LUKAS ARNOLD, DHRUV BHATNAGAR, CECILIA SHEN, AND EDUARD BERSHITSKIY*

Use of Facial Recognition Technologies for Law Enforcement: A Comparative Analysis

* Lukas Arnold, MSc, LL.M, is affiliated with Columbia University, Department of Computer Science, and University of Bern, Department of Public Law. Dhruv Bhatnagar, LL.B., has been a practicing attorney in India and is currently affiliated with Columbia Law School. Eduard Bershitskiy, LL.M., has been a practicing attorney in Russia and is associated with Columbia Law School Cecilia Shen, BSc, is affiliated with Columbia University, Department of Computer Science.

ABSTRACT

We perform a comparative analysis of how law enforcement in India, Europe, and the United States uses facial recognition technology (FRT), highlighting India's regulatory gaps. The growing use of FRT by police raises concerns regarding fundamental rights, including privacy rights, freedom of expression, and due process. We critically examine the relevant legal and regulatory frameworks. After providing an overview on technical limitations of the technology and issuing technical recommendations, we discuss the legal framework in India.

We identify a regulatory vacuum that severely concerns fundamental and constitutional rights. In contrast, we note that regulatory attempts are underway or completed in the European Union and the United States. We examine the European Union's Artificial Intelligence Act and its implications for human rights. In the United States, our analysis covers federal bills and state regulations. In all examined jurisdictions, we find the current legal framework insufficient to protect the affected rights. There remains potential for the misuse of such technology by law enforcement. For each case, we issue recommendations for introducing or amending regulations to restrict, make transparent, and mandate specific requirements for law enforcement's use of facial recognition technology.

INTRODUCTION

In recent years, a particularly contentious use case of intelligent algorithms has been the development and deployment of automated facial recognition technologies (FRTs) for law enforcement and surveillance purposes. FRTs use machine learning or other techniques to identify or match faces. These techniques typically require vast troves of facial images compiled into training databases from which the software learns how to identify or match faces.

Concerns have been raised globally about the human rights implications of FRTs. These mainly concern human rights related to privacy, freedom of expression, and nondiscrimination. There is also concern in the context of the right to freedom and due process rights. The nonconsensual gathering of images that form training databases for FRTs interferes with privacy rights.[1] These databases often expose bias that may translate into uneven distribution of the algorithm's classification accuracy among different demographics.[2] This affects not only the prohibition of discrimination but also, in the context where misidentification of a non-suspect can lead to arrest, the right to freedom and procedural rights. The application of FRT impinges upon the principle of due process.

After an outline of technical arguments, we will lay down the Article's focal point—the legal framework for FRT use for law enforcement in India. We will discuss two case studies in India: the

1 Constantine Gidaris, *The Problem with Regulating Facial Recognition Technology in a Digital Culture of Visibility*, 48 CANADIAN J. COMMC'N 124, 128–29 (2023).

2 *See infra* Section I(D).

implementation of facial recognition technology in Telangana State and the National Crime Record Bureau's (NCRB) National Automated Facial Recognition System (NAFRS). We identify an ambiguity of existing legislation in respect to their applicability to FRT use for law enforcement; the lack of regulation poses severe dangers to constitutional and fundamental rights.

Having identified the lack of a regulatory framework on the use of FRT for law enforcement in India, we will engage in a cross-jurisdictional analysis of current regulatory attempts. For this, we will discuss the European Union's proposed AI Act (expected to be enacted in the near future); regulatory attempts in the United States on the federal level; and regulations on the state level in California and Texas.

I
TECHNICAL BACKGROUND AND ARGUMENTS

A. Facial Image Database and Breach Risk

A facial recognition system combines a database of reference images called a *gallery* and a facial recognition algorithm, which does the work of matching the input probe image to images in the gallery.[3] The images in this gallery might be acquired using a variety of sources.

In the case of Clearview AI, a private US company, Clearview AI sources the photos by scraping online sources like social media. This presents problems with infringing on various websites' privacy policies. Multiple companies, including Google, YouTube, and LinkedIn, have already sent cease and desist letters to Clearview AI; however, it is unclear how effective these were.[4] Two other companies, hiQ and LinkedIn, settled the case with Clearview AI. However, the final settlement of that case does not establish a binding legal precedent.[5]

---

3 Muhtahir O. Oloyede et al., *A Review on Face Recognition Systems: Recent Approaches and Challenges*, 79 MULTIMEDIA TOOLS AND APPLICATIONS 27891, 27892 (2020).

4 *Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App That Helps Law Enforcement*, CBS NEWS (Feb. 5, 2020), http://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/ [https://perma.cc/7NVQ-MH2U].

5 Jeffrey D. Neuburger, *hiQ and LinkedIn Reach Proposed Settlement in Landmark Scraping Case*, NAT'L L. REV.: NEW MEDIA & TECH. L. BLOG (Dec. 8, 2022), https://www.natlawreview.com/article/hiq-and-linkedin-reach-proposed-settlement-landmark-scraping-case [https://perma.cc/J8V4-E7EQ].

Meanwhile, and more relevant for law enforcement, government-funded facial recognition systems are often connected to a government database of facial images, for example, from criminal mugshots[6] or visa photos. These kinds of databases can be subject to strict privacy standards as facial data is a highly sensitive form of personal information.[7] As a type of physiological data, it "has the characteristics of uniqueness, forever identification, replicability, irreversibility of damage and relevance of information."[8]

Compared with other physiological data, facial data is unique. Facial data can be collected imperceptibly and used widely compared with fingerprint, palmprint, or iris data. As no close contact is needed, and face recognition technology can be widely applied, this leads to higher breach risks in our opinion. However, there is little research on the breach risks for identification of personal physiological data, especially facial data. In the tender document for India's proposed National Automated Facial Recognition System (NAFRS) (discussed in the subsequent chapter), there is no specification for a risk analysis of a database of facial data. This is especially important because facial recognition systems could run on PCs[9] or mobile devices[10] and might integrate with an unspecified number of other automated facial recognition system services. These would all serve as vectors of attack. The privacy implications and data breach risk of the facial image database can potentially be mitigated by technology such as privacy-preserving face recognition. Privacy-preserving face recognition would allow one party to provide the face image, and another party to provide the facial image database.[11] The first party would only be able to learn of the facial recognition result, with no access to the database.[12] The second party would perform the facial recognition computation but

6 *See* PATRICK J. GROTHER ET AL., *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY INTERAGENCY REPORT, 7709 (2011).

7 Meng Wang et al., *Identifying Personal Physiological Data Risks to the Internet of Everything: The Case of Facial Data Breach Risks*, 10 HUMANS. & SOC. SCIS. COMMC'NS 1, 4 (2023).

8 *Id.* at 2.

9 Prashant Modi & Sanjay Patel, *A State-of-the-Art Survey on Face Recognition Methods*, 12 INT'L J. COMPUT. VISION & IMAGE PROCESSING 1, 11 (2022).

10 Kornel Bertók K. & Attila Fazekas, *Face Recognition on Mobile Platforms*, *in* 7TH IEEE INTERNATIONAL CONFERENCE ON COGNITIVE INFOCOMMUNICATIONS 37 (2016).

11 Zekeriya Erkin et al., *Privacy-Preserving Face Recognition*, *in* PRIVACY ENHANCING TECHNOLOGIES 235 (Ian Goldberg & Mikhail J. Atallah eds., 2009).

12 *Id.* at 236.

would not have access to the input photo.[13] For facial recognition systems that need to integrate with many other systems with uncertain security, this would further protect the privacy of both the users in the database and the owner of the query image.

Lastly, most state-of-the-art facial recognition systems rely on deep learning algorithms that have their own unique weaknesses. For example, they are vulnerable to adversarial attacks[14] in ways manual facial recognition is not. This is still an active area of research, and the specifics of the vulnerabilities are still not fully understood as these deep learning algorithms are usually a black box system.[15]

Hence, our conclusion is that implementing such a system without a thorough risk assessment is irresponsible and cannot be done without putting millions of citizens at risk of irreparable harm in the form of racial or gender discrimination or political persecution.

B. Facial Image Quality Requirements

Many factors impact the accuracy of the facial recognition algorithm such as pose, occlusion, lighting, and the environment.[16] For law enforcement use cases, the photos submitted are often from surveillance footage taken in an uncontrolled environment that differs greatly from the image environment of reference images.[17] India's NAFRS tender document specifies that

> [t]he solution should provide advanced technological capabilities to be able to identify a facial image by extracting landmarks, features, contour, prominent points and then match with the database to provide quick results. It should be able to match facial images with change in facial expression, direction, angle, lighting, age, hairstyle, beard, glasses and scars, marks and tattoos.[18]

---

13 *Id.*

14 Ying Xu et al., *Adversarial Attacks on Face Recognition Systems*, *in* HANDBOOK OF DIGITAL FACE MANIPULATION AND DETECTION 139, 157 (Christian Rathgeb et al. eds., 2022).

15 Gaurav Goswami et al., *Detecting and Mitigating Adversarial Perturbations for Robust Face Recognition*, 127 INT'L J. COMPUT. VISION 719 (2019).

16 Oloyede et al., *supra* note 3.

17 *See* Qinghan Xiao & Xue-Dong Yang, *Facial Recognition in Uncontrolled Conditions for Information Security*, 2010 EURASIP J. ON ADVANCES SIGNAL PROCESSING 345743 (2010).

18 National Crime Records Bureau, *Request for Proposal to Procure National Automated Facial Recognition System (AFRS)* (2019), 5.

This specification for matching images with changes in facial expressions, directions, and other appearance modifiers is one of the main challenges in FRT.

Some systems, like Clearview AI, have better performance on different angles because they have more varied reference photos than traditional government facial databases, which have only very standard eye-level, evenly lit identification photos.[19] However, even Clearview AI had concerns regarding accuracy of surveillance footage as "[m]ost of the photos in Clearview's database are taken at eye level. Much of the material that the police upload is from surveillance cameras mounted on ceilings or high on walls."[20]

To fulfill the requirements of the tender document, there must be a variety of reference photos in the facial image database, which calls into question where these images will be sourced from.

C. Evaluation of Facial Recognition System

The benchmarking of a facial recognition system is complex and should include many different factors, including the accuracy under different use cases and the potential for bias. This would include evaluating the system under challenging cases like heterogeneous face recognition, long-distance facial recognition, age differentials, etc. Until 2023, NIST provided the Facial Recognition Vendor Test (FRVT), which publicly evaluated and published submitted facial recognition algorithms. As of August 18, 2023, the FRVT project has been split into the Face Recognition Technology Evaluation (FRTE) and Face Analysis Technology Evaluation (FATE).[21] These projects run ongoing tests where participants can submit algorithms for evaluation every four months.[22] The FRTE track includes evaluations for 1:1 accuracy (verification of identity, i.e., submitted photo matches

19 Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/3BP8-W3AS].

20 *Id.*

21 *Face Technology Evaluations – FRTE/FATE*, NIST (Dec. 14, 2016), https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate [https://perma.cc/PX8A-NNZT]; PATRICK GROTHER & MEI NGAN, FACE RECOGNITION VENDOR TEST (FRVT) (2014); PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION (2019).

22 *Id.*

database identity)[23] and 1:N accuracy (identification of submitted photo, i.e., which database identity matches the submitted photo).[24] They also release reports on demographic effects[25] and face mask effects.[26] India's NAFRS tender document specifies that "[t]he system . . . should provide identification and verification of image/video (recorded video footage of a specified period related to the scene of crime) by searching the above database in 1:1, 1:N, N:N combinations and giving results to users."[27] There is currently no benchmark for N:N accuracy (identifying multiple subjects in a photo) in the Indian context yet.[28] As noted above, another specification from India's NAFRS tender document states that the solution must be able to extract "landmarks, features, contour, prominent points and . . . match facial images with change in facial expression, direction, angle . . . ."[29]

These specifications are not specifically evaluated in the FRTE suite. A facial recognition system used for law enforcement should have a standard for benchmarking the system's performance under all use cases. The NAFRS tender document makes no mention of using third-party evaluation. There is no evaluation for specific use cases nor specific scenarios like the abovementioned "change in facial expression, direction, angle."

For transparency and proper risk assessment, FRT systems must be evaluated under the conditions in which it is used. The difference between the development environment and the usage environment is referred to as the "domain shift"; this shift arises from the differences between the images used to train and evaluate the FRT system and the actual images it gets in its various use cases.[30] Therefore, as much as

---

23 *See* PATRICK GROTHER, ET AL., FACE RECOGNITION TECHNOLOGY EVALUATION (FRTE), PART 1: VERIFICATION, NISTIR DRAFT (July 3, 2024), https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing [https://perma.cc/HE3N-BF3F].

24 *See* PATRICK GROTHER ET AL., FACE RECOGNITION TECHNOLOGY EVALUATION (FRTE), PART 2: IDENTIFICATION (Supp. 2024).

25 *See* GROTHER, *supra* note 23.

26 *See* MEI NGAN, PATRICK GROTHER & KAYEE HANAOKA, ONGOING FACE RECOGNITION VENDOR TEST (FRVT) PART 6B: FACE RECOGNITION ACCURACY WITH FACE MASKS USING POST-COVID-19 ALGORITHMS (Supp. 2022).

27 National Crime Records Bureau, *Request for Proposal to Procure National Automated Facial Recognition System (AFRS)* (2021), 2.

28 ANUSHKA JAIN, NCRB'S NATIONAL AUTOMATED FACIAL RECOGNITION SYSTEM (2024).

29 National Crime Records Bureau, *supra* note 18, at 5.

30 Daniel E. Ho et al., *Evaluating Facial Recognition Technology: A Protocol for Performance Assessment in New Domains*, 98 DENV. L. REV. 753, 760 (2021).

possible, evaluation should be one with in-domain data (e.g., surveillance footage). This data should then be made available through artifacts common in the AI space like model cards,[31] which would specify the training data used in creating the algorithm, the data used for its evaluation, and its performance on different tasks, e.g., 1:1 verification, 1:N identification, N:N identification, or identification underage differentials. However, there is a lack of labeled datasets for in-domain data like surveillance footage.[32] Publishing the original training data and the evaluation data will help promote a better understanding of the system's possible weaknesses.[33]

There is also an "institutional shift" that can cause performance differences based on a user's interpretation of the system's results.[34] For example, if users have different understandings of a "confidence score," then the decisions based on an FRT result would differ greatly. This human aspect of FRT is difficult to evaluate ahead of time. One solution is to implement A/B tests while the system is in use to further understand the actual impacts of the system on human decisions.[35]

D. Bias and Accuracy

The performance of a facial recognition algorithm is often indicated in terms of overall classification accuracy—i.e., how many of the given images are correctly matched. A single value, however, is not suitable to reflect the complexity of classification performance. In fact, accuracy is unevenly distributed among different demographic groups, leading to biased outcomes.[36] It matters what benchmark set is used to train the facial recognition algorithm, which demographics are present in it, and under what conditions the images were taken.

---

31 Margaret Mitchell et al., *Model Cards for Model Reporting*, *in* PROCEEDINGS OF THE CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 220 (2019), https://doi.org/10.1145/3287560.3287596 (last visited Dec. 31, 2024).

32 *See* George Ekladious et al., *Dual-Triplet Metric Learning for Unsupervised Domain Adaptation in Video Face Recognition*, *in* 2020 INTERNATIONAL JOINT CONFERENCE ON NEURAL NETWORKS 1 (July 19, 2020).

33 *See* Ryan Burnell et al., *Rethink Reporting of Evaluation Results in AI*, 380 SCI. 136, 136–38 (2023).

34 Ho, *supra* note 30, at 762.

35 *Id.* at 768.

36 Lukas Arnold, *How the European Union's AI Act Provides Insufficient Protection Against Police Discrimination*, U. PA. J.L. & SOC. CHANGE ONLINE (May 14, 2024), https://www.law.upenn.edu/live/news/16742-how-the-european-unions-ai-act-provides [https://perma.cc/7A3E-948G].

Furthermore, the type of classification error matters. We suggest that there can be three types of classification errors. The first is a false positive, where an image of a person is incorrectly matched to an existing image of another person.[37] The second is a false negative, where the subject is not matched to an existing image of him or herself.[38] Third, if a person to be identified is not present in the database to be matched against, this will result in non-identification, which occurs because the person is not part of a particular database. These three kinds of errors can be subject to bias.[39]

However, false positives, in the context of law enforcement, have the highest potential negative implications. A false positive can mean that an innocent person is mistaken for a suspect, which can cause serious distress and harm to the wrongly accused individual. It can result in deprivation of their liberty or even the wrongful conviction of an individual. Therefore, the false positive rates, in relation to demographic bias, should be given special attention. However, the accuracy of FRT algorithms is often not reported in terms of false positive error rate, which is the most indicative rate in terms of individual rights. Most often in reporting, either the overall classification accuracy is given or the false negative error rate, which is relevant only for law enforcement.[40] Such reporting is likely to favor a relaxed confidence that will result in higher rates of false positives or misidentifications. False positives are particularly problematic since it disregards the detrimental and serious effects that misidentification might have on an individual, and the effect that—as shown below—is much more likely to happen for racial minorities and other population segments experiencing discrimination.

Studies that consider different demographics have consistently shown that the accuracy of facial recognition algorithms is unequally distributed among different demographic groups, particularly in relation to the false positive error rate. This bias poses significant issues regarding racial discrimination. For example, the Face Recognition Vendor Test (FVRT), a standardized test for benchmarking facial recognition technologies, found in 2019 that false positive error rates

---

37 *See* T.J. Benedict, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 WASH. & LEE L. REV. 849 (2022).

38 Sara Solarova et al., *Reconsidering the Regulation of Facial Recognition in Public Spaces*, 3 AI & ETHICS 625, 629 (2023).

39 *Id.* at 631.

40 Patrick Grother et al., *Face Recognition Vendor Test (FRVT): Part 3, Demographic Effects*, U.S. DEP'T OF COM., NAT'L INST. OF STANDARDS & TECH. 5–6 (2019).

were highest among East and West African and East Asian people, with differences as much as 100 times between countries.[41] In domestic mugshot classification, similar trends were observed for Black Americans.[42] Racial bias in FRTs was also confirmed in later studies.[43]

Racial and gender biases compound in the inaccuracies of FRT. In a 2018 benchmark study, classification error rates for dark-skinned females were up to thirty-four percent higher compared to light-skinned males.[44] While these error rates are higher than the average error rates for each individual category, they accumulate for individuals inside multiple marginalized demographics, such as Black females.[45] Error rates have consistently been found to be highest for young, dark-skinned females.[46] Transgender persons face significant bias as well.[47] Therefore, those demographics that already experience intersectional discrimination within society are also those at the highest risk for accuracy bias by FRT algorithms. It is suggested by Abdullah Sham, in an article published in 2023,[48] that an unbiased performance can be achieved by adding missing races into the training set in an equal manner.

In conclusion, FRT algorithms, without appropriate counteracting measures, reinforce existing discrimination that is unacceptable in terms of human rights protections and the severe consequences misidentification may have.

---

41 *Id.* at 2.

42 Carina Wang, *Failing at Face Value: The Effect of Biased Facial Recognition Technology on Racial Discrimination in Criminal Justice*, 4 SCI. & SOC. RES. 29, 31 (2022).

43 Seyma Yucer et al., *Measuring Hidden Bias Within Face Recognition via Racial Phenotypes*, *in* IEEE/CVF WINTER CONFERENCE ON APPLICATIONS OF COMPUTER VISION 995 (2022); Surbhi Mittal et al., *Are Face Detection Models Biased?*, *in* IEEE 17TH INTERNATIONAL CONFERENCE ON AUTOMATIC FACE & GESTURE RECOGNITION (FG 2023) 1 (2023).

44 Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *in* CONFERENCE ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 77 (2018), http://gendershades.org/ [https://perma.cc/Q62M-FJL5].

45 Hachim El Khiyari & Harry Wechsler, *Face Verification Subject to Varying (Age, Ethnicity, and Gender) Demographics Using Deep Learning*, 7 J. BIOMETRICS & BIOSTATISTICS 11 (2016).

46 Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SCI. NEWS 24 (2020).

47 Morgan K. Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services*, 3 PROC. ACM ON HUM.-COMPUT. INTERACTION 1, 2 (Nov. 2019).

48 Abdullah H. Sham et al., *Ethical AI in Facial Expression Analysis: Racial Bias*, 17 SIGNAL, IMAGE & VIDEO PROCESSING 399 (2023).

E. Recommendations

FRT is a sensitive technology that can have potentially devastating consequences for an individual's rights, including their right to freedom. Only if an FRT system's characteristics are transparent is the fairness of the algorithm ensured. Namely, it should be ensured that an FRT does not expose any significant bias against particular demographic groups. Therefore, we have several proposals. First, we propose making unbiasedness a strict requirement that has consequences for training data and thresholds. Secondly, to monitor the accuracy, bias, and performance of an FRT system, we propose a list of technical details that should be made transparent for each of such systems.

1. Unbiasedness

We recommend that any FRT algorithms be strictly mandated to be unbiased toward population segments experiencing discrimination as a prerequisite for deployment by law enforcement. Facial recognition algorithms usually contain an adjustable threshold in regard to the confidence of recognition.[49] If this threshold is lowered, a higher number of false positives is expected in return for a lower number of false negatives. On the other hand, a stricter threshold would potentially increase the number of false negatives *but* yield a lower false positive rate. We argue that in the context of biased algorithms, such thresholds should be set as strictly as possible to ensure unbiased outcomes.

2. Transparency

For any system that is to be implemented with a great impact on citizens, there should be transparency in the specifics of that system in order to hold it accountable in aspects like fairness assessments and security assessments. The European Union (EU) AI Act establishes different responsibilities for providers of different AI systems based on the system's risk assessment.[50] To fully understand and responsibly use FRT, the following data should be publicly accessible for any

---

49 Willem Verheyen, *Adaptive Thresholding for Fair and Robust Biometric Authentication*, *in* PROCEEDINGS OF THE 24TH INTERNATIONAL MIDDLEWARE CONFERENCE: DEMOS, POSTERS & DOCTORAL SYMPOSIUM 7–8 (2023).

50 *See Commission 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).

government use of FRT systems: risk assessments, accuracy, and data provenance.

a. Risk Assessments

A full risk assessment of the FRT system would include analysis on privacy impacts as well as the risks of data breaches and adversarial attacks. To fully analyze the security risk, databases should provide information on specifics like what types of access controls are present on each component, as it represents who has access to each component (e.g., general use, viewing facial image database, updating facial image database, etc.).

b. Accuracy

The accuracy of a system includes evaluations of the system on all its use cases (e.g., 1:1 verification, 1:N identification, N:N identification). It also includes the system's performance under special circumstances (e.g., demographic changes, age differentials, with-mask, lighting or angle changes). When possible, these evaluations should be done by trusted third parties like the NIST FRTE.

c. Data Provenance

The origins of the facial data must be disclosed to fully grasp the system's potential shortcomings and to understand the privacy implications thoroughly. For example, if the data sources encompass social media, this could have significant privacy repercussions.

3. Human Post-Verification

Automatic identification by law enforcement carries strong risks in cases of false positives in which a non-suspect is misidentified as a suspect.[51] A misidentification can lead to wrongful deprivation of liberty, sometimes for an extended amount of time, and increases the risk of wrongful conviction. In alarming instances of facial recognition technology failures, law enforcement has wrongfully arrested at least seven persons, six of them Black individuals.[52] One of them, Porcha Woodruff, was wrongfully arrested for carjacking while eight months

51 Benedict, *supra* note 37.

52 Alyxaundria Sanford, *Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated*, INNOCENCE PROJECT (Feb. 14, 2024), https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/ [https://perma.cc/ENE2-TKVZ].

pregnant and endured a distressing experience that endangered her health and the health of her unborn child.[53] This example underscores the necessity of mitigating measures to prevent misidentification.

In addition to the two measures proposed above, human validation of an automatic identification decreases the risk of misidentification. While human validation can reduce bias, it is unlikely to eliminate it. Firstly, the initial set of identifications presented for post-verification is likely biased if the underlying algorithm is biased. Under the assumption that human identification is not perfectly accurate, and human identification is biased as well,[54] this would also lead to biased outcomes. Human post-verification alone cannot eliminate bias. However, its effectiveness as a reduction tool varies, especially since a recent study found that strategic recruitment, selection, and comprehensive training of human operators can significantly enhance the accuracy of face recognition systems in operational settings.[55]

II
INDIAN FRAMEWORK

This Section will deal with our focal point: the FRT use by Indian law enforcement and its legal context. We begin by describing two case studies: the FRT systems used by the government in Telangana and India's National Crime Record Bureau's (NCRB) call for proposals for a National Automated Facial Recognition System (NAFRS). Next, this Article will undertake an examination of the extant surveillance law architecture in India and of India's recently enacted federal data protection law, assessing their adequacy in regulating the use of FRT by law enforcement authorities. Finally, we will highlight how the unregulated use of FRT by law enforcement disproportionately curtails individuals' constitutionally guaranteed rights to privacy and speech and provide suitable recommendations.

A. FRT in Use by Telangana Government

Hyderabad, a city in Telangana, is currently one of the most surveilled cities in the world, with approximately 83.32 cameras per

53 Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. TIMES (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html [https://perma.cc/Y7EG-X445].

54 *See* Leslie R. Knuycky et al., *Line-Up Misidentifications: When Being 'Prototypically Black' Is Perceived as Criminal*, 28 APPLIED COGNITIVE PSYCHOLOGY 39 (2014).

55 *See* David White et al., *Error Rates in Users of Automatic Face Recognition Software*, 10 PLOS ONE (Oct. 14, 2015).

1,000 people.[56] Combined with this surveillance, the Panoptic Tracker shows Telangana has the second most facial recognition projects in India, with twelve projects installed and four in active use.[57] The use cases include both "Authentication of Identity" and "Security/Surveillance."[58] Some projects store facial recognition data permanently (Hyderabad Police), while some are only temporary (Telangana Police).[59]

Information requests to the governmental bodies under the Right to Information Act (2005) (RTI request) have been filed by Anushka Jain for the use of FRT in the Telangana Police[60] and the Hyderabad Police;[61] however, there has been little to no transparency in these systems. The RTI request seeks information on the tender documents, databases to be integrated, authorized people in the systems, and accuracy data of the FRT systems.[62] Telangana Police have not responded to Jain's requests, while the Hyderabad Police claims that the information "has no relationship to any public activity or interest or which would cause unwarranted invasion of privacy of the individual" and, therefore, are exempted from providing the information.[63]

One of the few entities that has provided information on their system is the Telangana State Election Commission, which used FRT in polling booths for authentication of identity. It stated that the accuracy of the system was only approximately eighty percent, with some

---

56 Paul Bischoff, *Surveillance Camera Statistics: Which City Has the Most CCTV Cameras?*, COMPARITECH (May 23, 2023), https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ [https://perma.cc/59B2-QD8Q] (last visited Dec. 31, 2024). *Cf.* AIT News Desk, *Top 10 Countries and Cities by Number of CCTV Cameras*, AITHORITY (Dec. 5, 2019), https://aithority.com/news/top-10-countries-and-cities-by-number-of-cctv-cameras/ [https://perma.cc/XM6F-7TWP].

57 *FRT Systems in Telangana*, PANOPTIC TRACKER, https://panoptic.in/telangana [https://perma.cc/8UTP-LCXE] (last visited Dec. 31, 2024).

58 *Id.*

59 *Id.*

60 Anushka Jain, *RTI to Telangana Police on Darpan FRS*, PANOPTIC TRACKER (July 30, 2020), https://panoptic.in/right-to-information/RTI-00017 [https://perma.cc/9D4Q-BQXN] (last visited Aug. 1, 2024).

61 Anushka Jain, *RTI to Hyderabad Police on Facial Recognition*, PANOPTIC TRACKER (Dec. 10, 2020), https://panoptic.in/right-to-information/RTI-00036 [https://perma.cc/L7MU-4CQV] (last visited Aug. 1, 2024).

62 *Id.*

63 *Id.*

possible factors being poor lighting conditions and poor reference identity photos.[64]

In the absence of transparency, Amnesty International's Digital Verification Corps used open-source intelligence—in this case, publicly available videos from Twitter and news sites—and discovered

> dozens of purported incidents filmed from November 2019 to July 2021 showing Hyderabad police using tablets to photograph civilians in the streets, while refusing to explain why. In one case, an alleged offender was subject to unexplained biometric conscription. Other cases have shown the random solicitation of both facial and fingerprint reads from civilians.[65]

The Internet Freedom Foundation has sent legal notice that remains unanswered.[66]

Amnesty International's "Ban the Scan" campaign emphasizes the concerns of the lack of transparency for the technical, legal, and enforcement aspects of these facial recognition systems and calls for "Indian law enforcement agencies to halt the procurement and use of facial recognition technologies."[67]

B. Request for Proposals for AFRS

The NCRB issued a "request for proposal" ("RFP"), i.e., a tender document, inviting bids for the creation of a National Automated Facial Recognition System ("NAFRS") in 2019.[68] On June 22, 2020, the NCRB recalled and canceled the original RFP issued on July 3, 2019.[69]

---

64 Anushka Jain, *RTIs to Telangana State Election Commission & Telangana State Technology Service on the Real Time Digital Authentication of Identity (RTDAI)*, PANOPTIC TRACKER (Jan. 24, 2020), https://panoptic.in/right-to-information/RTI-00025 [https://perma.cc/8KB7-NPCF].

65 *Hyderabad*, AMNESTY INTERNATIONAL, https://banthescan.amnesty.org/hyderabad/ [https://perma.cc/BP3B-LMVB] (last visited Dec. 31, 2024).

66 Tanmay Singh, *Hyderabad Police Force People to Remove Their Masks Before Photographing Them. We Sent a Legal Notice. #SaveOurPrivacy*, INTERNET FREEDOM FOUND. (2021), https://internetfreedom.in/hyderabad-police-force-people-to-remove-their-masks-before-photographing-them-we-sent-a-legal-notice-saveourprivacy/ [https://perma.cc/9CKC-2WBV] (last visited Dec. 31, 2024).

67 *Hyderabad*, *supra* note 65.

68 Anushka Jain, *IFF's Legal Notice to the NCRB on the Revised RFP for the National Automated Facial Recognition System #ProjectPanoptic*, INTERNET FREEDOM FOUND. (July 15, 2020), https://internetfreedom.in/iffs-legal-notice-to-the-ncrb-on-the-revised-rfp-for-the-national-automated-facial-recognition-system/ [https://perma.cc/H4SA-26JF].

69 Anushka Jain, *NCRB's National Automated Facial Recognition System*, PANOPTIC TRACKER, https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system [https://perma.cc/PW5Q-UWFN] (last visited Dec. 31, 2024).

A revised RFP was issued in its place. Some key functions that it calls for include:

> 1. [A] searchable image database of missing persons, unidentified found persons, unidentified dead bodies and criminals based around dynamic Police databases . . . .
> 2. Matching of still image of suspect against the recorded video footage of a specified period related to scene of crime and picking up the instances [the suspect appears].
> 3. The system will . . . provide identification and verification of . . . recorded video footage of a specified period related to scene of crime by searching the above database in 1:1, 1:N, N:N combinations and giving results to users.
> 4. The system should comply with Indian e-governance standards available on egovstandards.gov.in for facial attributes. . .
>
> . . . .
>
> 8. The system shall provide matching functions on images/ visuals of modified facial features like, plastic surgery, aged images, bearded faces, makeup, expression, hairstyle, glasses, scar marks, tattoos, face masks etc.
>
> . . . .
>
> 12. The vendor would be required to integrate the proposed system with existing AFRS systems (established by some advanced states already), [Crime and Criminal Tracking Network & Systems (CCTNS), Interoperable Criminal Justice System (ICJS), National Automate Fingerprint Identification System (NAFIS), and Talash Information System.][70]

The original RFP included CCTV integration as a requirement.[71] One of the most significant changes to the revised RFP is that it now states that the project "does not involve the installation of CCTV cameras nor will it connect to any existing CCTV camera anywhere."[72] This change affects many of the other requirements. For example, the revised RFP repeatedly states that FRT can be used on crime scene

---

70 *See* National Crime Records Bureau, *Request for Proposal to Procure Automated Facial Recognition System (AFRS)* (2021), https://drive.google.com/file/d/1KGrf8WwrxHXXCIhPQ3hwKLnSCifzjZRN/view [https://perma.cc/VWA6-LHTF].

71 Jain, *supra* note 69.

72 Soumyarendra Barik, *India Plans Facial Recognition Tool to Detect Faces with Masks, Sparking Privacy Concerns*, ENTRACKR (Sept. 28, 2021), https://entrackr.com/2021/09/india-plans-facial-recognition-tool-to-detect-faces-with-masks-sparking-privacy-concerns/ [https://perma.cc/UA8F-G682].

video footage.[73] If there were no integration with CCTV, this footage would likely need to be manually uploaded to the system rather than automatically captured.

The RFP also states that "[t]he system should comply with . . . standards available on egovstandards.gov.in for facial attributes."[74] However, the Face Image Data Standard states that the "[s]pecifications of Digital Face Image & Face Photograph Specifications [are] intended only for human visual inspection and verification."[75] While some of these specifications were formulated with the possibility of FRT in mind, these specifications were written in 2010 and have not been updated to take into account the proliferation of FRT, the limitations of FRT systems, and the developments in machine learning used by FRT.

There is also a lack of transparency in what integrations the FRT system will be required to have. The revised RFP requires that data is sourced from "dynamic Police databases,"[76] while the original RFP specified a list of data sources.[77] As stated by the Panoptic Project, "The lack of definitional clarity and broad scope surrounding this term sets up the AFRS for function creep and an open-ended data sharing/mining endeavor, which is untenable in law."[78] Additionally, the system is required to integrate with "existing AFRS systems" while not specifying any limitations on the types of AFRS systems.[79] This creates a possibility that the FRT system may integrate with private AFRS systems. This could have major security and data-sharing implications as it would open new vectors of attack.

---

73 *See, e.g., Request for Proposal to Procure Automated Facial Recognition System (AFRS)*, *supra* note 70, at 2.

74 *Id.*

75 *Face Image Data Standard for E-Governance Applications in India*, GOV'T OF INDIA DEP'T INFO. TECH. MINISTRY COMMC'NS INFO. TECH. (Nov. 2010), https://egovstandards.gov.in/sites/default/files/2021-07/Face%20Image%20Data%20Standards%20Ver1.0.pdf [https://perma.cc/S928-CEPK].

76 *Request for Proposal to Procure Automated Facial Recognition System (AFRS)*, *supra* note 70, at 2.

77 National Crime Records Bureau, *Request for Proposal to Procure National Automated Facial Recognition System (AFRS)* (2019).

78 Jain, *supra* note 69.

79 *Request for Proposal to Procure Automated Facial Recognition System (AFRS)*, *supra* note 70, at 3.

C. Legal Basis for the Deployment of FRT by Law Enforcement

While India has established laws governing state surveillance through the Information Technology Act of 2000 (IT Act) and the Telecommunications Act of 2023 (Telecom Act), neither of these statutes neatly addresses the use of FRT. Government interception of messages transmitted over telecommunication networks or services is permitted by the Telecom Act, while government access to information collected in computer records is permitted under the IT Act. The tenability of these laws as a legal basis for the deployment of FRT systems by law enforcement authorities is evaluated below.

1. Does the IT Act Constitute a Legal Basis for FRT?

The IT Act was enacted to facilitate economic growth by giving legal recognition to electronic transactions and e-commerce.[80] It created a legal framework to regulate India's digital ecosystem, cybercrimes, security practices, and electronic communication.[81] The IT Act also authorizes direct electronic surveillance.[82]

The State may authorize electronic surveillance if it is "necessary or expedient to do so in the interests of the sovereignty or integrity of India, the security of the state, its friendly relations with foreign Stales [sic] or public order or for preventing incitement to . . . any cognizable offence."[83] The procedure and safeguards for electronic surveillance under Section 69 are governed by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.[84] According to these rules, an order for electronic surveillance under the IT Act must be in writing,[85] contain the reasons for issuing such a direction, and specify the name and designation of the officer to whom the information is to be disclosed.[86]

---

80 Prateek Kalia et al., *Information Technology Act in India: E-Commerce Value Chain Analysis*, 5 NTUT J. INTELL. PROP. L. & MGMT. 55 (2017).

81 Information Technology Act, 2000, Statement of Objects and Reasons (India).

82 *Id.* § 69.

83 *Id.*

84 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E) (India).

85 Information Technology Act, 2000, § 69(1) (India).

86 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rules 7, 10 (India).

It is plausible that the State may, in the absence of any explicit law, rely upon Section 69 of the IT Act as a legal basis to authorize the use of FRT by law enforcement authorities. However, what is not apparent is whether facial recognition would fall within the scope of State interception, decryption, and monitoring activities, which are permitted by Section 69. This issue has not been examined by the Indian judiciary thus far. However, if the application of FRT is viewed as a separate activity beyond the scope of interception, decryption, or monitoring, it is clear that the IT Act would not explicitly allow for the implementation of facial recognition by the State.

Even if the scope of interception, decryption, or monitoring under Section 69 is considered broad enough to permit law enforcement authorities to collect information from existing CCTV feeds, no reasonable interpretative exercise could justify construing this section—or any other provision of the IT Act for that matter—as an explicit legal validation for the State to set up of FRT infrastructure, including dedicated FRT cameras.

2. Does the Telecom Act Constitute a Legal Basis for FRT?

The President of India assented to the Telecom Act on December 24, 2023, and it came into force on July 4, 2024.[87] Broadly, the Act regulates telecommunication services, networks, and the process for allocation of spectrum in India. It also repealed two archaic federal statutes governing this field, namely the Indian Telegraph Act of 1885 and the Indian Wireless Telegraphy Act of 1933.[88]

The term "telecommunication" is defined under the Telecom Act as "the transmission, emission, or reception of any message by wire, radio, optical, or other electromagnetic systems."[89] Further, "message" means any sign, signal, writing, text, image, sound, video, data stream, intelligence, or information sent through telecommunication.[90] Thus, regulated telecommunication services under the Telecom Act may include a broad array of services, including traditional telephone services as well as internet-enabled messaging, voice, and video-calling services.

87 *The Telecommunications Act 2023: Ushering in a New Era of Connectivity, Historic Shift: Replacing the Century Old Colonial Laws*, MINISTRY OF COMMC'NS (July 5, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2031057 [https://perma.cc/YB9V-NM7X].

88 Telecommunications Act, 2023, § 60(1) (India).

89 *Id.* § 2(p).

90 *Id.* § 2(g).

Section 20(2) of the Telecom Act empowers federal and state governments to order the interception or detention of messages transmitted or received over any telecommunication service or network.[91] The government's exercise of this power is subject to two substantive conditions:

(a) the occurrence of a "public emergency," or the interception is "in the interest of public safety";[92] and

(b) the interception is "necessary or expedient" in the interests of the "sovereignty and integrity of India, defence and security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any offence."[93]

An interception order under Section 20(2) of the Telecom Act should be in a writing detailing the reasons for the interception.[94] However, once a government tribunal approves an interception order, law enforcement power under the provision is broad. Any message or class of messages to or from any person or class of persons relating to any particular subject can be intercepted and disclosed to the concerned authorities.[95]

Whether the Telecom Act permits the use of FRT depends on whether the use of FRT can be considered within the scope of "interception" under Section 20(2). Notably, the scope of Section 20(2) is narrower than Section 69 of the IT Act. While Section 69 of the IT Act allows the government to intercept and monitor information in any computer resource (potentially including FRT systems), Section 20(2) permits only the interception of messages transmitted over telecommunication services or networks.[96] Given that information "monitoring" is expressly omitted from Section 20(2) of the Telecom Act, it is unlikely that the government would be able to successfully rely upon this provision as a legal basis for the deployment of FRT systems. However, even if law enforcement agencies claim legal authority to collect facial images from CCTV feeds based on Section 20(2)—much like Section 69 of the IT Act—the State certainly cannot

91 *Id.* § 20(2).

92 *Id.* § 20(1).

93 *Id.* § 20(2).

94 *Id.*

95 *Id.*

96 *Id.*; Information Technology Act, 2000, § 69 (India).

rely on this provision to legitimize the implementation of FRT infrastructure.

D. Impact of the Digital Personal Data Protection Act of 2023 on FRT Governance

Prior to the Digital Personal Data Protection Act (DPDP Act) of 2023, India had not enacted comprehensive federal legislation equivalent to the European Union's General Data Protection Regulation (GDPR) to interpret data protection cases. The DPDP Act introduced robust provisions concerning data principal notice[97] and consent obligations;[98] delineated the permissible "legitimate uses" for processing individuals' personal data without explicit consent;[99] established a grievance redressal for data principals;[100] and imposed enhanced responsibilities upon data fiduciaries when handling the data of children,[101] among other provisions. The DPDP Act is lean, and its provisions are principle-based and high-level. Details around implementation will be established through legislation in the future.[102]

The key features of the DPDP Act, relevant to the regulation of FRTs, are as follows:

(a) *Applicability*: The DPDP Act applies to personal data that is collected in digital form, or in non-digital form but digitized subsequently.[103] The term "personal data" is broadly defined under the Act to mean "any data about an individual who is identifiable by or in relation to such data."[104] Thus, facial images collected and processed by FRT systems fall within the scope of "personal data."

(b) *Processing*: The DPDP Act outlines the scope of "processing" by denoting it as a "wholly or partly automated operation or a series of operations conducted on digital personal data."[105] This definition encompasses various actions, including

97 Digital Personal Data Protection Act, 2023, § 5 (India).

98 *Id.* § 6.

99 *Id.* § 7.

100 *Id.* § 8(10).

101 *Id.* § 9.

102 Nandita Rao Narla, *5 Steps to Prepare for India's Digital Personal Data Protection Act*, INT'L ASS'N PRIVACY PROS. (Aug. 17, 2023), https://iapp.org/news/a/5-steps-to-prepare-for-indias-digital-personal-data-protection-act [https://perma.cc/86DD-XP97].

103 Digital Personal Data Protection Act, 2023, § 3(a) (India).

104 *Id.* § 2(t).

105 *Id.* § 2(x).

collection, recording, organization, structuring, storage, and adaptation of personal data.[106] It is broad enough to cover the processing of facial images by FRT systems.

(c) *Obligations of data fiduciaries*: Data fiduciaries under the Act refer to persons or entities that determine the "purpose and means of processing of personal data."[107] The Act imposes a slew of obligations upon data fiduciaries: obtaining explicit consent from data principals for consent-based processing of their personal data,[108] implementing "reasonable security practices" to safeguard personal data and prevent breaches,[109] establishing grievance redressal mechanisms for data principals,[110] and ensuring overall compliance with the provisions of the Act.[111]

The DPDP Act also creates a subcategory of data fiduciaries known as significant data fiduciaries (SDFs), which would be notified by the government based on factors such as high volume and sensitivity of personal data processed and risk to the rights of data principals.[112] SDFs are required to fulfill additional obligations under the Act, including appointing a data protection officer based in India,[113] undergoing periodic compliance audits,[114] and conducting data protection impact assessments.[115] Thus, in order to use FRTs, SDFs would be required to conduct a periodic data protection impact assessment.

The DPDP Act applies equally to both public and private organizations that handle data. Thus, law enforcement authorities, like any other state actors, must follow the Act's data protection requirements as data fiduciaries or SDFs. However, the DPDP Act also gives the federal government a blanket exemption to exempt any data fiduciary or class of data fiduciaries from any or all provisions of the Act.[116] Using this power, the government could exempt law

106 *Id.*
107 *Id.* § 2(i).
108 *Id.* § 6.
109 *Id.* § 8(5).
110 *Id.* § 8(10).
111 *Id.* § 8(4).
112 *Id.* § 10(1).
113 *Id.* § 10(2)(a).
114 *Id.* § 10(2)(b).
115 *Id.* § 10(2)(c)(i).
116 *Id.* § 17(5).

enforcement agencies from having to comply with the Act's requirements.

Further, Section 17(1)(c) also provides specific exemptions for law enforcement activities. When personal data is processed to prevent, detect, investigate, or prosecute any offense or any other contravention of any law, organizations are exempt from certain requirements.[117] These exemptions include the classification as an SDF and the obligation to conduct data protection impact assessments.[118] Although the DPDP Act creates a robust framework for personal data protection, its broad exemptions provided for state authorities make it ineffective at regulating how law enforcement authorities use FRT systems.

E. Impact of FRT Deployment for Law Enforcement on Fundamental Rights

1. Violation of the Right to Privacy and Chilling Effect on Expressive Freedoms

In recent years, nongovernmental organizations, such as the Internet Freedom Foundation, have raised concerns on the increased use of FRTs by Indian police forces, highlighting FRT's potential impact on fundamental rights guaranteed by the Indian Constitution.[119] Paramount among these concerns is the potential violation of an individual's right to privacy, read into Article 21 of the constitution by the Supreme Court of India in its landmark *Puttaswamy-I* judgment.[120] In that case, the Court unequivocally linked the right to privacy to the idea that individuals should be able to control access to and usage of their personally identifiable information:

> It was rightly expressed on behalf of the petitioners that the technology has made it possible to enter a citizen's house without knocking at his/her door and this is equally possible both by the State and non-State actors. It is an individual's choice as to who enters his house, how he lives and in what relationship. The privacy of the home

117 *Id.* § 17(1)(c).

118 *Id.*

119 *See* Disha Verma, *Why a Massive Leak in Tamil Nadu Police's FRT Database Must Herald the End of Police Use of Surveillance Technologies*, INTERNET FREEDOM FOUND. (May 17, 2024), https://internetfreedom.in/leak-in-tamil-nadu-polices-frt-database/ [https://perma.cc/DA2S-LPFK]; Anushka Jain, *From Investigation to Conviction: How Does the Police Use FRT?*, PANOPTIC TRACKER (July 2, 2021), https://panoptic.in/case-study/from-investigation-to-conviction-how-does-the-police-use-frt [https://perma.cc/4S3V-QZRW].

120 Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).

> must protect the family, marriage, procreation and sexual orientation which are all important aspects of dignity.[121]

The lack of clarity on how law enforcement authorities acquire training data for FRT systems puts individual autonomy at risk. In the broadest sense, CCTV footage, archived databases of images, and images available from personal identification documents (like drivers' licenses and passports) could be used to develop and train FRT tools. Using individuals' visual data to develop FRTs without their consent clearly violates the right to informational privacy established by the *Puttaswamy-I* judgment.[122] This practice denies individuals the ability to control how their personal data is collected and used.

Furthermore, law enforcement agencies can expand how they use FRT without oversight or procedural safeguards. This was demonstrated in 2020 when the Delhi Police, which had initially developed its FRT for tracing missing children, began using it to identify protesters in the anti-Citizenship Amendment Act protests.[123]

Law enforcement's use of FRTs also raises particular concerns about discriminatory surveillance. Vulnerable communities—including religious and ethnic minorities, political dissenters, and opposition members—often face disproportionate targeting. When law enforcement deploys FRT on a large scale, it can track people's identities, locations, and even their emotions *en masse*. This creates a more invasive form of surveillance than traditional CCTV, making people afraid to exercise their rights to free speech and public assembly.[124] To contextualize, in 2019, the Delhi and Uttar Pradesh police used automated facial recognition systems during the protests against the Citizenship Amendment Act to identify some of thousands of protesters for allegedly inciting violence during the protests.[125] In

---

121 *Id.* at 43.

122 *Id.*

123 Jay Mazoomdaar, *Delhi Police Film Protests, Run Its Images Through Facial Recognition Software to Screen Crowd*, INDIAN EXPRESS (Dec. 28, 2019), https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/ [https://perma.cc/CGX8-Q5TD].

124 Smriti Parsheera, *Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?* (Data Governance Network Working, Paper No. 05 Dec. 5, 2019), https://datagovernance.org/files/research/NIPFP_Smriti_FRT_-_Paper_5.pdf [https://perma.cc/32B5-GQTZ].

125 Sanchari Chatterjee, *Delhi, UP Police Use Facial Recognition Tech at Anti-CAA Protests, Others May Soon Catch Up*, INDIA TODAY (Feb. 18, 2020), https://www.indiatoday.in/india/story/delhi-up-police-use-facial-recognitiontech-at-anti-caa-protests-others-may-soon-catch-up-1647470-2020-02-18 [https://perma.cc/ASN7-EQ9M].

this process, the police ended up capturing the images of people engaged in a legitimate exercise of their rights to free speech and protest.[126] In the absence of a governing legal or regulatory framework, such unbridled and arbitrary exercise of surveillance measures can seriously impinge on the fundamental rights of free speech and expression, which enshrine within themselves the liberty to freely associate, organize, and protest.

Thus, as explained above, the deployment of FRTs by law enforcement authorities infringes the constitutional rights guaranteed under Article 21 (personal liberty and privacy) and Article 19 (free speech[127] and assembly[128]) of the constitution. However, these rights are not unbridled and can be reasonably restricted by the State on narrow grounds. To pass muster, any restriction on these fundamental rights must pass the test of proportionality articulated by the Supreme Court in *Puttaswamy-I*,[129] and subsequently endorsed in *Puttaswamy-II*[130] and *Anuradha Bhasin*.[131] According to this test, restrictions on fundamental rights must be (a) imposed by law (legality), (b) be a suitable means for achieving the State's legitimate aim (rational connection), and (c) necessary and balanced (necessity). We argue that the present FRT deployment by law enforcement authorities fails each of these three prongs:

(a) *Legality*: The legality prong requires that all executive action that violates individuals' fundamental rights must have the authority of law to support it and cannot rely solely on executive instructions.[132] However, as demonstrated in the preceding section of this paper, there is currently no statutory authorization that backs the legality or justifies the regulated use of FRTs by law enforcement authorities in India. Therefore, FRT is being deployed by law enforcement authorities in a legal vacuum in India.

---

126 Rakshitt C. Bajpai & Shivang Yadav, *Use of Facial Recognition Technology in India: A Function Creep Breaching Privacy*, OXFORD HUM. RTS. HUB (Jan. 11, 2021), https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/ [https://perma.cc/Y5T8-VU98].

127 INDIA CONST. art. 19, cl. 1(a).

128 INDIA CONST. art. 19, cl. 1(b).

129 Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.

130 *See* K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1.

131 Anuradha Bhasin v. Union of India & Ors., (2020) 3 SCC 637.

132 Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.

(b) *Rational connection*: The second prong of the proportionality test requires that the means used for restricting fundamental rights bear a rational nexus with the State's articulated legitimate aim. FRT is currently being deployed by Indian law enforcement agencies for a variety of vague and open-ended purposes, such as crime prevention, criminal profiling, and crime solving.[133] Even assuming these overbroad purposes can be considered legitimate, the rational connection test remains unsatisfied since FRTs are not a suitable means of achieving the State's goals of crime prevention or investigation. This is primarily due to efficacy and accuracy issues with FRT systems, in addition to the discriminatory effects they perpetuate. As demonstrated in the preceding sections, FRTs and facial analysis systems are not reliably accurate and suffer from bias, especially while dealing with women, people of color, and ethnic minorities.[134]

(c) *Necessity*: The necessity stage of the proportionality test requires that the government adopt the "least restrictive alternative"[135] that can adequately serve the legitimate state purpose, and that such a measure does not disproportionately impact the fundamental rights of citizens.[136] As stated above, the unchecked manner in which FRTs are currently being deployed by Indian law enforcement agencies results in the collection of large troves of biometric information, in utter disregard of the principles of data minimization, collection limitation, and purpose limitation, as are stipulated by EU's GDPR.[137] Such mass surveillance enabled through FRT systems can certainly not be regarded as the least restrictive

---

133 *Status of Policing in India Report 2023: Surveillance and the Question of Privacy*, COMMON CAUSE INDIA, https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf [https://perma.cc/JDF2-9TLJ] (last visited Nov. 10, 2024).

134 *See supra* Section 1(D).

135 *See* Anuradha Bhasin v. Union of India & Ors., (2020) 3 SCC 637.

136 *See* Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.

137 Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons Regarding the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

means of achieving the State's professed objectives of crime prevention.

2. Due Process Concerns

The Constitution of India establishes the idea of "procedure established by law" under Article 21 as an exception to the right to life and personal liberty afforded therein.[138] Over the years, constitutional courts have construed this phrase to encompass both procedural and substantive due process elements.[139] Consequently, a process or procedure must not only be established by law (i.e., procedural due process) but must also be just, fair, and reasonable.[140] In other words, under Article 21, no procedure or process established by law may arbitrarily deprive an individual of life or personal liberty.

The present unregulated use of FRT by law enforcement authorities in India seemingly vitiates the standard established by Article 21 from both procedural and substantive standpoints. Procedurally, the absence of any enabling statute authorizing the use of FRTs for law enforcement purposes, along with the methods and safeguards prescribed by Indian law enforcement agencies for their application are major lacunae. To add to that, a person can potentially be prosecuted based on evidence that is ungoverned or unauthorized in Indian law at the discretion of the authorities who have a clear conflict of interest in promoting the use of FRTs.

3. Violation of the Constitutional Prohibition Against Discrimination

Since the accuracy and reliability of FRT systems are largely contingent on the robustness of the data corpora used for training the underlying algorithms, there are risks of bias or discriminatory treatment being meted out to certain groups within a population.[141] Akin to other machine learning algorithms, FRTs are typically developed with the use of training datasets through which the algorithm learns to distinguish between faces.[142] If the training dataset contains a bias, such as the underrepresentation of a particular type of face, it

138 INDIA CONST. art. 21.

139 Abinav Chandrachud, *Due Process*, *in* THE OXFORD HANDBOOK OF THE INDIAN CONSTITUTION 777–93 (Sujit Choudhry, Madhav Khosla & Pratap Bhanu Mehta eds., 2017).

140 *See* Maneka Gandhi v. Union of India, 1978 SCC (1) 248.

141 *See supra* Section 1(D).

142 *See supra* Section 1(A).

would be less accurate in recognizing or categorizing that type of face.[143]

Literature on FRT in India suggests that FRTs can perpetuate existing social biases in the country related to not only skin color or gender but also to caste and religion.[144] For example, Indian researchers Marda and Narayan argue that decisions made on predictive policing systems suffer from measurement and representational biases in the data collection that tend to replicate biased policing practices; this, in turn, creates a vicious cycle where the probability of crime is indicated as higher in marginalized areas, leading to greater scrutiny and police intervention in these areas.[145]

The use of FRTs as predictive policing tools legitimizes discrimination and undermines India's obligation of nondiscrimination, enshrined under Articles 14 ("right to equality") and 15 ("prohibition of discrimination on grounds of religion, race, caste, sex or place of birth") of the constitution because of inherent bias issues.[146] Given the judicial scrutiny evident in cases like *Madhu v. Northern Railways*,[147] in which the Delhi High Court ruled against policies that are facially neutral but discriminatory in practice, predictive policing algorithms face significant challenges to their constitutional validity.

Consequently, the legal perspective of the Delhi High Court underscores the inherent risks associated with FRT systems. When such technologies serve as tools for predictive policing, they not only risk perpetuating biases but also may infringe upon India's obligations for nondiscrimination under Articles 14 and 15 of the constitution. This situation calls into question the broader application and reliability of FRTs in law enforcement, which highlights the critical need for evaluating and rectifying biases within these systems to ensure they align with constitutional guarantees of equality and nondiscrimination.

---

143 *See* Agnė Limantė, *Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out*, 42 NORDIC J. HUM. RTS. 115 (2024).

144 Karan Saini & Prem Sylvester, *India Is Falling Down the Facial Recognition Rabbit Hole*, WIRE (July 23, 2019), https://thewire.in/tech/india-is-falling-down-the-facial-recognition-rabbit-hole [https://perma.cc/YZP4-X2AU].

145 *See* Vidushi Marda & Shivangi Narayan, *Data in New Delhi's Predictive Policing System* (Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Jan. 27, 2020), https://dl.acm.org/doi/abs/10.1145/3351095.3372865 [https://perma.cc/CND4-73VF].

146 INDIA CONST. art. 14–15.

147 247 (2018) DLT 198.

F. Recommendations

1. Creation of a Legal Framework for FRT

As explained above, the use of FRTs is almost completely unregulated in India. This leaves citizens aggrieved by law enforcement's use of FRTs and compels them to engage in expensive and time-consuming litigation by approaching the constitutional courts for relief. Although courts play a vital role in protecting fundamental rights, they are not well suited or equipped to issue guidelines to regulate the varied uses of FRTs. Thus, the Indian Parliament must enact suitable legislation to fill this regulatory vacuum. Any law that enables the use of FRT must be enacted only after widespread and meaningful stakeholder consultation and incorporate the following elements.

First, any law that enables the use of FRT must be accessible, precise, and foreseeable to provide certainty about the basis for the collection of biometric data, the procedures and time limits for storage of this data, and the procedures for deletion and disclosure or use of such data by the data fiduciaries.[148] Second, the law must implement the data protection principles of data minimization, purpose, collection and storage limitation, transparency, and accountability as are enshrined in the GDPR.[149] Additionally, any large-scale deployment of FRT must be preceded by an algorithmic impact assessment and a data protection impact assessment.

Third, the law must build in the constitutional principles of necessity, proportionality, and procedural guarantees to strictly govern the use and deployment of FRT. If FRT is being deployed for law enforcement purposes, it must be accompanied by judicial oversight, and an exclusionary rule should prohibit courts from admitting evidence that is illegally obtained by law enforcement authorities.

Fourth, to ensure accuracy and address biases in FRT systems, given the risks of bias and discriminatory effects, it is essential that any deployment of FRT by law enforcement is mandated to rigorous and unbiased accuracy standards. These include mandatory, transparent scrutiny applied to FRT systems for accuracy and fairness, the creation

148 *See* Vrinda Bhandari & Renuka Sane, *A Critique of Aadhaar Framework*, 31(1) NAT'L L. SCH. INDIA REV. 72 (2019), https://repository.nls.ac.in/nlsir/vol31/iss1/4 [https://perma.cc/5DPE-53XM].

149 *See* Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons Regarding the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

of diverse and representative datasets, and the implementation of mitigating measures.

2. Transparency and Accountability

In India, a key concern surrounding the discretionary use of FRT in law enforcement has been how such actions are vaguely justified for security purposes. For instance, the NCRB's NAFRS proposal for constructing a nationwide facial recognition tool has been shrouded in secrecy; there is little to no publicly available information about how proposal decisions were decided.[150] Absent such confidence-building measures, legal academics and civil society activists have criticized the arbitrariness and haste in deploying FRT in India. It is, therefore, imperative to put all relevant details about the State's use of FRT in the public domain and for legislatures to enact laws to enforce transparency and accountability around the use of FRT.

III
REGULATORY FRAMEWORKS

In the previous section, we delved into the Indian framework with respect to law enforcement's use of FRT and identified gaps in regulation that could potentially have severe adverse effects on human rights. In this section, we look beyond India for other regulatory attempts at filling these regulatory gaps. We will examine the Artificial Intelligence Act in the European Union, as well as state and federal regulatory efforts in the United States. Our examination will focus on whether these approaches to regulation are suited to protect fundamental rights. We will also issue recommendations concerning the examined regulatory efforts.

A. European Framework

1. The EU's Artificial Intelligence Act

On August 1, 2024, the Artificial Intelligence Act (AI Act) came into force in the European Union.[151] The AI Act is a comprehensive regulatory framework on the use of artificial intelligence inside the

150 *See supra* Section II(A).

151 Press Release, Eur. Comm'n, *European Artificial Intelligence Act Comes into Force* (Aug. 1, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123 [https://perma.cc/73GK-9F2L].

EU.[152] The AI Act is the only law within the European framework directly addressing real-time biometric recognition systems (such as facial recognition systems). However, such systems have been previously addressed by a guideline of the Council of Europe, an international organization spanning a wider range of countries than the European Union. These guidelines set out by the Council of Europe set out principles of lawfulness[153] and, within the framework of the European Union, determined binding acts and directives regarding data protection, such as the GDPR[154] and the data protection law enforcement directive.[155] As discussed in our previous blog article, the AI Act is likely to set a global standard and influence legislative efforts around the world.[156]

a. Allowed Usage by Law Enforcement

The AI Act explicitly lays out the conditions on the usage, "'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement,"[157] which includes real-time facial recognition systems.[158] Generally, it prohibits its usage, except for where it is strictly necessary for one of three objectives enshrined in article 5 the Act.[159]

Objectives (i) and (ii) limit the use of FRTs to searches of victims of specific crimes and missing persons, and to cases where a concrete threat to life, physical safety, or a terrorist attack is imminent.[160] Objective (iii) allows the use of FRTs in the search of a suspect for a certain range of criminal offenses.[161] The crime has to be punishable by a maximum period of at least four years and be included in Annex II of

---

152 *Id.*

153 Eur. Consult. Ass., *Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*, Doc. No. 108 (1981).

154 2016 O.J. (L 119) 1.

155 2016 O.J. (L 119) 89.

156 Lukas Arnold, *How the European Union's AI Act Provides Insufficient Protection Against Police Discrimination*, U. PA. J.L. & SOC. CHANGE ONLINE (Mar. 14, 2024), https://www.law.upenn.edu/live/news/16742-how-the-european-unions-ai-act-provides [https://perma.cc/P9TH-FQMU]; Deborshi Barat, *The EU's AI Act and the Brussels Effect*, HINDU BUSINESS LINE (Dec. 31, 2023, 1:38 PM), https://www.thehindubusinessline.com/business-laws/the-eus-ai-act-and-the-brussels-effect/article67683158.ece [https://perma.cc/LUQ8-2MAP].

157 Artificial Intelligence Act, art. 5(1)(h).

158 *Id.* art. 3(37).

159 *Id.* art. 5(1)(h).

160 *Id.*

161 *Id.*

the Act.[162] Annex II includes high-level crimes such as human trafficking, rape, and sexual exploitation of children.[163] Furthermore, such deployment is restricted for the purpose of confirming the identity of a targeted individual;[164] this seems to prohibit the deployment for fishing expeditions, in which every person is matched against a suspect whose identity is unknown.[165] The use of the system must take into account "the seriousness, probability and scale of the harm that would be caused if the system were not used,"[166] and must be reported to the relevant surveillance authority.[167]

The AI Act requires that the consequences on rights and freedoms of affected people are taken into account when deploying a real-time biometric identification system.[168] In particular, the deployment can be carried out only if the law enforcement authority undertook an assessment on the impact on fundamental rights and has properly registered the system.[169] The latter requirement can be waived in urgent circumstances.[170] In addition, there is some form of a warrant requirement—the deployment has to be authorized after review.[171] However, judicial bodies are not the only ones who may issue such a warrant, "independent administrative authorit[ies]" may do so as well.[172] The authorization must be issued in advance, except in urgent cases, where such review can happen after the start of deployment.[173]

While the AI Act limits the scope of usage of FRTs to law enforcement, it lacks specificity; this lack of specificity, in our opinion, creates room for misuse. In the past, activists supporting refugees at Europe's borders have been charged with crimes related to human trafficking.[174] Such charges have been criticized of being politically

---

162 *Id.*

163 *Id.* at Annex II.

164 *Id.* art. 5(2).

165 The term "fishing expedition" was coined by *Hickman v. Taylor*, 329 U.S. 495, 507 (1947).

166 Artificial Intelligence Act, art. 5(2)(a).

167 *Id.* art. 5(4).

168 *Id.* art. 5(2)(b).

169 *Id.*

170 *Id.*

171 *Id.* art. 5(3).

172 *Id.*

173 *Id.*

174 Florian Schmitz, *Greece: Activists Go on Trial for Helping Migrants*, DEUTSCHE WELLE (Nov. 18, 2021), https://www.dw.com/en/greece-ngo-workers-could-face-prison

motivated to criminalize aid.[175] Human trafficking is one of the offenses where FRT can be deployed by law enforcement;[176] so, potentially, FRT can be used to persecute pro-refugee activists. While the AI Act demands the deploying law enforcement agency consider potential consequences, including consequences to the freedom of the use of FRT, and requires its use to be authorized in advance by a judicial or independent administrative body,[177] the vagueness of the provision still leaves room for misuse. An "independent administrative body" might not be so independent after all if it is staffed by a government, in our hypothetical example, that vows to be tough on pro-refugee activists. The Act does not provide appropriate safeguards against such hypothetical misuse. However, binding caselaw by the European Court of Human Rights sets restrictions on such abuse: "A high level of justification is therefore required in order for them to be considered 'necessary in a democratic society,' with the highest level of justification required for the use of live facial recognition technology."[178] While misuse could possibly be subject to judicial challenge and review, the lack of specificity in the provisions still remains an essential weakness of the AI Act.

b. Bias and Discriminatory Effect

Regarding so-called high-risk AI Systems that include FRT systems,[179] the AI Act holds multiple provisions that should minimize and mitigate AI-related risks connected to bias and discrimination.[180] However, we regard the Act's discrimination protection measures as insufficient. While the law requires developers to test examine a system

-for-helping-migrants/a-59857314 [https://perma.cc/PZ8L-5CMJ]; Weronika Strzyżyńska, *Poland Detains Activists Accused of Smuggling Migrants Over Belarus Border*, GUARDIAN (Mar. 25, 2022, 8:52 AM), https://www.theguardian.com/global-development/2022/mar/25/poland-detains-activists-accused-of-smuggling-migrants-over-belarus-border [https://perma.cc/Y9CE-V2RB].

175 Eric Reidy, *European Activists Fight Back Against 'Criminalisation' of Aid for Migrants and Refugees*, NEW HUMANITARIAN (June 20, 2019), https://www.thenewhumanitarian.org/news-feature/2019/06/20/European-activists-fight-criminalisation-aid-migrants-refugees [https://perma.cc/P5NA-K6A5].

176 Artificial Intelligence Act, Annex II.

177 *Id.* art. 5(3).

178 Glukhin v. Russia, App. No. 11519/20, ¶ 86 (July 4, 2023), https://hudoc.echr.coe.int/eng?i=001-225655 [https://perma.cc/H5N4-DYP3].

179 Artificial Intelligence Act, Annex III (1).

180 Artificial Intelligence Act, Chapter 3.

for bias[181] and undertake mitigating and correcting measures,[182] it does not oblige an algorithm to be unbiased; rather, it mandates human oversight on high-risk systems to minimize those risks.[183] This means that a biased FRT system falling into the category of a high-risk AI system may be deployed, as long as there is "appropriate and proportionate" human oversight.[184] However, the scope of human oversight with respect to high-volume automated face recognition is limited—it is our assessment that the volume an AI model produces can quickly outpace the volume a human can diligently verify. Secondly, significant human bias is present in law enforcement: human identification for law enforcement purposes (e.g., during lineups) consistently exhibits significant racial bias, which is assumed to be one of the leading causes for wrongful conviction. It is unlikely that (biased) human oversight can overcome biased automated decision making.[185] In light of the fact that FRT algorithms' bias adds to the existing bias within law enforcement, these algorithms increase the risk of civil rights violations for individuals.[186] With biased facial recognition systems, it would therefore still remain that the set of suspects turned in for human verification will contain a disproportionately high number of wrongful identifications (false positives) that are people of color, with human verification being unlikely to overturn machine bias.

c. Accountability

Authorities in Europe have misused FRT systems, leading them to restrict freedom of expression and silence dissent.[187] The AI Act imposes possible penalties in case of noncompliance, such as the illicit deployment of a facial recognition system, that can range up to thirty-five million Euros, or seven percent of the total worldwide annual

181 *Id.* art. 10(2)(f).

182 *Id.* art. 10(2)(g).

183 *Id.* art. 14(1–2).

184 *Id.* art. 14(4).

185 *See* Leslie R. Knuycky et al., *Line-Up Misidentifications: When Being 'Prototypically Black' Is Perceived as Criminal*, 28 APPLIED COGNITIVE PSYCH. 39 (2014); *See* Lukas Arnold, *How the European Union's AI Act Provides Insufficient Protection Against Police Discrimination*, U. PA. J.L. & SOC. CHANGE ONLINE (Mar. 14, 2024), https://www.law.upenn.edu/live/news/16742-how-the-european-unions-ai-act-provides [https://perma.cc/FSR9-WH8Q].

186 Arnold, *supra* note 185.

187 *See* Glukhin v. Russia, App. No. 11519/20, (July 4, 2023).

turnover.[188] In order to identify such noncompliance, transparency concerning the use and performance of AI systems such as FRTs toward affected persons is needed. While the Act generally requires transparency concerning AI use, the current requirements of the Act do explicitly exempt law enforcement agencies: "This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, unless those systems are available for the public to report a criminal offence."[189] As a consequence, it is difficult to detect and expose misuse of FRTs in use by law enforcement. In our opinion, while there is some interest by law enforcement to hold their use of FRTs absolutely confidential, privacy and human rights interests outweigh law enforcement's interest. It is hardly justifiable to withhold information from a person targeted for identification by live FRTs after sufficient time has passed (e.g., after a criminal investigation has been closed). The lack of transparency imposed on FRTs by law enforcement can easily lead to a lack of accountability, which creates ample opportunity for misuse. Another weakness of the AI Act is that, while it imposes fines in cases of noncompliance, it does not directly provide for just satisfaction in case of infringement of one's individual rights.[190] While such entitlements might arise from different regulatory instruments, concrete provisions to compensation would have created an additional safeguard against abuse of FRT.

2. Is There Sufficient Protection of Human Rights?

The current regulatory framework in Europe provides, in our opinion, insufficient protection concerning human rights. The obligation to prevent discrimination does not impose a strict requirement for FRTs to be unbiased[191], which makes it likely that using FRTs will amplify law enforcement bias and discrimination against people of color. We note that the nondiscrimination principle is firmly established in international public law, including the EU's Charter of Fundamental Rights,[192] the Council of Europe's European

188 Artificial Intelligence Act, art. 99(3).

189 *Id.* art. 50(1).

190 *Id*. at Chapter XII *e contrario*.

191 *Id. e contrario*.

192 Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1, art. 21.

Court of Human Rights (ECHR),[193] and—on a worldwide level—the Universal Declaration of Human Rights,[194] the International Covenant on Civil and Political Rights (ICCPR),[195] and the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD),[196] and thereon. We observe a conflict with the obligation carried by compelling international law to refrain from discrimination. Furthermore, the list of crimes for which FRTs might be used are vague in the AI Act, which allows room for misuse, including the unlawful restriction of not only to the right to privacy[197] but also to freedom of expression,[198] likewise firmly enshrined in international public law. Europe has misused FRTs to silence dissent,[199] and the current regulatory framework is, in our opinion, insufficient in terms of specificity and scope to prevent further misuse.

3. Recommendations

Given the previously described weaknesses, we recommend that the AI Act should be amended within itself or with another regulatory instrument, so to include the following recommendations:

(1) The European Court of Human Rights should be firmly incorporated into the regulatory framework for "the highest level of justification" in regard to the necessity of live facial recognition technology, instead of solely relying on *a posteriori* judicial oversight.

---

193 Eur. Consult. Ass'n., *European Convention for the Protection of Human Rights and Fundamental Freedoms*, art. 14, 1st Sess., Doc. No. 005 (1950).

194 G.A. Res. 3/217 (III), Universal Declaration of Human Rights art. 7, (Dec. 10, 1948).

195 G.A. Res. 2200A (XXI), International Convention on Civil and Political Rights art. 2, art. 4(1), art. 26 (Dec. 16, 1966).

196 G.A. Res. 2106 (XX), art. 1, (Dec. 21, 1965).

197 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950; 213 U.N.T.S. 221, U.N. GAOR; Universal Declaration of Human Rights, art. 12, U.N. Doc. A/RES/3/217 A (III) (Dec. 10, 1948); G.A. Res. 2200A (XXI), art. 17; U.N. GAOR, 21st Sess., Supp. No. 16, at 52; U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171; Charter of Fundamental Rights of the European Union, art. 7, Dec. 7, 2000; 2000/C 364/01.

198 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10, Nov. 4, 1950; 213 U.N.T.S. 221., U.N. GAOR; Universal Declaration of Human Rights, art. 19; U.N. Doc. A/RES/3/217 A (III) (Dec. 10, 1948); G.A. Res. 2200A (XXI), art. 19; U.N. GAOR, 21st Sess., Supp. No. 16, at 52; U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171; Charter of Fundamental Rights of the European Union, art. 11, Dec. 7, 2000, 2000/C 364/01.

199 Glukhin v. Russia, App. No. 11519/20, Eur. Ct. H.R. (2023).

(2) Strict requirements on the use of FRTs in bias should be imposed. We regard human oversight on biased systems insufficient for nondiscrimination requirements. Instead, we suggest implementing a requirement of proof that a High-Risk AI system performs without significant bias.

(3) Law enforcement exceptions for FRT transparency obligations should be eliminated or limited with mandatory post-operation disclosure.

(4) The regulations should provide that investigations into misuse of FRT by law enforcement agencies and their actors should be swift and effective on the EU and national level, and that the victims of such misuse should be entitled to just satisfaction.

(5) With reference to the technical recommendations for transparency in this Article, the details of any FRT in use by law enforcement should be made publicly available and be open to public scrutiny. Transparency provisions should also be provided so that anyone is, or can be, informed on the personal implications of FRTs (e.g., if someone's face is included in a training set, and where and when a successful or attempted negative or positive identification has been performed). Legal instruments should be accessible to anyone affected or potentially affected by FRTs to have law enforcement's use of FRTs judicially scrutinized.

Such regulatory measures can contribute to accountability and transparency.

B. U.S. Framework

While the technology at issue is extremely widespread in the United States,[200] the American framework is perhaps the most controversial

200 *See, e.g.*, Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES (Jan. 3, 2023), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html [https://perma.cc/S7JF-GU3P]; Craig McCarthy, *How NYPD's Facial Recognition Software ID'ed Subway Rice Cooker Kook*, N.Y. POST (Aug. 25, 2019, 7:51 PM), https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/ [https://perma.cc/DEH4-VYJR] (describing the arrest of a strange young man cooking rice in the subway based on the use of FRT, and quoting Chief of Detectives Dermot Shea: "To not use technology like this would be negligent. This is the future[.]"); James Clayton & Ben Derico, *Clearview AI Used Nearly 1m Times by US Police, It Tells the BBC*, B.B.C. (Mar. 27, 2023, 6:44 PM), https://www.bbc.com/news/technology-65057011 [https://perma.cc/5LCC-LHAR].

with respect to FRTs. The U.S. Supreme Court has not yet decided a single case evaluating the legality of FRT use in law enforcement, and scholars controversially discuss how precedent case law on new technology, such as *Kyllo v. United States*[201] and *Carpenter v. United States*,[202] shall be applied to the issue.[203] Lower court rulings on this issue, such as *Patel v. Facebook*[204] or *ACLU v. Clearview AI*,[205] are sporadic. Statutory regulation at the federal level is completely absent, although several bills have been proposed.[206] States have been the most successful in regulating FRTs—they regularly propose bills, introduce fairly elaborate legislation, or ban the technology altogether. The analysis in this Part goes through each of these frameworks in sequence: it begins with an examination of the Supreme Court jurisprudence, then moves on to discuss some lower court decisions; and then, more extensively, covers both federal and state laws and bills.

1. Federal Attempts

Again, there is no federal law in the US that regulates the use of FRTs for law enforcement purposes. That does not mean, however, that Congress is not concerned about the issue. Several bills—both FRT-prohibitory and FRT-regulatory—have been proposed in recent years; in this Section, we analyze two expired legislation attempts.

a. The Prohibitory Bill

Senator Edward Markey introduced the Facial Recognition and Biometric Technology Moratorium Act of 2020, which is now expired.[207] "Moratorium" here means that the bill declares it is "unlawful for any Federal agency or Federal official . . . to acquire,

---

201 Kyllo v. United States, 533 U.S. 27 (2001) [hereinafter Kyllo].

202 Carpenter v. United States, 585 U.S. 296 (2018) [hereinafter Carpenter].

203 The applicability of the Supreme Court's Fourth Amendment case law to the FRT has already been extensively explored by scholars. *See, e.g.*, Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of Carpenter v. United States*, 89 U. CIN. L. REV. 552, 568 (2021); Adriana Bass, *Smile! You're on Camera: Police Departments' Use of Facial Recognition Technology & the Fourth Amendment*, 55 LOY. L.A. L. REV. 1053, 1072 (2022).

204 Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019).

205 ACLU v. Clearview AI, Inc., No. 20CH4353, 2021 WL 4164452, at *5 (Ill. Cir. Ct. Aug. 27, 2021).

206 *See* Evan Ringel & Amanda Reid, *Regulating Facial Recognition Technology: A Taxonomy of Regulatory Schemata and First Amendment Challenges*, 28 COMM. L. & POL'Y 3 (2023).

207 S. 4084, 116th Cong. (2020).

possess, access, or use . . . (1) any biometric surveillance system; or (2) information derived from a biometric surveillance system operated by another entity."[208] A "biometric surveillance system" (BSS), in turn, is defined as "any computer software that performs facial recognition or other remote biometric recognition in real time or on a recording or photograph."[209] The draft law further identifies both FRTs[210] and "other remote biometric recognition"[211] quite broadly.

Further, no FRT use is allowed in any judicial proceedings, except for in private right actions alleging a violation of the bill.[212] The bill also introduces a cause of action for such violations[213] as well as civil penalties.[214] Additionally, "more stringent limitation[s]" at whatever statutory level are not intended to be preempted by the bill.[215] Lastly, the NIST is entitled to research and test BSS and other technologies "in commercial use."[216]

The ban, the bill's authors envision, should remain in effect unless Congress "explicitly" approves the use of FRTs[217]—indeed, not just approves, but puts a number of detailed provisions into law. These requirements include:

(1) prohibited and permitted uses (and purposes thereof), as well as the entities entitled to the use;

(2) "standards for use and management of information derived . . . including data retention, sharing, access, and audit trails";

---

208 *See id.* §§ 3(a), 3(e) (stating that no funds, including both federal and unallocated, may be used by agencies to purchase or employ any of the technologies covered by the bill).

209 *See id.* § 2(1).

210 *See id.* § 2(3) ("The term 'facial recognition' means an automated or semi-automated process that—(A) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating surveillance information about an individual based on the physical characteristics of the individual's face; or (B) logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual.").

211 *See id.* § 2(6) (Such a technology, according to the bill, is any process, other than fingerprint and palm print identification, that (i) performs the same functions as FRT under the bill's § 2(2)(A) but with respect to "the individual's gait or other immutable characteristic ascertained from a distance"; or (ii) "uses voice recognition technology"; or (iii) like in the bill's § 2(2)(B), "logs such characteristics to infer emotion, associations, activities, or the location of an individual.").

212 *See id.* § 3(c)(1).

213 *See id.* § 3(c)(2).

214 *See id.* § 3(d).

215 *See id.* § 3(f)(2).

216 *See id.* § 3(f)(1).

217 *See id.* § 3(b).

(3) "auditing requirements to ensure [technological] accuracy," including standards (both overall minimums and "accuracy rates by gender, skin color, and age");

(4) "rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity"; and

(5) compliance mechanisms.[218]

How should the proposed legislation be evaluated? On the one hand, it intends to ban FRTs, at least temporarily. Prohibited use under the bill includes not only direct employment by law enforcement but also use of the surveillance information obtained from a third-party-operated BSS, which further limits possible interactions with notorious providers such as Clearview AI.[219] The fourth requirement of the authorizing statute—concern for privacy, free speech, equal protection, and due process—shows that senators are quite aware of the legal risks associated with the use of FRTs. The third accuracy-related requirement, in turn, acknowledges technical considerations.[220] The no-preemption rule allows for greater protections by state law.[221]

Yet, the proffered ban is not permanent.[222] Also, there is no explicit provision for a warrant requirement—the requirement to obtain a warrant for the use of FRT—after the expiration of the moratorium.[223] If this omission is intentional, then even with all the safeguards, the bill misses the target. Inaccuracy in the application of FRTs, as we have shown, is far from the only problem. And, if the bill recognizes the threat to privacy, it needs to be more coherent and precise. The bill failed to pass.

b. The Regulatory Bill

The House of Representatives bill, the expired Facial Recognition Act of 2022,[224] proposes much more complex and granular regulation.

---

218 *See id.*

219 *See* Isadora N. Rezende, *Facial Recognition in Police Hands: Assessing the 'Clearview Case' from a European Perspective*, 11 NEW J. EUR. CRIM. L. 375 (2020).

220 S. 4084, 116th Cong. § 3(b)(3) (2020).

221 *See id.* § 3(f)(2).

222 *See id.* § 4.

223 *Id.*

224 H.R. 9061, 117th Cong. (2022).

First and foremost, while it does not ban the use of FRTs,[225] it does require the police to obtain a warrant for its employment.[226] Under the bill, an "investigative or law enforcement officer may only use or request facial recognition in conjunction with a reference photo database pursuant to [a court] order"[227] approving "[a]n application for a warrant to use" the database.[228] Before submission, the application must also be approved by the head of a law enforcement agency.[229]

The application is subject to very rigorous requirements, similar to the Wiretap Act.[230] In addition to identifying the applicants involved, both the requesting officer and approving officer must indicate and describe the person to be identified by their photo or video. These are formal requirements. The application must also contain (1) "details regarding other investigative measures [and procedures] taken to identify such person and an explanation for why such measures failed or are reasonably unlikely to succeed," and (2) a "[p]robable cause to believe that such person has committed or is committing a particular offense" (substantive requirements).[231]

The order, in turn, must include (1) all information that must be in the application, (2) "[a] prohibition on the use . . . of any photo or video not specifically listed in the order," (3) "[a] time period within which the search shall be made not more than 7 days," and (4) "[t]he authority under which the search is to be made."[232]

Similar to provisions of the Wiretap Act,[233] a warrantless search is allowed only in four instances: (1) "identifying any person who is deceased, incapacitated or otherwise physically unable of identifying himself" or crime victims who "cannot be identified through other means"; (2) identifying abducted children under the AMBER Alert program; (3) identifying those lawfully arrested or detained; and,

---

225 Similarly to the Senate bill, the House bill defines FRT as a "process that assists in identifying or verifying an individual or captures information about an individual based on the physical characteristics of an individual's face, head or body, or that uses characteristics of an individual's face, head or body, to infer emotion, associations, activities, or the location of an individual." *See id.* § 3(4).

226 *See id.* § 101(a)(1).

227 *Id.*

228 *See id.* § 101(b)(1).

229 *Id.*

230 18 U.S.C. §§ 2516, 2518.

231 H.R. 9061, 117th Cong. § 101(b)(3) (2022).

232 *See id.* § 101(b)(4).

233 18 U.S.C. § 2518(7).

crucially, (4) when an emergency exists.[234] The test to determine whether an emergency is present is two-fold:

(1) There must be either
   (a) an "immediate danger of death or serious physical injury" or
   (b) a situation where the FRT use is required before a warrant can, "with due diligence," be obtained.

(2) There are "grounds" (as defined in the bill) for the warrant to be authorized.[235] In emergency cases, the following rules must be followed:
   (a) the prosecutor "shall submit an affidavit" to the court stating the reasons why the emergency exists, and
   (b) the officer must
      i. apply for an *ex post* court authorization within 12 hours of the use; and
      ii. if authorization is denied or not obtained
         I. discontinue using the technology "immediately" in the case of a denial or, "in the absence of an application," within 12 hours; and
         II. "destroy all information obtained as a result of the search."[236]

Like the Senate bill, the House bill specifically outlines certain prohibited uses:

(1) to infringe constitutional rights, including free assembly, association, and speech;[237]

(2) relying on any suspect classification "except when there is trustworthy information . . . that links a person with a particular characteristic described . . . to an identified criminal incident or scheme";[238]

---

234 H.R. 9061, 117th Cong. § 101(c)(1) (2022).
235 *Id.* § 101(c)(1)(D).
236 *Id.* § 101(c)(2)–(3).
237 *Id.* § 102(a)(1).
238 *Id.* § 102(a)(2).

(3) in enforcing immigration laws;[239]

(4) use with officers' body cameras;[240]

(5) "face surveillance";[241]

(6) as a "sole basis upon which probable cause is established";[242] and

(7) in conjunction with illegitimately compiled databases.[243]

However, the bill does not preclude law enforcement from using FRTs "for other investigative procedures, such as finger printing, and shall only apply to the use of a reference photo database for the use of facial recognition."[244]

Moreover, facial recognition based on driver's license and identification card photographs, if contained in a state database, is prohibited unless state law "expressly and unambiguously" allows law enforcement to access and apply FRT to such photographs.[245]

The law also imposes certain restrictions on data retention. In particular, the custodian of the arrest photo database "used in conjunction with facial recognition" must remove from it every six months all photographs of (1) minors, (2) persons "released without" (or "acquitted of") a charge, or (3) persons "released after charges are dropped or dismissed."[246]

There are notice requirements in the bill as well. For example, each state's Department of Motor Vehicles is required to notify drivers both generally (in "conspicuous locations" at each office as well as on the website) and individually, as applicants, about "searches of driver's license and ID photos through facial recognition."[247] Law enforcement agencies are also required to notify, in detail, arrested individuals of the use of FRT on them for identification purposes.[248]

---

239 *Id.* § 102(a)(3).
240 *Id.* § 102(b).
241 *Id.* § 102(c).
242 *Id.* § 102(d).
243 *Id.* § 102(e).
244 *Id.* § 101(a)(2)(B).
245 *Id.* § 101(d).
246 *Id.* § 101(a)(2)(A).
247 *Id.* § 101(b)(5)(A).
248 *Id.* § 108.

Next, the bill also proposes detailed reporting (from both the judiciary and the prosecution)[249] and auditing requirements (a detected violation triggers suspension of the FRT use until corrected).[250] Each agency covered by the bill must publicly announce its FRT policy online.[251] In addition, both initial and annual NIST-administered benchmark testing is also mandated so as to ensure accuracy and eliminate the risk of bias; absent successful testing, not a single FRT could be used.[252]

If the facial recognition was conducted in violation of the bill—or, in the case of an emergency, no subsequent authorization was obtained—the recognition results are deprived of all evidentiary value in any "proceeding" before any "authority."[253] Finally, civil action is available for violations of the bill[254] (including a special cause of action for "disparate treatment"),[255] and if "serious questions [could be raised] about whether or not the officer acted intentionally with respect to the violation," such officer is subject to administrative discipline.[256]

As in the Senate bill, "more stringent limitations" on the use of FRTs are not preempted[257]—neither are "any other privacy, civil rights, and civil liberties laws and rules, by the Federal Government, a State, or a political subdivision of a State."[258] However, the bill has a caveat: it prohibits the use of FRTs by states "unless the laws of [a particular] State . . . expressly and unambiguously authorizes such use."[259]

The House bill has a lot of merit. Most importantly, the use of FRTs, in line with our reasoning over Supreme Court precedents, is expressly recognized as a search and, accordingly, a warrant is required. In principle, this alone would already be an acceptable place to end, but the bill goes much further than that. Law enforcement will not obtain the warrant unless it can show that other investigative measures failed or are "reasonably unlikely to succeed."[260] Facial recognition results

249 *Id.* § 104.
250 *Id.* § 105.
251 *Id.* § 203.
252 *Id.* § 106.
253 *Id.* § 107(a).
254 *Id.* § 107(c).
255 *Id.* § 107(d).
256 *Id.* § 107(b).
257 *Id.* § 202(a).
258 *Id.*
259 *Id.* § 202(b).
260 *Id.* § 101(b)(3)(D).

cannot serve as the "sole basis upon which probable cause is established"[261]—a high standard. The search itself is given a maximum of 7 days.[262] The bill additionally lists prohibited uses[263] and specifies very narrow exceptions.[264] Bias is addressed, among other things, by strict NIST testing requirements. No FRT use is allowed upon revelation of a violation until it is cured.[265] In short, this bill is a model piece of legislation.

Still, we would point out a few shortcomings. First, when the bill authorizes the exploitation of arrest photo databases in "other investigative procedures" and mentions fingerprinting as an example,[266] it does not make the list of exceptions exhaustive. Perhaps this should be done to avoid an extensive interpretation contrary to the spirit of the bill. Second, the state-use caveat[267] gives states broad discretion and partially overrides the no-preemption rule, as it is not always clear when privacy and civil rights laws would provide greater protections than the bill. We see the bill as a positive example; yet, the bill failed to pass. A newly introduced moratorium bill in the Senate—not discussed in this Article—did not advance past Committee referral.[268] While members of congress promised to take aim at FRT use in airports, no such undertaking has been announced with respect to FRT use by law enforcement.[269]

2. State Statutes and Bills

a. Overview

At the other end of the spectrum are some efforts to regulate the use of FRTs at the state and local level. For instance, around twenty local communities have imposed moratoria or banned the use of FRTs,

---

261 *Id.* § 102(d).

262 *Id.* § 101(b)(4)(C).

263 *Id.* § 102(b) to 102(e).

264 *Id.* § 101(c).

265 *Id.* § 102(e).

266 *Id.* § 101(a)(2)(B).

267 *Id.* § 101(d).

268 Facial Recognition and Biometric Technology Moratorium Act of 2023, S. 681, 118th Cong. (2023).

269 Luke Broadwater, *Senators Seek to Curb Facial Recognition at Airports, Citing Privacy Concerns*, N.Y. TIMES (May 7, 2024), https://www.nytimes.com/2024/05/07/us/politics/airport-facial-recognition-technology-congress.html [https://perma.cc/27FK-UKFB].

including Berkeley, San Francisco, Boston, and other cities.[270] Conversely, the Chicago Police Department is actively using FRTs.[271]

In some states, regulation varies by location or type of use. New York, for instance, has banned, with some few exceptions, the use of FRTs in schools.[272] Recently, the State Education Department Commissioner upheld the ban.[273] But otherwise, the NYPD quite freely uses the technology,[274] as it itself admits.[275]

While not explicitly directed at FRT, the Biometric Information Privacy Act in Illinois (BIPA),[276] enacted in 2008, is recognized as one of the most stringent state laws on biometric data privacy in the United States, however, it regulates only private sector use.[277]

Yet other states attempted to regulate FRTs,[278] balancing—albeit not always appropriately—law enforcement needs with privacy concerns.

---

270 Nathan Sheard & Adam Schwartz, *The Movement to Ban Government Use of Face Recognition*, ELEC. FRONTIER FOUND. (May 5, 2022), https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition [https://perma.cc/2C3G-JSR8].

271 *Chicago Police Launch New Facial Recognition Technology, They Say, to Catch Crooks*, CBS NEWS CHI. (Feb. 7, 2020, 10:22 PM), https://www.cbsnews.com/chicago/news/chicago-police-launch-new-facial-recognition-technology-they-say-to-catch-crooks/ [https://perma.cc/2HAH-JQZS]. ("The [Chicago Police] department has used some form of facial recognition tech since at least 2013.").

272 N.Y. STATE TECH. LAW § 106-B (2)–(3) (McKinney 2024).

273 Commissioner of Education of the State of New York, *Determination on the Use of FRTs in Schools*, U. STATE N.Y. (2023), https://www.nysed.gov/sites/default/files/programs/data-privacy-security/biometric-determination-9-27-23.pdf [https://perma.cc/P7VT-DGPX].

274 *See, e.g.*, *Surveillance City: NYPD Can Use More Than 15,000 Cameras to Track People Using Facial Recognition in Manhattan, Bronx and Brooklyn*, AMNESTY INT'L (June 3, 2021), https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/ [https://perma.cc/NX3H-3M8W] (observing that "[t]he NYPD has used facial recognition technology (FRT) in 22,000 cases since 2017—half of which were in 2019 alone").

275 *See Facial Recognition: Impact and Use Policy*, N.Y. POLICE DEP'T (2023), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_10.26.23.pdf [https://perma.cc/HTV6-6H7Y] (no warrant is required under the policy to conduct an FRT search).

276 Illinois Biometric Information Privacy Act, Pub. Act 95-994, 2008 Ill. Laws 380 (codified as amended at 740 ILCS 14/1 to 14/99).

277 Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, NE. U. SCH. L. PUB. L. & LEGAL THEORY RSCH. PAPER SERIES 96, 96–103 (2020).

278 *See, e.g.*, Carolina Rabinowicz, *Approaches to Regulating Government Use of Facial Recognition Technology*, HARV. JOLT DIGEST (May 4, 2023), https://jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-of-facial-recognition-technology [https://perma.cc/ZKH4-CT5G] (outlining the various approaches taken by different communities and states with respect to the FRT regulation).

Most notable examples worthy of further examination include California and Texas.

b. Texas

The 2009 Texas FRT statute is of particular importance, as it expressly prescribes that "[a] person who possesses a biometric identifier of an individual that is captured for a commercial purpose may not . . . disclose the biometric identifier to another person unless the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant."[279] "Biometric identifier," under the statute, means "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[280]

The Texas law also sets forth other imperatives, in particular, (1) the requirement to inform and obtain consent from the individual,[281] (2) the requirement to protect the identifier "from disclosure . . . using reasonable care and in a manner that is the same as or more protective than the manner in which the person . . . protects any other confidential information the person possesses" (a very high standard),[282] and (3) specific rules as to the retention and deletion periods (generally one year "from the date the purpose for collecting the identifier expires").[283]

The Texas statute, explicitly introducing the warrant requirement while not barring law enforcement use, can be seen as a reference for legislators in other states. At the same time, in the definition of a "biometric identifier," the law uses the outdated concept of "face geometry." As early as 2009 (the year when the statute was enacted), scholars noted that modern FRTs no longer utilize the geometry of the face,[284] but instead focus on its appearance (shape and texture).[285] Yet, since all three technology variants—geometry-based, appearance-based, and hybrid—are still in use,[286] the definition in the law is worth revising in favor of a more general one in the same manner as the House

279 TEX. BUS. & COM. CODE ANN. § 503.001(c)(1)(D) (West 2009).

280 *Id.* § 503.001(a).

281 *Id.* § 503.001(b).

282 *Id.* § 503.001(c)(2).

283 *Id.* § 503.001(c)(3).

284 *See* Lior Wolf, *Face Recognition, Geometric vs. Appearance-Based*, ENCYCLOPEDIA BIOMETRICS 347, 351 (Stan Z. Li & Anil K. Jain eds., 2009) (noting that "the leading face recognition methods [nowadays] are also appearance based").

285 *See id.* at 348–49 (describing the way appearance-based FRTs work).

286 *See generally id.* at 348–51 (outlining the three types of FRTs).

bill. Even in the absence of review, arguments can be made in favor of a broad reading of the statute.[287]

c. California

California's draft law that lapsed in January 2024,[288] introduced soon after the expiration of the state's three-year ban on January 1, 2023,[289] targets FRTs even more directly. The draft law provides its own definition of FRTs: "'Facial recognition technology' or 'FRT' means a system that compares a probe image of an unidentified human face against a reference photograph database and, based on biometric data, generates possible matches to aid in identifying the person in the probe image."[290]

The bill does not, as of now, require a warrant to use the FRT, but, nevertheless, imposes other significant limitations that appear to be borrowed from the House bill.[291] To name a few, the authorities may use the technology only for identifying (1) alleged criminals who, under "reasonable suspicion" of the officer, "ha[ve] committed a felony" or who "ha[ve] been lawfully arrested"; and (2) any persons if they are deceased, missing, or "an emergency situation exists that involves immediate danger of death or serious physical injury to" such persons (quite similar to the House bill).[292] Further, a detailed description and probe image are required and, more importantly, "[a]ny details regarding other investigative measures . . . and an explanation of why those measures failed or are reasonably unlikely to succeed"[293] also need to be presented (almost a verbatim borrowing from the Wiretap Act[294]).

---

287 *See* Pls.' Resp. to Def's. Mot. to Dismiss at 23–24, ACLU v. Clearview AI, No. 20 CH 4353, 2021 WL 4164452 (Ill. Cir. Ct. Aug. 27, 2021) (citing cases extensively interpreting a similar definition of an Illinois statute and stating that "facial geometry . . . can be derived from any source (including a photograph)"). The court sided with ACLU. ACLU v. Clearview AI, Inc., No. 20 CH 4353, 2021 WL 4164452, at *5 (Ill. Cir. Ct. Aug. 27, 2021) ("The Complaint describes a faceprint as just that, a scan of face geometry. The fact that the scan was made from a photo and not from a live person does not change that fact.").

288 Assemb. B. 642, 2023 Leg., Reg. Sess. (Cal. 2023).

289 CAL. PENAL CODE § 832.19 (repealed 2023) (criminalizing the use of FRTs).

290 Assemb. B. 642 § 13675(b)(1).

291 *See* H.R. 9061, 117th Cong. (2022).

292 Assemb. B. 642 § 13675.1(a).

293 *Id.* § 13675.1(b)(4) (emphasis added).

294 Wiretap Act, 18 U.S.C. § 2518(1)(c).

Next, though no warrant is required, officers are expressly prohibited to "[u]se an FRT match as the sole basis upon which probable cause is established for a search, arrest, or affidavit for a warrant"[295] (again a verbatim borrowing[296]). The bill also responds to the First Amendment and bias concerns by forbidding FRT identification "on the basis that the person is exercising . . . free assembly, association, and speech"[297] and relying on race and other suspect classifications, "except when there is trustworthy information . . . that links a person with a particular characteristic"[298] (the latter is again a complete copy of the House bill[299]). Furthermore, law enforcement reports on FRT use are to be prepared annually beginning this year, 2025.[300] Violations of all these strict rules are not considered a crime; rather, the victim may bring a civil action seeking statutory damages.[301]

Although the sponsors of the California bill have attempted to strike a proper balance between the divergent interests, the bill failed to do so.[302] Without the warrant requirement, this bill is but a pale shadow of the House bill.

3. Recommendations

Perhaps the most proportionate solution—at least in terms of the U.S. framework—would be to require a warrant for the use of FRTs in law enforcement similar to the requirements for wiretapping.[303] This seems to be in line with the Supreme Court's case law on privacy, free speech, and equal protection, as well as with other courts' recent developments. However, for FRT use to be universally recognized as a

295 Assemb. B. 642 § 13675.2(f).

296 H.R. 9061, 117th Cong. (2022), § 102(d).

297 Assemb. B. 642 § 13675.2(a).

298 *Id.* § 13675.2(b).

299 H.R. 9061, 117th Cong. (2022), § 102(a)(2).

300 Assemb. B. 642 § 13675.3.

301 *Id.* § 13675.6.

302 The bill has already received some critique. *See* Matt Cagle, *Progress in the Fight Against Face Surveillance*, ACLU N. CAL. (Aug. 8, 2023), https://www.aclunc.org/blog/progress-fight-against-face-surveillance [https://perma.cc/JCT7-AR8F] (labeling the bill as "a wolf in sheep's clothing" because it "claimed to limit face surveillance, but in reality, would have provided law enforcement with sweeping authorization to use the technology to scan, track, and record people without their knowledge or consent"). Note that another bill, calling for extension of the ban up to 2034, has been introduced as well. *See* Assemb. B. 1034, 2023 Leg., Reg. Sess. § 2(e) (Cal. 2023).

303 *See* Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165 (1952).

search, a Supreme Court ruling or a federal statute is highly desirable. While the former, in our estimate, is more than realistic and likely to happen in another 5–10 years, the latter requires a concerned legislature, and Congress is currently not one.[304] Nevertheless, at the state and local level, both statutory and case law FRT frameworks are gradually being fleshed out. In any case, the Texas FRT law and especially the House bill that both explicitly establish the warrant requirement, can serve as good reference points. On the other hand, to adopt the California draft bill that does not require a warrant for an FRT search would be a huge mistake.

A complete or temporary ban is another option, but its adoption at the federal level seems like a pipe dream. If the Supreme Court approaches FRT use, it is unlikely that it will go further than proclaiming the warrant requirement. The states, however, have been more successful in this endeavor.[305]

Nothing prevents combining a regulatory and prohibitory approach: recognizing the warrant requirement at the federal level (either in statute or by decision of the Supreme Court) and allowing states to impose "more stringent limitation[s]" (as proposed, e.g., by the Senate bill), and thus completely prohibit the use of FRTs.

If the use of FRTs is regulated legislatively, it will also allow for a more nuanced framework. As an analysis of the House bill, Texas statute, and California draft law has shown, there are many more FRT-related issues than just whether a warrant is required, and these issues appear to be better addressed by the legislature.[306]

CONCLUSION

By delving into the different legal and ethical challenges posed by FRT's use in law enforcement across three jurisdictions, this paper has sought to provide an accessible and comprehensible commentary to promote further deliberations on this issue. As highlighted in preceding

304 Joe Fisher, *Congress Ends 2023 as Most Inactive Year Since Great Depression*, UPI (Dec. 20, 2023, 11:32 AM), https://www.upi.com/Top_News/US/2023/12/20/2023-congress-year-in-review-inactive-session/4791703087623/ [https://perma.cc/3UTC-WDLX] (observing that "[t]he 118th Congress . . . ha[s] passed 22 pieces of legislation, the lowest tally since the Great Depression").

305 *See supra* Section III(B)(2).

306 One could also think of different measures incentivizing FRT developers to achieve greater accuracy. In addition to what we saw in the House bill, some researchers are also proposing to provide an R&D tax credit to FRT sellers to ensure continued improvements in accuracy. *See* Bass, *supra* note 203, at 1083.

Sections,[307] there are currently legislative and regulatory loopholes in the governance of FRTs in each of the jurisdictions under examination in this paper.

In India, there is currently a regulatory vacuum with respect to governance of FRTs for law enforcement purposes, despite the enactment of the DPDP Act.[308] There is an urgent need to fill this vacuum with a dedicated statutory framework, operating at the federal level, which is consistent with the principles of proportionality espoused in the landmark *Puttaswamy-I* judgment on the fundamental right to privacy.[309]

By contrast, the European Union will soon enforce the Artificial Intelligence Act, a comprehensive regulatory framework on the matter.[310] However, it provides inadequate human rights protection regarding FRT use by law enforcement due to its vagueness, its lack of transparency requirements, and its lack of a strict requirement against bias.[311] This raises concerns with regard to potential misuse and discrimination, particularly against people of color. While case law by supreme judicial bodies in Europe recently offered some protection on the right to privacy and the freedom of expression,[312] it would be highly recommendable to implement strict, concrete, and effective protection of human rights into the regulatory framework, instead of relying on judicial intervention.

Lastly, in the United States, like in India, there is also a certain regulatory vacuum. There is no U.S. Supreme Court decision that explicitly sets forth a particular regulatory regime with respect to FRT, nor is there any federal legislation.[313] However, a thoughtful analysis of the Supreme Court's decisions leads to the conclusion that the use of FRT is a search that requires a warrant.[314] Congress, on the other hand, has already proposed several noteworthy bills (both blocking and regulating the use of FRTs), but has since failed to pass a regulatory legal framework.[315] States are more successful in regulating facial

307 *See supra* Sections II(E), III(A)(2), III(B)(1).

308 *See supra* Section II(F).

309 *See supra* Sections II(E), II(F).

310 *See supra* Section III(A)(1).

311 *Id.*

312 Glukhin v. Russia, App. No. 11519/20, Judgement, (European Court of Human Rights (July 4, 2023)).

313 *See supra* Section III(B)(1).

314 *Id.*

315 *Id.*

recognition.[316] At the state and local level, we see a variety of approaches ranging from permissive (including the absence of regulation), to a permanent ban, or balanced regulation.[317] The best exemplars of which also require a search warrant for FRT deployment.

Broader questions as to whether FRTs need to be outright banned, temporarily suspended, or effectively regulated, can be addressed only through greater engagement with diverse stakeholders, including civil society activists, privacy advocates, academics, and members of the legal field.

As a parting note, although this Article highlights many challenges with the current accuracy and dependability of FRT systems, it is possible that, over time, this technology may mature to a state that can overcome several of these concerns. This makes it necessary to reinforce that the satisfactory performance of FRTs is only an important, but not sufficient, precondition for the deployment of such systems. The use of FRTs must be supported in all cases, but particularly in law enforcement, by a robust framework for gauging the suitability and proportionality of its deployment. There is also a need for broader, interdisciplinary studies to understand how societies are likely to be reshaped under the ubiquitous gaze of FRT systems.

316 *See supra* Section III(B)(2).

317 *Id.*