also* Jagdish Chandra Joshi & K.K. Gupta, *Face Recognition Technology: A Review*, 8 IUP J. TELECOMMS. 53, 54 (2016) ("[F]eature-based methods . . . are based on local facial characteristics (such as eyes, nose and mouth) and use parameters such as angles and distances between ducial points on the face as descriptors for face recognition."); Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 J. MECHATRONICS & ROBOTICS 237, 240 (2019) ("Certain face recognition algorithms identify facial features by extracting markers or features from a face-to-face image. For example, an algorithm can analyze the position, size and/or relative shape of the eyes, nose, cheekbones and jaw. These features are then used to look for other matching features").

II. CURRENT STATE OF THE ART – THE DIFFERENT TYPES OF FRT USES?

Biometric technology identifies individuals by measuring and analyzing physical and behavioral characteristics including eye irises, fingerprints, voices, gait, movements, and images of their faces.[28] FRT may be classified as part of this field as it identifies individuals by their images. Through the use of photos or still photos from video feeds, FRT is able to verify and identify individuals by their faces. The photos are then converted into mathematical representations in computer language. Through cross-reference, the AI FRT algorithm compares and contrasts one photo with another to determine their similarity. [29]

First, to understand what AI-based FRT is, and what it is not, one should understand how AI systems work. Secondly, one should consider the distinction between face matching and other uses, such as facial identification and face clustering.

A. Artificial Intelligence (AI) Systems

Although there is no singular definition of "Artificial Intelligence," it has been universally understood as a system that is capable of performing human-like tasks, with the capabilities to create, learn, evolve, communicate, and make decisions.[30] Through technology's progress, AI has become more autonomous and intelligent. Through "neural networks," AI systems are able to mimic the function of human brains by computerizing and calculating data via a tremendous number of parameters that calculate formulas that "find" connections, patterns, and similarities within the digital representation of the data that they process and distinguish them from other data according to the information that they were "fed with" in the training process.[31] In contrast to traditional software, current AI systems have the ability to create work without human intervention in the calculation process itself.[32] Through training, an AI system will be provided with data from multiple examples with their correct classifications. The data will then be "broken" down into electrical signals in which the AI parameters calculate and identify a formula that can accurately identify the sort of data the system was trained with and differentiate it from

28. *Id.*

29. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 1, at 3–4.

30. Shlomit Yanisky-Ravid, *Generating Rembrandt: Artificial intelligence, Copyright, and Accountability in the 3A Era—The Human-Like Authors are Already Here—A New Model*, 2017 MICH. ST. L. REV. 659, 673 (2017).

31. Dana S. Rao, *Neural Networks: Here, There, and Everywhere—An Examination of Available Intellectual Property Protection for Neural Networks in Europe and the United States*, 30 GEO. WASH. J. INT'L L. & ECON. 509, 511 (1997).

32. *See generally* Mauricio Orozco-Alzate & Germán Castellanos-Domínguez, *Nearest Feature Rules and Dissimilarity Representations for Face Recognition Problems*, *in* FACE RECOGNITION 337 (2007).

other data.[33] The AI shall be tested with a new data set to determine its functionality, efficiency, and accuracy. Finally, through experience and new data, the AI system can complete tasks autonomously, adapting and evolving. However, the formula that the AI calculates by its parameters is unknown to the people involved in the process, and it keeps on evolving with the new data that the system absorbs. FRT is based on AI systems. Therefore, it is crucial to recognize the features of AI systems. AI systems are creative, unpredictable, independent and autonomous, rational, evolving, capable of data collection and communication, efficient and accurate, and they freely choose among alternative options. [34]

B. The Components of FRT

FRT requires three components: facial recognition AI software, a database, and a camera.

i. Facial Recognition Software

Facial recognition AI systems first begin by analyzing a face in a photograph or video, breaking the image into pixels that are symbolized to the system as numbers, and starting to calculate parameters that accurately identify the person's face with a formula.[35] Many of the parameters are unknown. However, few of them may be measuring the distance between facial landmarks ("nodal points"), such as between the eyes, the width of the nose, or the length of the jawline.[36] The software then synthesizes all of the information into what is known as a "face print," and organizes the face prints into databases.[37] Cutting-edge systems have evolved to incorporate a technology called "neural networks," a machine-learning algorithm incorporating artificial-intelligence techniques.[38]

33. Anders Krogh, *What Are Artificial Neural Networks?*, 26 NATURE BIOTECHNOLOGY 195, 195–97 (2008).

34. *See* Yanisky-Ravid & Liu, *supra* note 5.

35. William Crumpler & James A. Lewis, *How Does Facial Recognition Work? A Primer*, CTR. FOR STRATEGIC & INT'L STUDY 3–4 (June 10, 2021), https://www.csis.org/analysis/how-does-facial-recognition-work (elaborating on the technological mechanisms that allows FRT to break down images).

36. Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm (last visited Nov. 22, 2019).

37. TASK FORCE ON FACIAL RECOGNITION SOFTWARE, PROJECT ON GOV'T OVERSIGHT, FACING THE FUTURE OF SURVEILLANCE 10 (2019).

38. Greg Allen, *Understanding AI Technology: A Concise, Practical, and Readable Overview of Artificial Intelligence and Machine Learning Technology Designed for Non-Technical Managers, Officers, and Executives*, JOINT A.I. INTEL. CTR. (April 2020), https://apps.dtic.mil/sti/pdfs/AD1099286.pdf.

ii. Facial Recognition Databases

For facial recognition software to operate successfully, it needs to have a large database of images to draw from. Law enforcement agencies and other U.S. government agencies as well as state's Departments of Motor Vehicles (DMV) have large databases. The DMV contains a very substantial database of images; over 87% of the American population (over the age of sixteen) is licensed to drive.[39] As of 2016, there are currently over 131 million people with U.S. passports.[40] The FBI's NGI system has over 30 million photographs of an estimated 16.9 million people.[41] Back in 2014, it was reported that the federal government had invested approximately $1 billion into this system.[42]

In addition, the State Department maintains the "Terrorist Screening Center," which monitors and maintains reference "face prints" for anyone known or suspected of terrorist activity.[43] Lastly, local law enforcement agencies maintain databases of those suspected of gang activity.[44] Overall, it has been reported that 117 million Americans, regardless of whether or not they were involved in criminal conduct, are currently enrolled in a facial recognition reference database that, while collaborating with private FRT firms, serves the facial recognition interests of federal agencies and law enforcement.[45]

One of the many concerns is the question of whether the photos that build the databases must be given with explicit consent and a full understanding of the implications of FRT using the photo. The New York Police Department (NYPD) has explicitly stated that they do use facial recognition software, although only with lawfully obtained images.[46] However, the claim of strictly using lawfully obtained images was called into question considering the fact that police departments have used the private company Clearview AI's facial recognition software.[47] One of the many examples of the question of consent is

39. Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1599–1600 (2017).

40. U.S. DEP'T OF STATE, BUREAU OF CONSULAR AFFAIRS, *U.S. Passports & International Travel: Passport Statistics*, https://travel.state.gov/content/passports/en/passports/statistics.html (last visited Nov. 22, 2019).

41. U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 10 n.23 (2016), https://www.gao.gov/assets/680/677098.pdf.

42. Jose Pagliery, *FBI Launches a Face Recognition System*, CNN BUSINESS (Sept. 16, 2014), https://money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition/.

43. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 41, at 16 tbl.2.

44. Hirose, *supra* note 39, at 1599.

45. GARVIE ET AL., *supra* note 3.

46. George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology in Siege of Black Lives Matter Activist's Apartment*, GOTHAMIST (Aug. 14, 2020), https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

47. Evan Selinger & Albert Fox Cahn, *Did You Protest Recently? Your Face Might be in a Database*, THE GUARDIAN (July 17, 2020), https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database.

when a photo is uploaded by a person to social media, as seen in the Derrick Ingram case.[48] After being accused of assault by shouting into a police officer's ear with a bullhorn, a slew of police went to Ingram's home with the intent to arrest him. The NYPD stated that they had captured the face of Ingram on surveillance cameras throughout the streets of New York, although many have expressed disbelief and have asserted that the image that NYPD had used was in fact taken from Instagram.[49] This discussion involves the third inoperable component of facial recognition systems – the camera.

iii. Facial Recognition Cameras

Lastly, for FRT to be effective as an investigative or surveillance technology, the state needs to have access to a network of cameras. In China, as discussed previously, there are around 200 million CCTV cameras across the country.[50] The United Kingdom's network is particularly developed as well, with an estimated 5.9 million CCTV cameras spread throughout the nation.[51] The United States has a surprisingly large amount of publicly owned and operated cameras in dense cities like New York and Los Angeles.[52] Chicago, for instance, has 30,000 cameras throughout the city, and even smaller cities like New Orleans and St. Louis have begun to build up their camera networks.[53]

Stationary cameras, however, are not the only source of video feed for law enforcement. Across the nation, police forces are implementing the use of body-worn cameras.[54] The U.S. Department of Justice has awarded over $20 million in body-worn cameras through grants called "Smart Policing Initiatives."[55]

---

48. James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, THE VERGE (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

49. *Id.*

50. *See* Robert B. Zoellick, Deputy Sec'y of State, Dep't of State, Remarks to National Committee on U.S.-China Relations (Sept. 21, 2005) (transcript available in the U.S. Dep't of State Archive) https://2001-2009.state.gov/s/d/former/zoellick/rem/53682.htm.

51. James Temperton, *One Nation under CCTV: The Future of Automated Surveillance*, WIRED (Aug. 17, 2015), https://www.wired.co.uk/article/one-nation-under-cctv.

52. AMERICAN CIVIL LIBERTIES UNION, *What's Wrong with Public Video Surveillance?* (Mar. 2002), https://www.aclu.org/other/whats-wrong-public-video-surveillance.

53. Marc Jonathan, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity Blitz*, 82 TEX. L. REV., 94 (2004)

54. U.S. DEP'T OF JUSTICE, *Department of Justice Awards over $20 Million to Law Enforcement Body-Worn Camera Programs* (Sept. 26, 2016), https://www.justice.gov/opa/pr/department-justice-awards-over-20-million-law-enforcement-body-worn-camera-programs.

55. *Id.*; *see also* Ava Kofman, *Real-time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, THE INTERCEPT (Mar. 22, 2017), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/ (noting that private companies are racing to connect body-worn cameras to their real-time facial recognition software).

Additionally, law enforcement does not need to rely solely on publicly owned video sources. Police are increasingly relying on privately owned cameras by enticing citizens to register their home surveillance cameras with law enforcement's network.[56] Considering the rapid increase in popularity of affordable products like Amazon's Ring, there is a significant threat of unrestrained growth of law enforcement's surveillance network.[57]

As is typical of the twenty-first century, the law regarding technological surveillance is being greatly outpaced by the technology, and the courts need to think proactively about how to adjust its privacy approaches to properly deal with the changing environment. Therefore, the Tripartite Model we are suggesting in this paper is based on understanding the technology, specifically, the three types of FRT uses that the next section addresses.

C. The Types of AI Facial Recognition Technology

Face matching is the process that uses software in order to compare two images and return either a yes or no; facial identifying goes a step further, comparing a photo or a frame from a video to a database and returning a name or profile of the subject.[58] Face clustering occurs when a camera records every face it sees while implementing software to categorize its subjects.[59] Face clustering is based on images from open-sourced libraries such as Google, YouTube, and even social media profiles. This technique can enable the recognition of a massive amount of people without their awareness or their consent for all purposes and it can even create faces that do not exist in photos and videos.[60]

i. Face Matching

Searches and comparisons through facial recognition are generally classified into two categories: verification and identification. Verification aims to confirm that an individual in a stored photo is the same person as an individual in another stored photo. This is known as a one-to-one search. In a

---

56. Faith Karimi, *Home Surveillance Cameras are the New Neighborhood Watch*, CNN (Aug. 31, 2018), https://www.cnn.com/2018/08/30/us/home-surveillance-cameras-neighborhood-watch/index.html.

57. Ben Fox Rubin, *Amazon's Ring Takes Heat for Considering Facial Recognition for its Video Doorbells*, CNET (Dec. 14, 2018), https://www.cnet.com/news/amazons-ring-takes-heat-for-considering-facial-recognition-for-its-video-doorbells/; *see also* James Vincent, *Facial Recognition Smart Glasses Could Make Public Surveillance Discreet and Ubiquitous*, THE VERGE (June 10, 2019), https://www.theverge.com/2019/6/10/18659660/facial-recognition-smart-glasses-sunglasses-surveillance-vuzix-nntc-uae (*Vuzix*'s glasses operate as a scanning camera-like tool that implement the use of FRT, allowing the wearer to scan any crowd and compare the face to images in a database that contains over one million images. The glasses have a very high accuracy rate and are currently being sold strictly to law enforcement).

58. PROJECT ON GOV'T OVERSIGHT, *supra* note 37, at 10.

59. *See id.*

60. *See* Sawinder Kaur, Parteek Kumar & Ponnurangam Kumaraguru, *Deepfakes: Temporal Sequential Analysis to Detect Face-Swapped Video Clips Using Convolutional Long Short-Term Memory*, 29 J. ELEC. IMAGING 3 (2020), https://doi.org/10.1117/1.JEI.29.3.033013.

one-to-many search or identification, a photo of a single individual is compared to a library of stored images where a cross-reference is used to determine whether there is a match. This is often used to identify an unknown individual in a photo taken at a crime scene.[61]

The most basic form, face matching, is already prevalent in the United States today. Back in 2018, face matching was used prominently by the FBI, conducting over 52,000 searches using the Next Generation Identification (NGI).[62] Additionally, in 2016 the Georgetown Law Center on Privacy & Technology surveyed law enforcement agencies across the country, finding that at least 52 local or state agencies had engaged in, or were preparing to adopt this technology and that at least one in every four local agencies has the option to run searches.[63] Face matching has shown to be an effective law enforcement tool for investigative purposes.

Outside of law enforcement, face matching techniques have also been used effectively by the DMV for detecting fraudulent driver's licenses.[64] Between 2010 and 2015, New York's DMV identified 14,500 people who have been issued more than one license for fraudulent purposes.[65] Similarly, the DMV in New Jersey identified 2,500 fraud cases using the technology.[66] Face matching has also been used by the United States Customs and Border Protection agency (USCBP) in its "biometric exit program," a tool that checks the identity of an individual boarding a flight to leave the country against photos from the flight manifest of passengers.[67] Face matching is a much more simplistic application of general FRT, and does not typically incur the same constitutional and privacy related issues that facial recognition does. We argue that the question of face matching does not stand alone. It should be combined with questions such as how does one obtain the data (e.g., the photos) that enables systems to match the face to a person; what is the purpose of using the face matching; is there a legitimate and justified legal-ethical goal; and are there alternative more proportional and less pervasive means to obtain the legitimate goal? Nevertheless, we argue that this method is less challenging to privacy violations than the others, as detailed below.

---

61. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 1, at 4.

62. Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 Geo. Mason L. Rev. 409 (2013–2014). *See also*, *September 2019 Next Generation Identification (NGI) System Fact Sheet*, FBI, https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view (last visited Nov. 22, 2019).

63. *See* GARVIE ET AL., *supra* note 3, at 15.

64. *See* Jenni Bergal, *States Use Facial Recognition Technology to Address License Fraud*, GOVERNING (Jul. 15, 2015), https://www.governing.com/topics/public-justice-safety/states-crack-down-on-drivers-license-fraud2.html.

65. *Id.*

66. *Id.*

67. *See* Frank Bajak & David Koenig, *Face Scans for US Citizens Flying Abroad Stir Privacy Issues*, ASSOCIATED PRESS (July 12, 2017), https://apnews.com/acf6bab1f5ab4bc59284985a3babdca4.

ii. Facial Identifying

Facial identifying is the technique of comparing photographs and video footage to existing databases, allowing the software to return a name or profile, rather than a simple yes or no. Facial identifying techniques break down into two categories: historical facial recognition, and real-time facial recognition.

Historical (past) facial recognition involves taking an existing video or photo after the event has taken place. This technique is particularly useful for investigative purposes, such as when law enforcement has surveillance footage, or in identity theft cases.[68] Historical facial recognition can be exploited with the use of 3D software, as well. For example, in 2017, the NYPD took surveillance footage from a nightclub where a shooting had occurred, created a full 3D model of the suspect, and then used facial recognition software and a database of images to identify 200 possible suspects.[69] Investigators were then able to narrow this list, using physical characteristics and other information, down to a single suspect, who was ultimately shown to witnesses to confirm.[70]

We argue that historical facial recognition equips law enforcement with a powerful new investigative tool, but with it come important privacy and bias concerns. The use of this tool essentially considers every citizen as a potential criminal. It also allows law enforcement to follow us wherever, whenever using our data trail through the means of surveillance cameras, social media, phone location, and more. This means that more likely than not, law enforcement has a photo of every citizen on file in a database.[71]

Real-time facial recognition, of course, is an exponentially greater threat to privacy.

Federal agencies access private companies, which conduct on their behalf facial recognition searches using publicly available images in order to assist with identifying subjects of criminal investigations.[72] For example, they help to identify perpetrators and victims in domestic and international child exploitation cases, to identify criminals, and to identify subjects who have been arrested previously, were deported, or attempted to re-enter the United States at the border.[73]

---

68. *See, e.g.*, United States v. Green, No. 08-44, 2011 WL 1877299, at *2 (E.D. Penn. May 16, 2011).

69. *See* Greg B. Smith, *Behind the Smoking Guns: Inside the NYPD's High-Tech Battle Against Gun Crimes*, N.Y. DAILY NEWS (Jul. 8, 2014).

70. *See id.*

71. *See* Matthew Wall, *Is Facial Recognition Tech Really a Threat to Privacy?*, BBC NEWS (June 19, 2015), https://www.bbc.com/news/technology-33199275.

72. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (March 18, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

73. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 1, at 4.

The earliest example of real-time facial recognition being used by law enforcement was in the 2001 Super Bowl.[74] Thousands of fans were scanned and checked against a database for wanted and suspected criminals, ultimately identifying 19 individuals in the crowd with outstanding warrants.[75] Similarly, in 2013, real-time facial recognition software was used, albeit unsuccessfully, during the immediate aftermath of the Boston Marathon bombings in an attempt to identify and find the suspects.[76]

Despite the inherent privacy concerns, facial identifying proves to be a beneficial tool for public safety. However, due to the intensified intrusion into privacy, this tool must be carefully monitored and regulated.

iii. Face Clustering

An even further invasion into one's privacy can be caused by the technique of face clustering, which monitors all subjects that come into the field of view, rather than individual targets. Face clustering software then problematically categorizes individuals who are scanned based on certain features such as gender, ethnicity, or age range as well as other traits, features, and categories.[77] This technology can also track facial features or movement to recognize expressions or gaze, among other analyses. Facial analysis can be part of an eye-tracking system or used by Google Glass.[78]

We state that this technology raises a lot of challenges and concerns with respect to human and civil rights.

Without minimizing the many concerns, there may be legal and beneficial purposes for face clustering. For example, face clustering can be used to identify gamblers in casinos who behave inappropriately,[79] or even spot

74. *See* Jennifer Tucker, *How Facial Recognition Technology Came to Be*, BOS. GLOBE (Nov. 23, 2014, 12:17 AM), https://www.bostonglobe.com/ideas/2014/11/23/facial-recognition-technology-goes-way-back/CkWaxzozvFcveQ7kvdLHGI/story.html.

75. *See* Kaleigh Rogers, *That Time the Super Bowl Secretly Used Facial Recognition Software on Fans*, MOTHERBOARD (Feb. 7, 2016, 9:13 AM), https://www.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans.

76. *See* Brian Ross, *Boston Bombing Day 3: Dead-End Rumors Run Wild and a $1B System Fails*, ABC NEWS (Apr. 20, 2016, 6:00 AM), https://abcnews.go.com/US/boston-bombing-day-dead-end-rumors-run-wild/story?id=38375724.

77. *See* Mei Wang & Weihong Deng, *Deep Face Recognition with Clustering Based Domain Adaptation*, 393 NEUROCOMPUTING 1 (2020).

78. *See* Julia Calderone, *Eye Tracking in Google Glass: A Window into the Soul?*, SCI. AM. (Jan. 1, 2015), https://www.scientificamerican.com/article/eye-tracking-in-google-glass-a-window-into-the-soul/.

79. *See* Dan Robson, *Facial Recognition a System Problem Gamblers Can't Beat?*, TORONTO STAR (Jan. 12, 2011), https://www.thestar.com/news/gta/2011/01/12/facial_recognition_a_system_problem_gamblers_cant_beat.html.

underage people drinking alcohol at a bar, both for the safety of other attendees.[80] However, there are far more nefarious purposes as well.

Likely the most well-known use of large-scale face clustering is the Chinese social scoring system. Since its first pilot implementation and more so after 2020, around 300 million closed-circuit television (CCTV) cameras have been activated in China.[81] China's system is aimed at recording all citizens' behavior, digitizing that data, and implementing sanctions and rewards to incentivize what the government has determined to be "good" behavior.[82] Bad behaviors include major transgressions such as drunk driving or fraud, but also include other activities like playing too many video games.[83] In 2017, 6.15 million Chinese citizens were barred from getting on planes because of their social scores.[84] The dragnet use of mass surveillance by the Chinese government is a vivid illustration of the overreach that can occur when the state is free to employ new technologies without proper control, restraint, and regulation. Recently, China adopted privacy regulations that have been in force since November 1, 2021. The "Personal Information Protection Law" limits the violation of privacy by private entities with fewer restrictions on the state, especially in relation to previous laws.[85]

In Daniel Solove's article, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, he articulates the conceptualization of the current privacy problem.[86] He argues that the current issue at hand deals with the government's use of databases, which are identified as collecting information for the purposes of record keeping.[87] Despite these concerns, in the United States throughout the years there has been an increase in the use of the collected data that manifest in social security numbers, public records, property ownership, voter registration, and even DNA.[88] All this information is stored

80. *See* Ryan Breslin, *Bars Using Facial Recognition to Prevent Underage Drinking*, SPECTRUM NEWS (June 23, 2017, 9:48 PM), https://spectrumlocalnews.com/nc/triad/top-videos/2017/06/23/bars-using-facial-recognition-to-prevent-underage-drinking.static.

81. *See* Mozur, *supra* note 6.

82. *See* Bernard Marr, *Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?*, FORBES (Jan. 21, 2019, 12:37 AM), https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#1c9adf5948b8.

83. *See* Nadra Nittle, *Spend "Frivolously" and be Penalized under China's New Social Credit System*, VOX (Nov. 2, 2018, 6:50 PM), https://www.vox.com/the-goods/2018/11/2/18057450/china-social-credit-score-spend-frivolously-video-games.

84. Lily Kuo, *China Bans 23m from Buying Travel Tickets as Part of 'Social Credit' System*, THE GUARDIAN (Mar. 1, 2019, 8:48 AM), https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system.

85. *See* Eva Xiao, *China Passes One of the World's Strictest Data-Privacy Laws*, WALL ST. J., (Aug. 20, 2021), https://www.wsj.com/articles/china-passes-one-of-the-worlds-strictest-data-privacy-laws-11629429138.

86. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

87. *Id.*

88. *See id.* at 1403.

in over 2000 databases that are maintained on a state and federal level. The legal challenges that Solove provides depict a dystopian society, which he compares to George Orwell's Big Brother narrative.[89] The current situation has resulted in the bureaucratic authority having complete power over civilians, where there is little control over what information civilians consent to giving, and the bureaucratic process in which decisions are made.[90]

III. LEGAL LANDSCAPE – CAN THE FOURTH AMENDMENT PROTECT PEOPLE'S PRIVACY AGAINST FRT?

A. The Current Legal Regime

There has yet to be any federal statute regarding law enforcement's use of FRT. Therefore, modern courts will rely on constitutional law and the respective progeny of cases.[91] However, the Washington State Bill includes limitations on the use of FRT, among them, [92] there are clear guidelines that state the exact terms of how a state or government agency shall apply to use FRT, requiring a limited warrant in order to use FRT for ongoing surveillance. Additionally, there are cases in which various uses of facial recognition systems are deemed unnecessary. For example, a state or local government may not use FRT to identify a person based on their religious, political, or social beliefs.[93] In 2021, the Facial Recognition and Biometric Technology Moratorium Bill was also introduced, prohibiting biometric surveillance by the Federal Government, without explicit statutory authorization.[94]

Locally, sporadic U.S. states took a stance and regulated local acts focusing mainly on the use of consumer biometric data, which may influence the uses of FRT by either banning or limiting the use of FRT. Biometric technology may include FRT, as explained above, because it refers to systems that, through an automated process, can recognize or identify the individual based on their biological or behavioral characteristics.[95]

We allege that there are drawbacks to the current legal regime.

First, there is no U.S. Constitutional protection to privacy in general, nor to privacy of data or online data. Second, there is no general cohesive federal legislation in regard to FRT and more specifically to the uses of FRT by federal agencies. Third, the lack of harmonization among states is crucial when we address online data. Fourth, and most importantly from this study's perspective, the regulation does not reflect the understanding of the technology itself. Fifth,

89. *Id.* at 1413.

90. *Id.* at 1422.

91. *See* Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. 57, 63 (2019).

92. E.S.S.B. 6280, 66 Leg., Reg. Sess. (Wash. 2020).

93. *See id.*

94. *See* S. 2052, 117th Cong. (2021).

95. *See* KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE, 18–19 (2011).

the acts do not differentiate among the different types of FRT, as our Tripartite Model suggests.

Regarding data privacy law, the European Union (EU) enacted sweeping legislation in 2018 called the General Data Protection Regulation (GDPR).[96] The EU has recognized the right to privacy for one's personal data which is widely defined. However, the GDPR as well as CCPA provide an exemption for law enforcement when collecting data for the purposes of investigation or prosecution.[97] The EU Proposal on Regulation AI suggested directly outlawing surveillance through AI systems when encountering unacceptable risks, such as social scoring and live FRT. When there is a high risk to human rights, such as the use of FRT and biometrics, on some occasions, by law enforcement, as well as, for recruitment, medical services, and education, with limited exceptions (e.g. in the case of immediate threat or victims), the user would have to receive prior approval.[98] The EU Proposal on Regulation AI further suggests accountability and transparency rules, clarifying who is liable for failure to comply with the regulation, (e.g. the provider and the user), creating a new EU AI member states agency for the governance of AI on the member states level, and suggesting very high sanctions of thirty million Euro or six percent of the entity total worldwide annual turnover, whichever is the higher as an administrative decision. [99]

This article calls for a balanced approach between privacy and public safety based on the way the technology is built and the use of FRT.

In the absence of coherent and harmonized regulation in regard to the use of FRT by law enforcement and in light of the intensive use of FRT by these forces and the massive investments in the future, the next steps are to explore the Supreme Court precedent of a constitutional approach to privacy and freedom of assembly. Then we can suggest principles for a solution that will reflect this Supreme Court constitutional approach while understanding the technology and adequacy of these to the challenge that FRT imposes.

Thus, facing a lacuna in formal legislation, courts will rely on case law to address the First and Fourth Amendment claims that may be brought regarding FRT. As discussed *infra*, part of that analysis involves deciding if society has an objectively reasonable expectation of privacy in a certain area.[100] To make that judgment, courts often rely on Congress to be the voice of the people and look to what legislation on the subject matter has passed. Here, the courts should view consumer data privacy law and consumer biometric data law as relevant contexts.

---

96. *See* Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED UK (Mar. 24, 2020, 4:30 PM), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

97. *See* HIPPA J., *GDPR Exemptions: Who is Exempt from GDPR Requirements?* (May 11, 2018), https://www.hipaajournal.com/gdpr-exemptions-who-is-exempt-from-gdpr/.

98. *See Proposal for a Regulation of the European Parliament*, *supra* note 4, Titles II-III, Articles 5–6.

99. *See id.* at Articles 12–13 (Record-keeping and Transparency); Title VI (New Agent member states), and Article 71 (penalties).

100. *See infra* Part III.B.

B. Fourth Amendment Privacy Considerations Under Supreme Court Privacy Decisions

Discussions regarding the Fourth Amendment implications on FRT usually revolve around deciding whether to favor privacy over public safety; the two, however, are not mutually exclusive. FRTs can better equip law enforcement agencies for investigations, identify missing persons and/or suspects, and ensure public safety during emergency situations. Yet, as Justice Sotomayor stated in *United States v. Jones* (discussion *infra*[101]), abuse can result in surveillance of "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."

We assert that there are real benefits of FRT that should not be foregone because of the possibility of abuse; rather proper safeguards and regulations must be put in place so that these gains may be properly realized.

The Fourth Amendment protects against unreasonable searches and seizures.[102] Where a person may have a reasonable expectation of privacy, the Supreme Court laid out a two-part test in *Katz v. United States*: (1) whether the person, *subjectively*, demonstrates an expectation of privacy, and (2) whether that expectation is one that society, *objectively*, recognizes as reasonable.[103] Prior to *Katz*, privacy considerations under the Fourth Amendment primarily focused on trespass to property or body searches; the *Katz* test, however, extended the right to privacy beyond an individual's home, and instead to wherever society deems there to be an expectation of privacy.[104] We claim that *Katz*, however, does not provide comprehensive guidelines in regard to the numerous challenges of the 3A digital era and data economy.

In *Katz*, law enforcement, without a warrant, attached an electronic listening device to a phone booth that was partially constructed of glass, so to be able to listen in on Charles Katz's conversation.[105] Under common law, because this action was done in public, it would not be protected by the Fourth Amendment. The Court found that when Katz closed the door to the booth however, he exhibited a subjective expectation of privacy and thus protected the conversation from the "uninvited ear," even if his actions were not protected from the "intruding eye."[106] This holding extended privacy protections under the Fourth Amendment to public spaces where there is a reasonable expectation of privacy.

Due to the lack of explicit and direct protection of data in a mandatory legal rule, neither in the U.S. Constitution nor in most of the states' laws, court decisions are the main sources to rely on. However, the expectation of privacy

---

101. *See infra* Part III.d; United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 12 N.Y.3d 433, 441-442 (2009)).

102. *See* U.S. CONST. amend. IV.

103. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

104. *See id.* at 351 ("For the Fourth Amendment protects people, not places.").

105. *See id.* at 349, 352.

106. *Id*. at 352.

test is very vague and unclear, especially when discussing data. This situation results in an uncertain realm.

A lot of questions arise when addressing, applying, and implementing the expectation of privacy rule to FRT. Do we refer to the uploading of the photos; the use; the maintaining of the data, or to FRT in general? How can someone conclude on subjective or objective expectations in this regard? Professor Mariko Hirose argues that because "people in contemporary American society have the reasonable expectation of privacy in identifying information about themselves even as they expose their faces to public view," that under *Katz*, such information should be protected by the right to privacy.[107] However, this conclusion analyzes only the second prong of *Katz*. The first prong is more challenging though: how may a person, who has not *subjectively demonstrated* an attempt to protect their face from the "intruding eye," be protected by the right to privacy under *Katz*?

Considering only the *Katz* second prong, in regard to FRT, it is not so obvious that society has an objectively reasonable expectation of privacy in facial data. In 2015, the Pew Research Center conducted a study that found 81% of people "agree that surveillance cameras are hard to avoid."[108] Noting that the majority of people may believe they are under near-constant surveillance, a court may well consider the lack of any significant protest or outcry as an indicator that this is not an area of privacy our society feels very strongly about.
On the one hand, if we rely on statistics to prove the second objective test of *Katz*, there may not be a reasonable expectation of privacy for FRTs, largely because of statistics that indicate people don't think they can avoid FRTs.[109] However, on the other hand, a question may arise as to whether the second (objective) prong of *Katz* is an empirical question (do people think that their photos will be kept private and won't be used to FRT) or a normative question (*should* a sphere of privacy be recognized here). The criticism is based on the redundancy of *Katz's* subjective expectation of privacy test.[110]

Even when accepting the normative approach to expectation of privacy, one can still claim that public safety shall allow under limitation the use of tools, once proven efficient for the purpose of preventing crime and terror. Additionally, we contend that many uses of FRTs may not fit within the *Carpenter* claim as discussed below.[111] A broader understanding of the

---

107. *See* Hirose, *supra* note 39, at 1601.

108. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RSCH. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-viewsabout-data-collection-and-security/ [https://perma.cc/9LRA-3E95].

109. *See, e.g.*, Jamali v. Maricopa Cnty., No. CV-13-00613, 2013 WL 5705422, at *2 (D. Ariz. Oct. 21, 2013) (holding that the Maricopa County Sheriff's "seizure and publication of Plaintiff's [mugshot] and personal information did not violate his Fourth Amendment rights").

110. *See* Hirose, *supra* note 39, at 1601. In *Carpenter* (see *infra* Part III.B.i) for example, the Court uses the normative approach to the second test of *Katz* precisely because there is no way to avoid cell phone use, the same as there may be no getting away from FRT exposure.

111. *See infra* Part III.B.i.

protection of data privacy may establish a legal interest in the protection of privacy under the Fourth Amendment that may limit certain uses of FRT.

We contend that the classic and current definition of privacy is a narrow one. "The right to be left alone" does not include situations that modern day technology creates.[112] Privacy violation needs to be redefined to include not only physical intrusion but also receiving information without consent, specifically through investigation on social media platforms.[113]

The "balloon theory of privacy," by the author Yanisky-Ravid, illustrates a broadened concept of privacy in cyber spheres. The theory asserts that there is a sphere of privacy on the internet and on social media platforms that provides protection of data on users.[114] The scope of the balloon changes depending on the social interaction.[115] When thinking in terms of different social settings, individuals feel different levels of comfort when sharing information.[116] For example, generally speaking, one feels more comfortable sharing information in private than one would in a workplace or in public. Therefore, the question that arises is whether it is considered an intrusion of privacy when an employer follows an employee's social media accounts and not only scrutinizes but holds them accountable for actions that were not committed within a workplace environment. [117] When justified from a public perspective, the Balloon Theory suggests minimizing the balloon of privacy even though it is always there. Therefore, public figures, as role models that the public follow, have limited protection of their privacy.[118]

Nevertheless, from the Fourth Amendment's cases discussed above, we conclude that according to the theory, the problem remains for private personal photos of peoples' faces, which are in many cases open to the public. As a result, relying solely on an expectation of privacy may leave society with considerable uncertainty.

---

112. Shlomit Yanisky-Ravid, *To Read or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory*, 64 AM. U. L. REV. 53, 85 (2014).

113. *See id.*

114. *See id.* at 83–84 (discussing privacy spheres that exist even when employees upload personal data to social media, which might be used against them by employers).

115. *See id.*

116. *See id.* at 84.

117. *See id.* at 59.

118. *See* Shlomit Yanisky-Ravid & Ben Zion Lahav, *Public Interest vs. Private Lives—Affording Public Figures Privacy in the Digital Era: The Three Principle Filtering Model*, 19:4 U. PA. J. CONST. L. 975 (2017), available at: https://scholarship.law.upenn.edu/jcl/vol19/iss4/4 (the article suggests a Three Principle Filtering Model, to be used in determining whether or not the rationale for publishing information about public figures, in the digital era, is legitimate and hence should be allowed or prohibited: (1) the relevancy of the private information to the public and (2) whether access to the information is necessary for imparting knowledge, and then the application of (3) a proportionality rule).

i. FRT Historical (Past) Surveillance and the Fourth Amendment

Modern technology has pushed this *Katz* test to its limits, with courts often struggling to apply it in the 3A Era.[119] Due to the invasive nature of surveillance technology in the current 3A Era, as mentioned, courts have separated the question into two categories, historical and real-time surveillance. We address the historical aspect first.

The Supreme Court addressed the question of historical data in the digital era in *Carpenter v. United States*.[120] In *Carpenter*, the FBI sought the "cell-site location information" (CSLI) of a suspect without a warrant. Based on CSLI, the FBI was able to track where the suspect had been at any moment over a span of 127 days.[121] Relying on *Katz*, the Court held narrowly that CSLI data could not be obtained without a warrant, provided that (1) no exigent circumstances exist, and (2) that the date range of data does not extend longer than six days.[122]

This holding was heavily based on a theory called the third-party doctrine. Before the landmark decision in *Carpenter*, the Court had traditionally held that information that has been voluntarily disclosed to a third party loses its privacy protection.[123] In *United States v. Miller*, the Court held that there was no privacy interest in bank statements that are routinely shared with the bank and its employees in the ordinary course of business.[124] Similarly, in *Carpenter*, the Court took up the question of whether CSLI data, which is routinely shared with one's cell provider in the ordinary course of business, falls under third-party doctrine, and loses its Fourth Amendment protection. The Court declined to extend the third-party doctrine to CSLI data because, based on the "nature of the particular documents sought," the level of intrusiveness of CSLI is unprecedented in third-party doctrine's progeny.[125] FRTs, much like CSLI, would provide law enforcement the ability to conduct detailed and extended surveillance with minimal human labor, to an extent not seen before.[126]

Analogously, FRT creates many of the same risks as posed to the Court in *Carpenter*, as did CSLI data. In addition, much like how CSLI data is shared with a third party, individuals often share their face prints with social media and technology companies, and individuals constantly share their faces with the

119. *See* Yanisky-Ravid & Liu, *supra* note 5.

120. *See* Carpenter v. United States, 138 S. Ct. at 2206 (2018).

121. *See id.* at 2208–09.

122. *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, ABA (2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

123. *See* United States v. Miller, 425 U.S. 435, 442 (1976).

124. *See id.*

125. *See Carpenter*, 138 S. Ct. at 2219.

126. Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS (April 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

public. If the holding in *Carpenter* applies to facial recognition, any limited, short-term use would not be protected under the Fourth Amendment.

However, applying the two-step test in *Carpenter* to FRT may justify the use of FRT when there is an emergency (probability of conducting a crime or terror act) and when relying on a photo for a short time prior to its use.

The Supreme Court, however, declined to address whether short-term or even real-time use of CSLI data would implicate the Fourth Amendment.[127] Real-time use of FRT, of course, could reveal to law enforcement many intimate details of a person's life and may be found to constitute a search under the Fourth Amendment.

ii. FRT and Real-Time (Non-Stop) Surveillance

The Supreme Court took up the question of real-time surveillance in *United States v. Jones*.[128] In that case, law enforcement installed a GPS tracking device on a suspect's car without a warrant. Justice Scalia delivered the majority opinion of the Court, holding that the government's installation of a GPS tracker on the defendant's car without a warrant violated his Fourth Amendment rights under trespass to property.[129] Concurrences by Justice Sotomayor and Alito however, highlighted that this case should have been decided using the expectation of privacy test under *Katz* rather than the traditional property approach to the Fourth Amendment.[130] The Justices argued that *Katz* "*added to*, not *substituted for*, the common-law trespassory test."[131]

The criticism of the *Katz* test is completely subjective and vague which in turn allows for immense judicial discretion as well as uncertainty.

The privacy interests implicated with real-time surveillance do not comport with classical third-party doctrine because the information revealed is *not* the information that was provided to the third party. Unlike bank statements, for which the only information provided is transactional, the information conveyed in CSLI data is more substantial. It is a person's precise location at any given time, which can be exploited to learn who they associate with, what their habits are, who they communicate with, and a plethora of other information.

Additionally, it is important to mention that the use of tracking devices is very much similar to gathering information without explicit consent. Recently, Senate Bill No. 6793–A, passed by the New York Senate, "require[s] members of the metropolitan transportation authority police force to wear body cameras."[132] This bill demands that certain bodies of law enforcement record visually and auditorily at all times. Once the body cameras are activated, everything that is recorded is effectively collected and stored by authorities.

127. *See Carpenter*, 138 S. Ct. at 2220.

128. *See* United States v. Jones, 565 U.S. 400 (2012).

129. *See id.* at 404.

130. *See id.* at 414 (Sotomayor, J., concurring); *see also id.* at 427 (Alito, J., concurring).

131. *Id.* at 409.

132. S. 6793–A, 2019-2020 Reg. Sess. (N.Y. 2019).

This can lead to the complete misuse of private information by means of facial recognition seeing as images of private individuals that were obtained without consent could be utilized through FRT.

Images and recordings do not allow for clear and precise information at all times, they do however build an eerily similar picture to a person's daily habits, associations, and even emotions. FRT shares more than just a face, it contains information that conveys names, locations, profiles, race, and history; the entirety of the information conveyed with modern digital surveillance techniques implicates greater privacy concerns than the traditional third-party doctrine cases. Therefore, the doctrine is not fully equipped to deal with real-time surveillance in the digital era.

iii. Sense-Enhancing Technological Surveillance: Courts Struggled to Fit Cutting Edge Technologies into Existing Rules

We allege that despite a long progeny of cases defining the bounds of privacy, the Court has always struggled to fit cutting-edge technologies into existing legal rules. The case of *Kyllo v. United States* may reflect this challenge.[133] There, the police used thermal imaging technology to determine that the defendant was growing marijuana.[134] The Court held that the use of sense-enhancing technology, such as thermal imaging, was a violation of the Fourth Amendment on two grounds: first, officers used the sense-enhancing technology to obtain information that would not otherwise have been available; second, the technology itself was not generally available to the public.[135]

Applying each of these reasons to FRT suggests that such use may not be considered a violation of the Fourth Amendment. First, the data being collected is information that is freely available to the public, such as a digital face print of a person's biological features, especially when uploaded to cyber spheres or given to third parties. Additionally, the information could be obtained in alternative ways. However, similar to the rationale in *Carpenter*, the technology seems to go further than what one could reasonably learn without the technology—it enables law enforcement to track one's locations and thus can learn one's activities, associations, religious beliefs, relationships, etc., and so law enforcement may be obtaining information that would not have otherwise been (easily) available. Applying the second ground of *Kyllo*, that thermal imaging is not generally available to the public, facial recognition is more common in modern society.[136] Most consumers have facial recognition software installed on their phones, laptops, and other devices.[137] Nevertheless, FRT is not just the software, but also includes databases and cameras. Law

133. Kyllo v. United States, 533 U.S. 27 (2001).

134. *See id.*

135. *See id.* at 34.

136. *See* Kwame Opam, *Apple Takes on Google Photos with New Photos Update*, THE VERGE (June 13, 2016, 2:16 PM**),** http://www.theverge.com/2016/6/13/11922626/apple-photos-update-announced-new-features-wwdc-01 [https://perma.cc/M9GJ-H7H3].

137. *See id.*

enforcement's FRT includes large databases of face prints with names and information; those databases are not generally available to the public.[138]

iv. Probable Cause for an Arrest

Critical to the protections of the Fourth Amendment is the requirement that police action, whether that is an arrest, search, investigation, or stop-and-frisk, be subject to proper checks and balances. Facial recognition, however, offers law enforcement a new means to circumvent such requirements, and thus regulators must be particularly skeptical of the abuse of such technologies. The following subchapters address some of these challenges.

(1) Inaccuracy

First, facial recognition creates "probabilistic findings."[139] Currently, such technologies cannot determine with certainty that the result is 100% correct. They may only do so with a percentage of confidence within a margin of error.[140] Unfortunately, if equipped with the ability to use facial recognition software to establish probable cause to constitute police action, law enforcement may be incentivized to use software with lower thresholds of accuracy. For example, software with 80% accuracy would provide the officer authority to exercise action over more individuals than would software with 99% accuracy.[141] If facial recognition were to be allowed as evidence to establish probable cause, then regulators must establish a strict approach that only allows the implementation of systems that have proven consistency and high, immutable confidence thresholds. The technology is rapidly and significantly improving in many senses to recognize photos from shades and different angles, and with faces being covered with masks.[142] Moreover, the results can be tested before law enforcement starts using this technology. Advanced FRT returned a correct match in 99.8% of searches in a test conducted by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) while testing over 100 facial-recognition results.[143] Furthermore, when we compare the level of recognition of FRT with humans, FRT outperforms by far human recognition performance.[144] Therefore, FRT tools should improve human

138 *See* Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, ELEC. FRONTIER FOUND. (Feb. 12, 2018), https://www.eff.org/wp/law-enforcement-use-face-recognition.

139. *See* GARVIE ET AL., *supra* note 3, at 9.

140. *See id.*

141. *See* PROJECT ON GOV'T OVERSIGHT, *supra* note 37, at 28.

142. *See Facial Recognition Identifies People Wearing Masks*, BBC (Jan. 7, 2021), https://www.bbc.com/news/technology-55573802.

143. *See* Patrick Grother et al., *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

144. *See* P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, 115 (24) PROC. OF THE NAT'L ACAD. OF SCI. OF THE U.S. OF AM. 6171, 6173 (2018), https://www.pnas.org/content/115/24/6171; *Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy Before the H. Comm. On Oversight & Reform*, 116th Cong. (2020) (testimony of Dr. Charles H. Romine, Dir.

inefficiency. For example, the fault rate of eye witnessing in identifying suspects in a witness row is above 60% error, a percentage that FRT can improve in terms of accuracy.[145]

Nevertheless, we still miss standards and tests to measure the accuracy and certify the efficiency, especially when law enforcement uses this tool against humans in a way that may violate human rights.[146] Establishing a test of performance as a mandatory prior phase before authorized use is crucial because the result of a false positive would be a severe violation of human and civil rights, which would inevitably cause false detentions, false arrests, and violations of peoples' privacy.

(2) Racial Bias in Facial Recognition

Aside from the privacy issues, further complicating the matter is facial recognition's inconsistency across different races and genders. Facial recognition is significantly less accurate at identifying females and people of color than it is for white males. MIT found that systems with success rates as high as 99% for white males had success rates as low as 65% for women with dark skin.[147] Similarly, the American Civil Liberties Union (ACLU) found comparable error rates for women and people of color.[148] If FRT is often used by law enforcement, especially in an era where police officers may be able to use body-worn cameras to establish probable cause, it is vital that legislatures consider the inherent drawbacks of such technology as it relates to those most at risk in the justice system today.

As previously mentioned, many different types of software prove to have a racial bias which can potentially lead to disastrous effects. One possible explanation for this bias is how the technology is trained, and who is in charge of training the software in the process of identification.[149] This problem was

---

Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce), https://www.nist.gov/speech-testimony/facial-recognition-technology-part-iii-ensuring-commercial-transparency-accuracy.

145. *See* P. Jonathon Phillips & Alice J. O'Toole, *Comparison of Human and Computer Performance Across Face Recognition Experiments*, 32 IMAGE AND VISION COMPUTING 74, 81 (2014).

146. *See* Shlomit Yanisky-Ravid & Sean K. Hallisey, *"Equality and Privacy by Design": A New Model of Artificial Intelligence Data Transparency Via Auditing, Certification, and Safe Harbor Regimes*, 46 FORDHAM URB. L.J. 428, 448 (2019) (focusing on the data and suggesting a certification procedural).

147. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1, 9 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

148. *See* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (Jul. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

149. *See* Johana Bhuiyan, *Facial Recognition May Help Find Capitol Rioters—But It Could Harm Many Others, Experts Say*, L.A. TIMES (Feb. 4, 2021, 6:00 AM), https://www.latimes.com/business/technology/story/2021-02-04/facial-recognition-surveillance-capitol-riot-black-and-brown-

further addressed in a study done by the AI Now Institute of New York University, explaining how AI can be shaped by the environment upon which it is built.[150] This refers to the lack of diversity not only within social media photos and in the public opinion in general, but also within companies that tend to promote a system predominantly led by white males.[151]

Accuracy and non-biased performance of FRT are interrelated. We allege that improving the accuracy of FRT and relying on a representative dataset will improve the biases and that this improvement must be tested and affirmed periodically before law enforcement starts using FRT.

v. FRT May "Skip" the Fourth Amendment by Supreme Court Cases

Although in *Katz*, the Court granted Fourth Amendment protection against unreasonable searches and seizures beyond property and body searches, the extension was only granted to public places in which an individual had a reasonable expectation of privacy. One can argue that FRT is not protected by the Fourth Amendment, or its extension under *Katz*, for several reasons. First, as opposed to *Katz*, when one walks in the street or enters a store, there is no proverbial phone booth door to close. By entering these public places, each individual is making the proactive choice to forgo their privacy, and in effect, their Fourth Amendment protections. The next question to address is whether the third-party doctrine applies to FRTs, in which any expectation of privacy is given up when an individual gives up information to a third party. In other words, it can be argued that Fourth Amendment protections are foregone when an individual uploads his or her picture to social media.

Our conclusion is that the Fourth Amendment may not protect against the threat of violating people's privacy by FRT. The constitutional analysis cannot be complete without addressing the First Amendment.

IV. FIRST AMENDMENT CONSIDERATIONS AND FRT

A. The Right to Assembly

The First Amendment to the United States Constitution protects the right to freedom of expression from government interference.[152] As such, in general, individuals cannot be held liable for anything written or spoken as long as it is truthful or based on an honest opinion. In determining whether something is in fact "truthful," Justice Holmes famously wrote in *Abrams v. United States* that

communities#:~:text=More%20than%20600%20law%20enforcement,who%20participated%20in%20the%20riot.

150. *See* SARAH MYERS WEST ET AL., DISCRIMINATING SYSTEMS: GENDER, RACE AND POWER IN AI (AI Now Institute, 2019), https://ainowinstitute.org/discriminatingsystems.pdf (explaining how the diversity crisis in the field of AI disadvantages minorities).

151. *See id.* at 12–15.

152 U.S. CONST. amend. I.

"the best test of truth is the power of the thought to get itself accepted in the competition of the market, and . . . truth is the only ground upon which [people's] wishes safely can be carried out."[153]

The right to assemble allows people to gather for lawful and peaceful purposes. As opposed to freedom of speech, freedom of assembly cannot be conducted alone. Additionally, assembly is often premeditated and therefore the protections are extended to the preparatory activities leading up to the actual assembly.

The right to assembly and one's freedom to associate and freely express her view protects a democracy's ability to advocate for minority positions.[154] While the use of photography during a public demonstration has generally been held as not violating any First Amendment protections,[155] facial recognition for the use of targeted surveillance crosses a line and violates an individual's First Amendment protections.[156] Without comprehensive regulatory oversight of the use of FRTs during public demonstrations, speech suffers a chilling effect, potentially leading to self-censorship and diminished participation in the political process.[157] Unfortunately, there have been targeted use of FRT for the purpose of silencing public speech in the United States. As recently as 2015, the Baltimore Police Department used social media monitoring service Geofeedia in conjunction with FRT to "identify and arrest people with outstanding warrants during the unrest in Baltimore."[158]

According to the Baltimore Sun, at least five police departments paid Geofeedia to monitor citizens' social media posts.[159]

The ACLU announced in an investigation that three social media companies — Facebook, Instagram, and Twitter — in some cases, blocked access of companies they collaborated with to the media platforms in order to avoid FRT uses.[160] As such, it is apparent that not only does facial recognition provide the possibility of police abuse, but such misuse exists already. Inaction

---

153. Abrams v. United States, 250 U.S. 616, 630 (1919). *But see* Yanisky-Ravid & Lahav, *supra* note 118, at 994 (an overview of the journalist exemption).

154. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 64 (1960).

155. *See* Laird v. Tatum, 408 U.S. 1 (1972); Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337-38 (3d Cir. 1974); Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972).

156. *See* Hassan v. City of New York, 804 F.3d 277, 292 (2d Cir. 2015).

157. *See* GARVIE ET AL., *supra* note 3, at 43.

158. Kevin Rector & Alison Knezevich, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest*, THE BALTIMORE SUN (Oct. 11, 2016. 7:46 PM), https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.

159. *Id.*

160. *See* Sam Levin, *ACLU Finds Social Media Sites Gave Data to Company Tracking Black Protesters*, GUARDIAN (Oct. 11, 2016), https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter.

on the part of Congress will have (and already is having) a chilling effect on free speech, and one that particularly affects targeted minorities.

Although the use of facial recognition software during the Capitol riots was generally accepted as appropriate, there has been criticism due to the implications of FRT use upon minorities.[161]

Even though claims have been made that FRT software is increasingly precise in identification, this capability should be regulated or self-regulated with a certified test before being authorized to use in order to lead to a safer society as intended, rather than to a more dangerous one.[162] Generally, after attacks that occur within America, the repercussions are mainly felt by minorities, as proven by blanket surveillance in predominantly Black and Muslim neighborhoods following 9/11.[163] One of the many repercussions the recent Capitol riot created was a demand in passing acts regarding domestic terrorism that will ultimately affect minorities, and as previously mentioned these acts will specifically affect people of color.[164] These examples show the potentially deleterious effects of FRT used by the government.

B. Anonymity and the Speech Clause under the First Amendment

i. The Right to Anonymity

The relationships between anonymity and the Speech Clause under the First Amendment are complicated. On the one hand, freedom, under the First Amendment, should extend to anonymous speech as long as it is truthful. However, on the other hand, there are instances in which anonymity leads to dangerous abuse and misinformation.[165]

We claim that not only does the First Amendment protect the right to free speech, but it shall also protect the right to *anonymous* speech, subject to justified exceptions and limitations. This distinction is critical in that it supports one's ability to make speech that may be critical of, for example, law enforcement, without the fear of consequence that they might exercise an

---

161. KRISTIN FINKLEA & KELSEY Y. SANTAMARIA, CONGRESSIONAL RESEARCH SERVICE, U.S. CAPITOL ATTACK AND LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY (2001).

162. *See* Shlomit Yanisky-Ravid & Sean K. Hallisey, *"Equality and Privacy by Design": A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes*, 46 FORDHAM URB. L.J. 428, 476 (2019).

163. *See* Saher Khan & Vignesh Ramachandran, *Post-9/11 Surveillance Has Left a Generation of Muslim Americans in a Shadow of Distrust and Fear*, PBS (Sept. 16, 2021), https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear; *see also* Bhuiyan, *supra* note 149.

164. *See* Bhuiyan, *supra* note 149 (assessing the harmful implications of FRT).

165. Jason M. Shepard & Genelle Belmas, *Anonymity, Disclosure and First Amendment Balancing in the Internet Era: Developments in Libel, Copyright, and Election Speech*, 15 YALE J. L. & TECH. 92 (2012) (The Supreme Court, on the one hand, has long protected anonymity for speakers and writers under the First Amendment, however, on the other hand, the web anonymity raises a challenge for to sue anonymous speakers for libel, copyright infringement, or election speech).

outdated warrant in response. The U.S. Supreme Court in *McIntyre v. Ohio Elections Commission* stated that: "Anonymity is a shield from the tyranny of the majority."[166]

The right to anonymous speech was first recognized in *NAACP v. State of Alabama ex rel. Patterson* in 1958.[167] In 1955, the NAACP participated in the Montgomery Bus Boycott and helped Black students seek admission to the state university. In response, the state charged the association for "causing irreparable injury to the property and civil rights of the residents and citizens of the State of Alabama for which criminal prosecution and civil actions at law afford no adequate relief."[168] The state issued a subpoena for the name and addresses of the NAACP's members, which the NAACP resisted and was held in contempt. The Court held in favor of the NAACP, finding that immunity from state scrutiny of their membership list is so intricately tied to those members' interest to associate freely, that to allow its disclosure would be a constitutional violation.[169]

In *Bates v. Little Rock* (1960)[170] and *Gibson v. Florida Legislative Investigation Committee* (1963),[171] the Supreme Court ruled that the First Amendment right of association protected the anonymity of members of controversial groups.

Furthermore, in *Talley v. California* (1960),[172] *McIntyre v. Ohio Elections Commission* (1995),[173] *Buckley v. American Constitutional Law Foundation* (1999),[174] and *Watchtower Bible and Tract Society of New York v. Village of Stratton* (2002),[175] the Supreme Court protected those who engaged in personal political activity anonymously, like passing out leaflets or gathering petitions.

One can also learn about the debate on the protection of anonymity and the Speech Clause under the First Amendment from court decisions regarding compelled disclosure laws. Cases discussing the legality of compelled disclosure laws triggered Speech Clause scrutiny. In some cases, courts have invalidated these laws (and hence, protected anonymity under the First Amendment).[176]

---

166. McIntyre v. Ohio Elections Comm'n., 514 U.S. 334, 357 (1995).

167. NAACP v. State of Alabama ex rel. Patterson, 357 U.S. 449 (1958).

168. *Id.* at 452.

169. *Id.* at 466.

170 Bates v. Little Rock, 361 U.S. 516 (1960).

171 Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539 (1963).

172 Talley v. California, 362 U.S. 60 (1960).

173 McIntyre v. Ohio Elections Comm., 514 U.S. 334 (1995).

174 Buckley v. Am. Const. L. Found., 525 U.S. 182 (1999).

175 Watchtower Bible & Tract Soc'y of N.Y. v. Village of Stratton, 536 U.S. 150 (200).

176. *See* Alabama ex rel. Patterson, 357 U.S. at 460–61, 466 ("It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech."); *see also* Americans for Prosperity Foundation v. Bonta, 141 S. Ct. 2373, 2382 (2021) ("[In *Patterson*,] [w]e held that the First Amendment prohibited such compelled disclosure."); *Ohio Elections Comm'n*., 514 U.S. at 337–39.

In *Americans for Prosperity Found. v. Bonta*, for example, the disclosure law was held unconstitutional because California wasn't using the disclosed information for anything other than risking harm to donors. [177]

Nevertheless, in other cases, the Court has found disclosure requirements to be generally permissible. In *Citizens United v. Federal Election Commission*, the Court upheld campaign finance disclosure laws as valid; [178] in the same year, the Court upheld in *Doe v. Reed*, a requirement that petition signers have their contact information revealed even though it meant allowing the creation of online databases of the people backing a particular political petition (opposition to gay marriage).[179]

Despite the occasional finding that a law is unconstitutional for compelling disclosure, the more common conclusion seems to be that the Speech Clause mostly permits disclosure laws notwithstanding the privacy interests they implicate. However, this conclusion cannot guarantee the protection of people from FRT threatening the right to assembly.

ii. Anonymity and FRT in the 3A Era

Today, in the 3A Era, however, without proper regulation, a subpoena for a membership list may not be necessary anymore, as FRT has made it possible to determine such information by simply reviewing a nearby camera, and algorithmically identifying all individuals who associate with a given organization.

Recently, since the use of FRT has become accessible, law enforcement uses FRT to detect people who were involved in infringing public safety by unveiling their identity according to photos and videos that were taken at the scene during the events. In response to former President Trump's apparent defeat, on January 6, 2021, demonstrators voiced their outrage over the 2020 election results.[180] The media reported that a rally dubbed "Save America" began.[181] Media further reported that the group of rioters stormed the Capitol, an act that has not been committed since the early 1800s.[182] Once within the Capitol, the mob began to vandalize the building, all while recording, posting, and even livestreaming on various social media platforms.[183] The aftermath left

177. *See Bonta*, 141 S. Ct. at 2389.

178. Citizens United v. Fed. Election Comm'n., 558 U.S. 310, 347 (2010).

179. John Doe No. 1 v. Reed, 561 U.S. 186, 220 (2010).

180. Katherine Faulders & John Santucci, *As He Seeks to Prevent Certification of Election, Trump Plans to Attend DC Rally*, ABC NEWS (Jan. 4, 2021), https://abcnews.go.com/Politics/seeks-prevent-certification-election-trump-plans-attend-dc/story?id=75042176.

181. Dan Barry & Sheera Frenkel, *'Be There. Will Be Wild!': Trump All but Circled the Date*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2021/01/06/us/politics/capitol-mob-trump-supporters.html.

182. *Capitol Riots: Has the US Legislature Been Attacked Before?*, BBC (Jan. 7, 2021), https://www.bbc.com/news/world-us-canada-55572825; Barry & Frenkel, *supra* note 173.

183. Sara Morrison, *The Capitol Rioters Put Themselves All Over Social Media. Now They're Getting Arrested.*, VOX (Jan. 19, 2021, 6:52 PM), https://www.vox.com/recode/22218963/capitol-photos-legal-charges-fbi-police-facebook-twitter.

five people dead and dozens more injured, resulting in seemingly few immediate consequences.[184] The FBI immediately created a portal in order to upload pictures or videos exhibiting violence or destruction.[185] Over the course of the following days, law enforcement identified those that took part in the riot, and one of the many means of identification was executed by means of facial recognition technology.[186] The media confirmed that law enforcement had increased its use of the software the day following the riot.[187]

This is but one instance of history repeating itself. Such practices are not considered to be unique seeing as they date as far back as the 1950s. In the wake of the terrorist attacks on September 11, 2001, the New York Police Department recruited "mosque crawlers" to spy on the specific ethnic community and generate lists of active members, in what is now known as the NYPD surveillance program.[188] The NYPD's reasoning for this practice was captured in a 2007 NYPD Intelligence Division report called "Radicalization in the West: The Homegrown Threat," which claims a "radicalization process" so broad that it considers anyone who identifies as belonging to a specific ethnic origin to be suspicious.[189] When challenged, the court in *Hassan v. City of New York* found that pervasive use of undercover video surveillance could have a chilling effect, and may thus be unconstitutional.[190] The threat of indiscriminate use of surveillance technologies is present in the United States, and legislatures must address these concerns not only by prohibiting unconstitutional uses, following the uncertainty in this arena, but also providing a path for fair and beneficial gains to be realized.

V. THEORETICAL APPROACHES TO PRIVACY: SHOULD AND COULD WE PROTECT PRIVACY WHILE USING FRT?

A. Law and Economics Approach

A common approach to privacy law in the United States is the theory of law and economics, popularized by Judge Richard Posner. The central goal of this approach is to maximize efficiency and utility in the distribution of goods and services at the lowest cost. This utilitarian approach promises the optimization of social welfare from the consumer's perspective.

The theory of law and economics is helpful in understanding imposed limits on the right to privacy; the approach idealizes the dissemination of

184. *Id.*

185. *See* Bhuiyan, *supra* note 149.

186. *Id.*

187. *Id.*

188. Hassan v. City of New York, 804 F.3d 277, 285 (2d Cir. 2015); *see also* Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, ASSOCIATED PRESS (Feb. 23, 2012), https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.

189. *Factsheet: The NYPD Muslim Surveillance Program*, ACLU, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program.

190. *Hassan*, 804 F.3d at 292.

information and a free market of ideas to provide the lowest costs and minimized transactional friction.[191] Posner generally held the concept of a right to privacy, in certain circumstances, as an inefficiency and argues that the legal system should reduce the esteem with which they view the right.[192]

The concept attempts to push back against the "free rider" problem – the existence of individuals who use and enjoy products or services (or data) without providing any form of compensation for the creator.[193] Posner argues, however, that privacy is something individuals tend to surrender for very small gains.[194] People are likely to surrender their facial data to devices like phones, for example, for the mere benefit of unlocking the device without having to enter a personal pin or password.[195]

Furthermore, Posner states that privacy does not exist in the digital era. Once your photo appears on the internet, it cannot be deleted and can be tracked. Privacy is a right of an affluent society and, culturally speaking, it did not exist in traditional societies. Most relevant to the FRT discourse is Posner's claim that privacy allows and disseminates the existence of terror and crime when criminals and terrorists hide under the veil of privacy protection.[196] In the public sphere, the benefits are arguably much greater, with national security and personal safety being at the forefront of a properly regulated FRT.

We argue that privacy and consent shall be kept when using FRT. Nevertheless, Posner's arguments cannot be ignored while regulating FRT. Exceptions and limitations may be considered when discussing an actual threat to public safety.

In the 3A digital era, the challenge of considering privacy as inefficiency approach by Professor and Judge Richard Posner may, on the one hand, lead to the conclusion that in the digital age, privacy lost all its meaning.[197] However, on the other hand, scholars suggest different approaches, such as seeing privacy as property, meaning that we own our data,[198] or "The Fiduciary Model of Privacy."[199]

---

191. *See generally* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978).

192. *See id.*

193. *See generally* Shlomit Yanisky-Ravid, *The Hidden Though Flourishing Justification of Intellectual Property Laws: Distributive Justice, National Versus International Approaches*, 21 LEWIS & CLARK L. REV. 1, 7 (2016).

194. *See generally* Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 246 (2008).

195. *See* Opam, *supra* note 136.

196. *See generally* Posner, *supra* note 194.

197. Posner, *supra* note 194, at 393; *see also* Big Think, *Judge Richard Posner: Privacy*, YOUTUBE (Apr. 23, 2012), https://www.youtube.com/watch?v=kQu0et1jXfs ("Learn to light a candle in the darkest moments of someone's life. Be the light that helps others see; it is what gives life its deepest significance.").

198. Vera Bergelson, *It's Personal but is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 430 (2003).

199. *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. FORUM 11 (2020) (describing generally the asymmetric relationship between digital users and digital

B. The Fiduciary Approach to Privacy

"The Fiduciary Model of Privacy" by Professor Jack Balkin introduces a different model that defines the term privacy in the context of a relationship founded on loyalty and trust.[200] Balkin explains that in today's digital age, we find ourselves heavily reliant on digital businesses which creates an asymmetrical relationship between the user and the fiduciary.[201] The fiduciary, which collects users' data, not only places the user in an extremely vulnerable position but also forces the user to trust the fiduciary not to misuse private information.[202] However, the privacy problem does not only rest in the collection of data but also in the encouragement of disclosing information.[203] Balkin asserts that the growing dependency upon technology may serve us, but it does ultimately monitor us.[204]

The fiduciary model rests upon the understanding that the law acknowledges the existence of relationships where one side has power over the other.[205] The law aims to discern the exact imbalance of sides in terms of power, dependence, and knowledge that creates vulnerability and the need for trust.[206] According to Balkin, information fiduciaries have three basic kinds of duties towards their users: a duty of confidentiality, a duty of care, and a duty of loyalty in order to correctly maintain user data.[207]

We argue that under this fiduciary model of privacy as applied to FRT, the public individual is left in a vulnerable position when his or her images are being collected and cross-referenced, without guaranteeing confidentiality, a duty of care, and a duty of loyalty. For example, when one uploads an image to a social media platform, under this model, it can be argued that the user of FRT has a duty to ensure that the image won't be handed over to a party that may misuse the media against the person, but to her benefit.

---

companies, and the necessity for users to trust that corporations will not manipulate or betray the users).

200. *Id*.

201. *Id*. at 11.

202. Jack M. Balkin, *Fixing Social Media's Grand Bargain*, *in* AEGIS SERIES PAPER NO. 1814 (2018) https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf [https://perma. cc/774R-AD7D].

203. *See, e.g.*, Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://nyti.ms/3a5VCbp [https://perma.cc/7KQG-X3MB].

204. *See* LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 59–93 (2020).

205. *See* Balkin, *supra* note 199, at 13 n.10.

206. *See* Paul B. Miller, *The Identification of Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 367, 374 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) (listing factors relevant to fiduciary relationships); TAMAR FRANKEL, FIDUCIARY LAW, at xvi, 4, 6, 18, 29 (2011) (noting that asymmetries of knowledge and power characterize most fiduciary relationships).

207. Balkin, *supra* note 199, at 14 ("The duties of confidentiality and care require digital companies to keep their customers' data confidential and secure . . . . The duty of loyalty means that digital companies may not manipulate end users or betray their trust.").

In a discussion on privacy, Pamela Samuelson presents a different approach, where she argues for analyzing the right under property doctrine, reasoning that one's personal data should be intellectual property.[208] While it is reasonable to expect one to have an ownership stake in their own data, this view simplifies the requisite research and development that goes into building these technologies and instead delivers the resultant resources and compensation to the consumer as an effortless windfall.[209] This is exemplified in the GDPR's right to portability: such a demand requests that a company invest valuable time and resources into digitizing your personality, likes and dislikes, distilling them into a form processable by advertisers and social media companies alike, and then provide the package to the consumer at no cost, so that the consumer may reap the benefits somewhere else.[210] Less demanding, and more apt to consumer privacy, is the right to erasure, or the right to be forgotten. This right returns to the consumer the ability to have their data deleted but does not go as far as allowing the consumer to own and/or profit from data mined by other entities. This is a more appropriate approach in the consumer world, as it properly balances both an individual's interest in privacy, while also properly allocating the resources required to develop these technologies to the third-party entity invested in the research.

We propose that adopting the property approach to data, by Professor Samuelson and other scholars, in the realm of FRT, may result in viewing photos as biometric data. Such data should be owned by the individual and should not be taken or used by third parties without the consent of the individual, combined with other neighboring property rights. We assert that this conclusion may be in conflict, which few scholars have ignored, with the governmental duty to protect the citizens.

C. Privacy Versus Public Safety

In the public sphere, the balance sought by Professor Samuelson's IP approach is more difficult to ascertain because of the enhanced emphasis on public safety over consumers' interests. Generally speaking, governments have a duty to protect their citizens and to ensure public safety in favor of their citizens.[211] Therefore, the government may be able, under certain circumstances, to prioritize public benefit over individual interests in property,

208. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1134 (2000) (arguing that a property right would give individuals a chance to monetize their data by selling it in the marketplace).

209. *See id*.

210. Lydia F. de la Torre, *The Right to Data Portability Under EU Data Protection Law*, MEDIUM (Feb. 22, 2019), https://medium.com/golden-data/what-is-the-right-to-data-portability-under-eu-data-protection-law-8efa509fc788.

211. CONG. GLOBE, 39th Cong., 1st Sess. 1293 (1866) (It was a "self-evident" principle, declared Representative Samuel Shellabarger of Ohio, "that protection by his Government is the right of every citizen").

as exemplified by the doctrine of eminent domain.[212] On the one hand, it is in the public's interest to ensure the government uses efficient tools to prevent crime and terror, hence, ensuring public safety. However, on the other hand, the public shall have safeguards to be protected from misusing governmental power against the citizens and from violating human rights.[213]

Professor Pollack argues we should be thinking about personal data given to internet service providers and accessed by the government as amounting to a government attempt to use its eminent domain power and therefore as limited by the Takings Clause of the Fifth Amendment.[214] We assert that this interesting argument would likely not impede a government's ability to use that data for public benefit, a sort of digital-eminent domain.

VI. THE TRIPARTITE MODEL

In response to recent developments in FRT, lawmakers should adopt a regulatory model that will balance the competing interests of an individual's expectation of privacy with the state's interest in public safety from the standpoint of understanding the technology itself. This approach comports with the fiduciary approach to privacy described and analyzed above, which, in our opinion, is the best approach to regulating FRT.

Until now, scholars have proposed approaches that treat all uses of FRT equally. Such an approach is naïve because subjecting non-invasive uses of FRT, such as mere facial matching for investigative purposes, to the high scrutiny applied to mass surveillance applications will only result in stifling innovators and will degrade law enforcement's ability to develop this innovative technology, which might derogate public safety.

We contend that Congress should adopt a Tripartite Model to regulate the space with different requirements based on whether law enforcement is engaging in facial matching (least invasive), targeted facial identification, or indiscriminate facial recognition and clustering (most invasive). Distinguishing these three categories, and approaching each of them differently, will help to better balance private citizens' interest in privacy with the state's interest in public safety. Without this Tripartite approach, subjecting non-invasive uses to the regulation made for highly invasive uses will result in giving a high value to privacy, but at the same time, we would be outlawing FRT or inhibiting law enforcement's ability to provide public safety.

A. Facial Matching

As discussed *supra*, facial matching is the practice of using FRT to compare two images, with a certain confidence threshold, and returning a yes

212. *See generally* Kelo v. New London, 545 U.S. 469 (2005) (ruling that the Fifth Amendment's Takings Clause allows the government to promote economic development for the public).

213. *See* Samuelson, *supra* note 208.

214. Michael Pollack, *Taking Data*, 86 U. CHI. L. REV. 77, 100 (2019).

or no response.[215] Facial matching techniques, because of their targeted nature, are the least invasive investigative application of FRT, and for that reason are unlikely to rise to the level of an unreasonable search under the Fourth Amendment.[216] Facial matching techniques are hardly sense-enhancing and thus should not be subject to the higher scrutiny applied in *Kyllo*. Similarly, such techniques do not provide for substantially more invasive law enforcement techniques seen in *Carpenter* and thus are most analogous to the facts of *Katz*. In addition, we propose that facial matching techniques do not implicate the First Amendment concerns addressed above, and so when considering the balance being struck, we claim that it might be considered to be a legitimate tool that is less harmful to individuals' privacy as well as public privacy protection as a whole.

All uses of FRT should require some form of secondary validation by meeting standards of accuracy, non-biased functionality, and reliable representative data that was legally collected, to warrant law enforcement action. Due to its imperfect nature, FRT should never, alone, satisfy probable cause. Facial matching techniques, however, are inherently validated because the investigative process requires other evidence to narrow the list down to individual suspects. Facial matching as an investigative technique provides law enforcement with substantial benefits and only a minimal impact on privacy. Due to its relatively less invasive nature, this first part of the Tripartite Model should be legally regulated, in a less restrictive manner. Within a non-regulated arena, it is recommended that the Department of Justice publish guidance documents clearly defining the scope of facial matching and acceptable practices and policies. Congress should promulgate legislation providing safe harbors for agencies that take affirmative steps to establish they are using FRT in this very limited scope, and in return be awarded safe harbor from any litigation or disciplinary against them.[217]

B. Targeted Facial Identification

Unlike facial matching, facial identification is broader because it is the analysis of a photograph or video frame against an entire database and can identify individuals who are not suspected of having committed any crime. Additionally, it is not inherently validated by secondary evidence as is facial matching. Targeted facial identification, specifically, is the application of FRT to identify an individual suspected of crime. It is important to distinguish this from indiscriminate facial recognition, which would analyze every face print that came into screen, regardless of any suspicion of a crime or terror. Targeted facial identification, however, is substantially more informative than the mere listening device employed in *Katz*, making this category more analogous to the CSLI data obtained in *Carpenter*. However, this application of FRT is similar

215. *See infra* Part II.A.

216. PROJECT ON GOV'T OVERSIGHT, *supra* note 37, at 10.

217. Shlomit Yanisky-Ravid & Sean K. Hallisey, *"Equality and Privacy by Design": A New Model of Artificial Intelligence Data Transparency Via Auditing, Certification, and Safe Harbor Regimes*, 46 FORDHAM URB. L.J. 428, 476 (2019).

to the information a police officer tailing a subject could obtain, and thus it is likely not to be considered sense-enhancing technology as analyzed in *Kyllo*. Targeted facial identification, unlike facial matching, does likely implicate the First Amendment issues discussed above, and therefore must be substantially more restricted to protect an individual's right to privacy in relation to the state's interest in public safety.

Because targeted facial identification is not inherently validated, regulators must establish a program that incentivizes and requires secondary evidence to establish probable cause; facial recognition should never alone be sufficient for a warrant. Note, however, that as of now, there have not been many reports of FRTs being the sole basis for an arrest.[218] Further, when it released its NGI system, the FBI stated that the system would not be used as the sole basis for arrest, and it would be used for investigative purposes only.[219]

There are drawbacks to allowing state use of FRT in this way. Overall, this is a lowering of the threshold to probable cause for a warrant or arrest. Likely if FRT were not in any way making it easier to obtain a warrant or probable cause for arrest, agencies would not be investing the significant capital required to develop and acquire it. There is substantial debate on whether the current level for probable cause is already too low, and this could further the issue. However, if properly regulated, the impact on privacy using FRTs will be greatly outweighed by the substantial gains to be realized through its application.

Following our Tripartite Model, we suggest that Congress should regulate the use of targeted facial identification by promulgating a narrow safe harbor. To qualify for the safe harbor, agencies would have to establish that they are taking affirmative steps to ensure the privacy of its citizens who are not suspected of any crime. First, this would require validation with secondary evidence of the person being surveilled. Second, agencies should be required to take affirmative steps to ensure they are not recording or storing the location or activity data of any citizen not suspected of a crime. This includes deleting all video evidence that is not necessary to the investigation. This will establish that the agency is not practicing indiscriminate facial recognition, as discussed *infra*.[220] If the agency can meet these requirements, it should be protected from private action against them resulting from targeted facial recognition techniques.

There is a complicated issue resulting from the use of real-time facial recognition compatible with body-worn cameras. Critics have commented on the threat of this technique, in conjunction with lowering confidence thresholds, to allow police officers to stop and frisk an individual without probable cause

---

218. *See* Alexander J. Martin & Tom Cheshire, *Legal Questions Surround Use of Police Facial Recognition Tech*, SKY NEWS (Aug. 23, 2017, 6:27 PM), https://news.sky.com/story/legal-questions-surround-police-use-offacial-recognition-tech-11001595.

219. Jose Pagliery, *FBI Launches a Face Recognition System*, CNN TECH (Sept. 16, 2014, 4:48 PM), https://money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition/index.html.

220. *See infra* Part V.C.

for the stop.[221] This recommended model, however, prevents such action by requiring secondary validation. The major drawback here is transparency – there is always a concern about whether law enforcement will use the technology appropriately. Lawmakers should require regular audits by third parties, as well as promulgate a private cause of action for those individuals improperly stopped.

Additionally, improper use of this technology will be particularly harmful when it results in First Amendment violations, as was the case in Baltimore, discussed *supra*.[222] During public demonstrations, facial recognition software should be outright banned, as the privacy implications now substantially outweigh the minor cost of having to disable the software for short periods during political speech. Because of the seriousness of such a violation, facial identification systems on body-worn cameras should be required to record when they are disabled to affirmatively confirm that they were disabled during the required times. Data confirming that facial identification was disabled should be checked periodically by third-party audits, and internal affairs departments should be charged with enforcing consequences for violations.

C. Indiscriminate Facial Recognition and Facial Clustering

The third prong of the tripartite analysis should be reserved for indiscriminate facial recognition, identification, or clustering. Such practices employ facial recognition software without any articulated target, but rather record and store information about every subject who enters the camera's field of view. This use of FRT is most analogous to *Kyllo*, in that it provides law enforcement with a continuous, omniscient view of every individual's location and interactions. It is substantially more invasive than the facts of *Katz* and *Carpenter*. In addition, it has substantial implications on the First Amendment issues addressed above, in that it effectively nullifies any citizen's right to anonymity.

Generally speaking, Congress should enact an explicit ban on such uses, as the privacy implications of such use greatly outweigh the state's interest in public safety. There are drawbacks to such an approach, however. First, law enforcement agencies will not have a perfect record of crime – this will result in the commission of preventable crimes. Second, there are strong commercial interests in such a system, even beyond law enforcement. For instance, banks and lenders, as well as customers, can benefit greatly from the vast amounts of information gained from these systems. Such economic losses suffered are the cost of privacy.

221. Ringrose, *supra* note 91, at 62.

222. *See supra* Part IV.A.

VII. EPILOGUE

This article covers how extensively this new technology is being employed by agencies in the U.S., how the technology works, and how the current body of law regulates this technology.

The article suggests a Tripartite Model to better balance privacy and public safety based on the way the technology is built and the different types of FRT being used by law enforcement. The article addresses privacy implications stemming from the Fourth Amendment and one's expectation of privacy, the property approach to the Fourth Amendment, and privacy in the technological era post-*Carpenter*. It discusses First Amendment issues relating to the right to associate and the right to anonymity. Lastly, the article proposes that regulators should adopt a tripartite approach to analyzing and regulating FRT and practices of applying it, which will seek to incentivize the application of FRT to only useful, constitutional law enforcement practices while inhibiting dragnet-type surveillance. To do so, this article proposes that Congress develop safe harbor legislation that provides the state with protection provided they take certain affirmative steps. The courts should not recognize a reasonable expectation of privacy in the use of FRT in investigative applications, such as body-worn cameras and CCTVs, provided no dragnet surveillance is occurring.

On the one hand, FRT may blatantly violate privacy by the wide use of photos without consent and by selling FRT tools to entities for surveillance purposes, including law enforcement, without any certifying process.[223] In these cases, the AI FRT is being trained by scouring the internet, specifically on public sites such as Facebook and YouTube.[224] Simply by uploading an image, any related photo will pop up along with a location of where the photo appears.[225] However, on the other hand, although the use of FRT is a contentious subject, it is important to show the obvious benefits. Under unique circumstances, facial recognition software had an influential role in ensuring civilian safety. Countries such as Russia, and even the United States of America have implemented the use of FRT by the means of surveillance cameras in order to ensure that civilians stay in their homes.[226]

Throughout the past decade, technology has made drastic leaps in fine tuning software, as seen in FRT.[227] Results from The Face Recognition Vendor Test have shown a significant increase in matching accuracy between databases

223. *See* Hill, *supra* note 3.

224. *Id*.

225. *Id*.

226. *See* Pam Greenberg, *Facial Recognition Gaining Measured Acceptance*, NAT'L CONF. OF STATE LEGIS. (Sept. 18, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx (discussing states' use of FRT during the COVID-19 pandemic to identify those that defy quarantine rules).

227. *Id*.

and a photograph.[228] It should be noted, however, that there are obvious limitations to what this technology can do. It is crucial to recognize the risks of false positive readings in minority groups.

For these reasons, this article tries to bridge the missing dialogue between the industry and policymakers in order to promote a profound understanding of the technology and its uses. The article challenges the concept of either banning or approving while suggesting new solutions.

228. Peter Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NAT'L INST. OF STANDARDS & TECH., 8280 INTERNAL REPORT 40 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.