FACING // THE FUTURE:

Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement

Case Studies from the United Kingdom and the United States

Henriette Ruhrmann

May 2019

CITRIS AND THE BANATAO INSTITUTE | CITRIS POLICY LAB

FACING // THE FUTURE:

Protecting Human Rights in Policy Strategies
for Facial Recognition Technology
in Law Enforcement

Case Studies from the
United Kingdom and the United States

Henriette Ruhrmann
May 2019

Author Contact
henriette_ruhrmann@berkeley.edu

GOLDMAN SCHOOL OF PUBLIC POLICY
UNIVERSITY OF CALIFORNIA BERKELEY

CITRIS AND THE BANATAO INSTITUTE

CITRIS POLICY LAB

The author conducted this study as part of the program of professional education at the Goldman School of Public Policy, University of California at Berkeley. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgements and conclusions are solely those of the author, and are not necessarily endorsed by the Goldman School of Public Policy, by the University of California or by any other agency.

About the CITRIS Policy Lab

The CITRIS Policy Lab is a sub-organization of the Center for Information Technology Research in the Interest of Society (CITRIS) and the Banatao Institute headquartered on the UC Berkeley campus. CITRIS and the Banatao Institute were founded in 2001 as part of an initiative launched by California Governor Gray Davis to leverage science and innovation to address societal problems. With the goal to develop technology applications with societal and economic benefits, the Institute facilitates interdisciplinary research across four UC campuses in Northern California at Berkeley, Davis, Merced, and Santa Cruz, and offers resources including seed funding and a startup accelerator. As part of the Institute's focus on societal impact, the CITRIS Policy Lab was established in 2018 with the goal to support interdisciplinary technology policy research analyzing technology capabilities and their implications for society. Through its collaboration with public and private sector stakeholders, the CITRIS Policy Lab seeks to contribute to ensuring technology is designed and deployed in the interest of society.

Executive Summary

Facial recognition technology (FRT) is gaining traction in law enforcement as a tool to identify persons of interest in criminal investigations. However, FRT leverages a uniquely sensitive biometric trait that is both immutable and always exposed to the public, which means that unregulated use of FRT in law enforcement creates risk for human rights. The goal of this policy analysis is to serve as a resource for discourse and policymaking around FRT by providing a systematic three-dimensional policy analysis framework to assess to which degree regulatory policies safeguard the most relevant human rights in the context of FRT, privacy, equity or non-discrimination, and due process. The analysis draws on qualitative methods, including a literature review, expert interviews, and archival research to operationalize each concept in measurable sub-variables and apply the framework to two case studies of two mature democracies active in FRT use and committed to protecting civil liberties, the UK and the US.

The findings show that in both countries, FRT-specific regulation is necessary to account for the unique risks FRT poses for human rights. In the area of privacy, both countries enroll images without the data subject's active consent, including criminal booking photos, including of individuals never charged or convicted. While neither country has comprehensive FRT legislation, in the UK, data subjects enjoy rights under general data protection regulation for personal data. Equity is problematic in both countries due to a lack of critical engagement with bias in enrollment practices and the algorithm leading to a disparate impact of FRT, particularly for ethnic minorities. Regarding due process rights, UK law enforcement agencies consult and communicate more effectively with stakeholders whereas in the US federal programs operated for years prior to the publication of a privacy impact assessment.

Overall, the comparative policy analysis demonstrates that even in countries with a strong commitment to civil liberties, FRT-specific legislation is necessary to enforce human rights in the context of this emerging technology. A challenge highlighted by the findings is the knowledge gap between innovators and the public, as well as their elected representatives, which creates a concerning information asymmetry. In the future, approaches should be developed facilitate knowledge transfer to bridge the gap and create legislation driven by informed public preferences and specific to the risks posed by FRT to ensure the respect of human rights in this new socio-technical context.

Contents

Figures & Tables

Abbreviations

Technical

AI	Artificial Intelligence
API	Application programming interface
CNN	Convolutional neural networks
CCTV	Closed-circuit television
EER	Equal error rate
FAR	False acceptance rate
FRR	False rejection rate
FRT	Facial recognition technology
FRVT	Facial Recognition Vendor Test
FTE	Failure to enroll
ICCPR	International Covenant on Civil and Political Rights
ID	Identity
ML	Machine Learning
UDHR	Universal Declaration of Human Rights

UK Context

APP	College of Policing's Authorised Professional Practice
BFEG	Biometrics and Forensics Ethics Group
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
EPRS	European Parliamentary Research Service
EU	European Union
FOI Act	Freedom of Information Act
GDPR	General Data Protection Regulation
MOPI	Code of Practice on the Management of Police Information
PACE Act	Police and Criminal Evidence Act
SOI	Subject of Interest
UEFA	Union of European Football Associations

US Context

ACTIC	Arizona Counter-Terrorism Information Center
ACLU	American Civil Liberties Union
BPCS	Booking Photo Comparison Software
CITRIS	Center for Information Technology Research in the Interest of Society
CJIS	Criminal Justice Information Services
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
DOJ	Department of Justice
DPPA	Driver's Privacy Protection Act
EFF	Electronic Frontier Foundation
FACE	Facial Analysis, Comparison, and Evaluation Services Unit
FACES	Face Analysis Comparison & Examination System
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
IPS	Interstate Photo System
MCSO	Maricopa County Sheriff's Office
NGI	Next Generation Identification System
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
PIA	Privacy Impact Assessment
PCSO	Pinellas County Sheriff's Office
PD	Police Department
SANDAG	San Diego Association of Governments
SORN	Systems of Records Notice
UPF	Unsolved Photo File

INTRODUCTION

PROBLEM DEFINITION

Frame AI-enabled FRT holds the potential to enable greater efficiency in the provision of vital services that depend on the accurate identification of individuals by both the public and private sectors. Facial recognition technology may prove to be a key technology in increasing efficiency in contexts where establishing identity has been inherently difficult and crucial for ensuring individuals' safety online and offline. Prominent examples of public sector applications include the rapid verification of identities of large numbers of people, for example, in the context of law enforcement, for real-time searches for persons of interest, including missing persons or suspected criminals among large populations,[1–5] and border security[6–8]. At present, governments around the world face a critical moment as they establish identity systems using FRT or integrate FRT in existing systems, in which they need to develop a viable policy framework that ensures the respect of protected human rights principles.

Realizing significant efficiency gains in public service delivery through FRT, depending on the design of the technology application, may come at the cost of fundamental societal values, in particular: privacy, non-discrimination, and due process. Problem areas include the handling of misidentification cases, in particular, considering the misidentification bias against

women and people of color,[9] and the threat of perpetual surveillance eroding reasonable expectations of privacy given that facial recognition only requires passive rather than active consent (like fingerprinting), as well as facilitating public discourse on a system that utilizes one of the most immutable biometric characteristics.[10] Microsoft has led major players in the development of AI-enabled FRT in recognizing the substantial scale of the technology's potential beneficial and harmful impacts and calling for a principle- or value-based framework for the design and commercialization of AI-enabled facial recognition applications.[11–13]

At present, however, the use of FRT in law and border enforcement is subject to insufficient regulation in the UK and US that is specifically designed to protect human rights given the new challenges posed by the emerging technology, and the public with democratic popular sovereignty has too little awareness of these risks.

Quantify Over the past 20 years, the academic interest and volume of research in terms of the number of papers published on AI has increased at a four times higher rate than research overall. Computer vision, including facial recognition, is among the top three most researched areas of AI. In the US, the corporate sector dominates the AI research space whereas in China and Europe the public sector is leading.[14] In conjunction with this increase in research, the number of AI startups has increased at almost double the rate of startups overall since 2015 fueled by a fourfold increase in venture capital funding over the same period.[14] However, most of the countries leading in AI research, including the US and China, as well as countries of the European Union (EU) did not establish national high-level AI policy strategies before 2017 let alone comprehensive regulation of specific AI-enabled technologies such as FRT. Both the US and the UK did not develop AI strategies until 2018, for example.[15] Only 8% of 52 US government agencies (not bound by strict data protection regulation such as the EU's General Data Protection Regulation (GDPR)) in a comprehensive study had a publicly available FRT use policy.[10] Moreover, as late as 2017, a Eurobarometer survey found that 52% of Europeans had not heard of AI in the past 12 months and Morning Consult that 48% of US Americans had not heard much or anything about AI.[16,17] Certain demographic groups are more at risk of being unaware of AI, including women, seniors, African Americans, individuals who are unemployed or of low socioeconomic status, and individuals who reside in rural communities.[16,17]

However, 117 million US American adults or more than every third US American is included in facial recognition networks.[10] In the UK, at least 12.5 to 16.6 million images are searchable using FRT, which means that up to every fourth to fifth UK resident's image may be automatically recog-

nized.[18,19] Survey results suggest that over 80 percent of US American and European respondents believe the development of AI should be carefully managed.[16,20] However, with regard to FRT specifically, only 26.2% agree with the statement that "the government should strictly limit the use of surveillance cameras" and more than every third US American had no opinion on the issue.[21] Moreover, almost 40% of survey respondents agreed that "Police departments should be allowed to use facial recognition technology to help find suspects if the software is correct 80% of the time."[21] The public may still be underestimating the risks posed by harmful AI as survey respondents viewed "harmful consequences of AI" as a relatively unlikely and unimpactful global risk in stark contrast to expert assessments.[20,22,23] This is due in part to a lack of government agencies' contribution to public awareness and accountability.

Diagnose Contributing factors to this growing gap between public awareness and the rapid development and adoption of AI applications include the prioritization law and border enforcement goals and protection of industrial secrecy that allow developers to shield their models from public scrutiny. In particular in application cases where the public sector employs AI for facial recognition, agencies find themselves in a conflict of interest between their organizational goals and the public interest in transparency and accountability.[24] Moreover, AI development and employment occur in a context of rapid innovation in an arms race with domestic and foreign competitors. Lastly, regulating innovation in the area of AI is often opposed based on the argument that public consultation processes slow down the innovation process, which may lead to competitive disadvantages or, in the case of applications relevant to national security, geopolitical vulnerability.

Government Intervention The international community and many nation-states have affirmed their commitment to protecting privacy and non-discrimination as a fundamental right. At the international level, the 1948 Universal Declaration of Human Rights (UDHR) in Article 12 states that "no one shall be subjected to arbitrary interference with his privacy (...)" and in Article 2 that "everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[25] Moreover, major national and supranational jurisdictions have recognized the right to privacy, including the US[26] the EU.[27] The right to non-discrimination is even more firmly rooted in the constitutional documents of the US[28] and the EU.[29–31] These legal protections attest to the fact that protecting privacy and freedom from discrimination are widely desirable shared social preferences that generate utility for all protected individuals. Furthermore, in the context of their status as fundamental rights, violations of the right to privacy and non-dis-

crimination, for example, due to the institutional overreach of government agencies, create an unacceptable institutional outcome. Therefore, addressing impending threats to the rights to privacy and non-discrimination is an urgent public responsibility.

Objectives Given the strong moral and legal obligation to ensure effective protection of fundamental rights in the context of emerging technology risks, including threats posed by AI-enabled facial recognition, national and international policymakers should develop policy strategies that allow their constituents to understand and influence the deployment of this technology. Specifically, the public must be aware of the use of facial recognition technology, its implications, and their rights in this context. Moreover, both the technology development and implementation process must afford opportunities for the public to voice concern and effectively object via democratic engagement.

ANALYTICAL APPROACH

The objective of this policy analysis is to develop an analytical framework that allows policy practitioners to evaluate to which degree regulatory policy strategies around the use of AI-enabled FRT by law enforcement agencies protect internationally recognized human rights. To this end, the project develops a policy analysis framework around the three most relevant human rights in the context of FRT: Privacy, equity or non-discrimination, and due process. These three human rights principles form the analytical axes which current regulatory strategies can be measured against in a cross-jurisdictional comparison. Moreover, the policy analysis framework is applied in two case studies which map existing regulatory strategies in the US and UK and assess their capacity to safeguard fundamental human rights both countries are committed to protecting.

Research Methods

The research methodology follows a qualitative multi-method approach to inform the development of the policy analysis framework and its application to the two case studies. In particular, the research draws on semi-structured interviews with experts in the area of computer vision and data privacy. Moreover, the study is informed by extensive archival research spanning a diverse range of source documents including legislative archives, parliamentary hearing protocols, Freedom of Information requests, as well as internal memos and investigations.

Case Selection

The comparative policy analysis focuses on the UK and the US, which are both leaders in FRT adoption in law enforcement and exhibit relevant structural similarities. Both countries are highly developed and among the most mature, consolidated, modern democracies. Moreover, both countries have a long tradition of a commitment to protecting civil liberties. However, the US and European countries generally vary in their approach to regulating emerging technologies as the US pursues a more fast-paced, innovation-friendly, market-driven strategy and European countries pursue a relatively cautious, value-driven strategy with relatively less innovative momentum.

Despite their similar economic development and democratic political system, the US is almost five times more populous than the UK and FRT has been used more extensively by various jurisdictions. For this reason, a relatively longer section of the analysis is devoted to mapping the FRT use cases and regulatory policies across the US. The UK case study to the author's knowledge comprehensively maps FRT use in law enforcement. However, given the greater number of jurisdictions employing FRT in the US case study, the analysis highlights in depth only one jurisdiction at each level of government, the federal, state, county, and city level. Within the US, cases were selected based on variation in FRT use policies to illustrate the most exemplary and the most problematic use of FRT in law enforcement.

Structure

The report is organized in the following four sections: Part 1 discusses the architecture of an FRT system, its functional logic, and technological capabilities and limitations. Part 2 develops the three-dimensional criteria-based policy analysis framework around the axes of Privacy, Equity, and Due Process. Each human rights concept is operationalized in the context of FRT and a three-point coding scheme for each individual sub-variable is developed to score policies on the degree to which they are effective in protecting each human right. Part 3 maps existing alternative regulatory policy strategies in the US and UK and score them on the basis of the criteria in the policy analysis framework. Part 4 discusses emerging issues related to the regulation of FRT.

01 //

TECHNOLOGICAL CAPABILITIES AND RISKS

01 //

TECHNOLOGICAL CAPABILITIES AND RISKS

A biometric ID system involving facial recognition capability is comprised of several critical system elements. Understanding these key elements of the facial recognition architecture is essential to recognize the implications and tradeoffs of alternative system and policy design choices. The following technical terms will be used throughout this section:

Data Subject:
An individual whose identity the system aims to verify or establish

Biometric Sample:
A representation of a biometric trait, in this case, the face

Sensor:
The camera equipment necessary to capture the biometric sample

Reference Template:
Key unique features extracted from the biometric sample

Reference Storage:
The permanent repository where a reference template is stored

Overall, a facial recognition system operates across two distinct operational phases,[32] firstly the enrollment phase, during which a data subject is registered in the system, and secondly the matching phase, during which facial recognition is used to draw conclusions about a data subject's identity based on information in the system. Broadly speaking, the matching phase may have two goals: Firstly, matching may serve to verify an individual's identity, for example, upon presenting a biometric passport at an airport, by matching the individual's biometric sample to a stored template linked to their identity (1-to-1 matching). Secondly, matching may serve to identify an individual by matching their biometric sample against all templates stored in the system (1-to-N matching).

KEY FEATURES OF THE TECHNOLOGICAL INFRASTRUCTURE

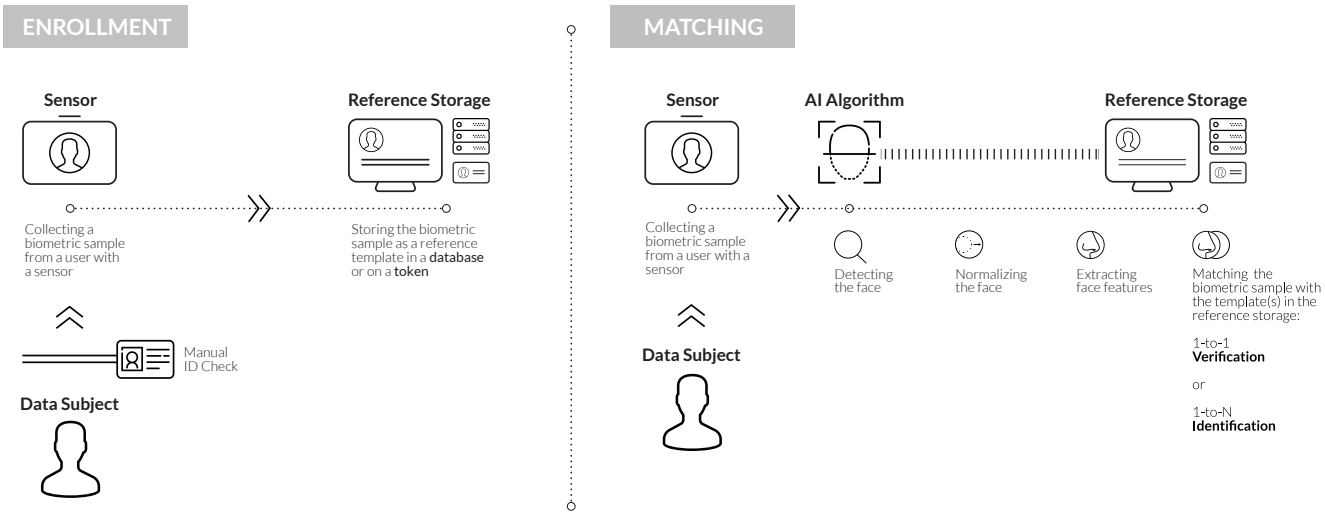


Figure 1 // Facial Recognition System Architecture

Enrollment Phase

In the enrollment phase, the data subject is first registered in the facial recognition system, which means information about their biometric trait in question, the face, is linked with information about their identity. For this reason, a manual ID check is a crucial part of the enrollment phase to ensure that the link of information is accurate.[32] Once the data subject's identity was manually established during enrollment, a sensor is used to capture a biometric sample of the data subject. In the case of facial recognition, the sensor consists of a camera capturing an image.[32] The biometric sample is then permanently stored as a template in a reference storage. The storage solution may either consist of a centralized or distributed database where all reference templates are stored collectively or of a token, for example, a biometric passport, on which the reference template is stored individually.[33]

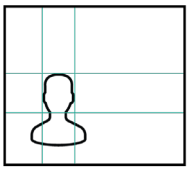
Main System Design Choice

Sample Quality Threshold The quality of the biometric sample for the purposes of facial recognition is determined by a number of factors, including characteristics of the biometric trait in the person, the sensor equipment and handling thereof, or factors in the environment such as lightning. The quality threshold set in the system design process sets the minimum acceptable quality of a sample for the facial recognition process and is directly related to the failure-to-enroll (FTE) rate as a system performance metric.[33,34]

Matching Phase

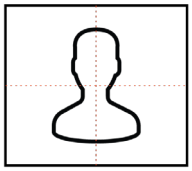
The matching phase may have two distinct purposes: On the one hand, the goal may be to verify or authenticate a data subject's identity by comparing a biometric sample collected from them with a specific enrolled template in the reference storage with a unique identifier linked to the data subject (1-to-1 matching). On the other hand, matching can serve to identify a data subject by comparing their biometric sample to all templates enrolled in the reference storage (1-to-N matching). In the matching phase, a biometric sample is again collected with a camera as the sensor from a data subject whose identity is in question. With recent technological advances, a biometric sample can be obtained in more and more challenging conditions including, for example, just relying on thermal images.[35] An AI algorithm determines the degree of match with one or all reference templates in the reference storage. The main technological foundations for this capability are image processing and pattern recognition.[32] The process can be

summarized in four distinct steps connected in an "information pipeline", which means that each step is critical for the subsequent steps and the success of the process.



Detecting the Face

There are many computational strategies for detecting a face in an image,* which subsequently inspect subregions of an image, locate image patterns, and compare the patterns found with a training data set of known faces using machine learning (ML).**[41] One common method is to move a sliding window across an image and for each subregion within that window identify contrasting areas, for example, between the darker eye and lighter forehead region. The seminal algorithm developed by Viola & Jones in 2001[42] relies on two-toned rectangles called Haar-like features to sum these regional differences in light. Using ML, the algorithm then passes regions as "face candidates" through a cascade of stages in which non-faces are rapidly rejected at the end of each stage. Another common method is to evaluate each pixel as a subregion based on the change in light and dark areas between the pixel and the surrounding pixels to identify border areas. This Histograms of Oriented Gradients (HOG) approach developed by Dalal & Triggs in 2005[43] relies on the information captured about each pixel and pixel group and uses machine learning to compare the information with known images of faces in the training data set.[44] The process of detecting a face in an image can be further automated using deep learning, specifically convolutional neural networks (CNN) to locate visual patterns automatically and even integrate the following step of face normalization on the basis of vast training data sets.[45,46]



Normalizing the Face

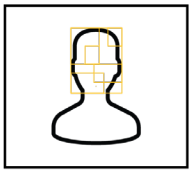
Once a face is detected, it needs to be aligned or normalized to correct for variation in preprocessing, including reducing the variation in sizes and poses (geometric normalization) and in illumination (photometric normalization).[47] The goal is then to estimate the position of facial landmarks such as the corners of eyes and mouth and adjust their position in the image

---

* Several techniques have been employed to avoid detection and identification by FRT applications including morphing, the blending of two images[36,37] occlusion with accessories,[38] and confusion through camouflaging makeup and hairdos[38,39].

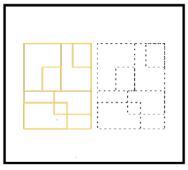
** Machine learning applications pass training data through a learning algorithm, for example, a decision tree that splits the dataset based on variables available in the dataset into a number of different groups or classifications. This process generates a machine learning model specific to the type of training data used. The machine learning model acts as a learned algorithm that a new data point is passed through to arrive at the desired answer, for example, a classification.

frame. Accurate image transformations in this stage are key for the success of face matching at stages further down the pipeline, which means that it is critical to correctly place facial landmarks to not distort the image.[44]



Extracting Face Features

From the normalized face image, an AI/ML model determines which features of the face are most salient in distinguishing one face from another. Given that the ML model selects the face features, they are not the features that can be interpreted or would typically be used to describe a face by a human observer. The algorithm captures information about the selected features in a numerical encoding (face vector, face print, or face embedding) with a standard set of 128 numbers that describe face features. The distance between the numbers in the encoding can be interpreted as the degree to which two faces are different. At this stage, a disconnect emerges between the interpretation of a face image by the algorithm and a human observer because a small change in a pixel that changes a face feature that the algorithm considers critical is highly relevant to the machine but may be irrelevant to a human observer.[44]



Matching Face Features

On the basis of the encoding, an AI/ML model determines the degree of similarity between the encoded face and one or all face templates in the reference storage. It is important to note that regardless of which of the continuously developing AI/ML models is employed in the matching task, the result is invariably a similarity score and not an authoritative matching decision. The matching decision is a product of the similarity score and a deliberately chosen threshold above which a similarity score justifies a match.[32]

Main System Design Choices

Degree-of-Match Threshold The choice of the degree-of-match threshold must strike a balance in the tradeoff between accuracy and efficiency. The higher the degree-of-match threshold, the more difficult it is to produce a similarity score that satisfies the requirement in the matching process both for a fraudulent and a genuine data subject who may, depending on external circumstances, need several attempts to authenticate herself. The lower the degree-of-match threshold, the easier it is for authentic and fraudulent data subjects to pass, which makes the system easy to use but vulnerable to fraud. This tradeoff implies that the rate at which genuine data subjects are falsely rejected (false rejection rate, FRR) increases and the rate at which fraudulent data subjects are falsely accepted (false acceptance rate, FAR) decreases when raising the degree-of-match threshold (see Fig. 2). The degree-of-match threshold at the point where FRR and FAR are equal, referred to as the equal error rate (EER), can but does not have to be the preferred threshold to balance the tradeoff.[32,33]

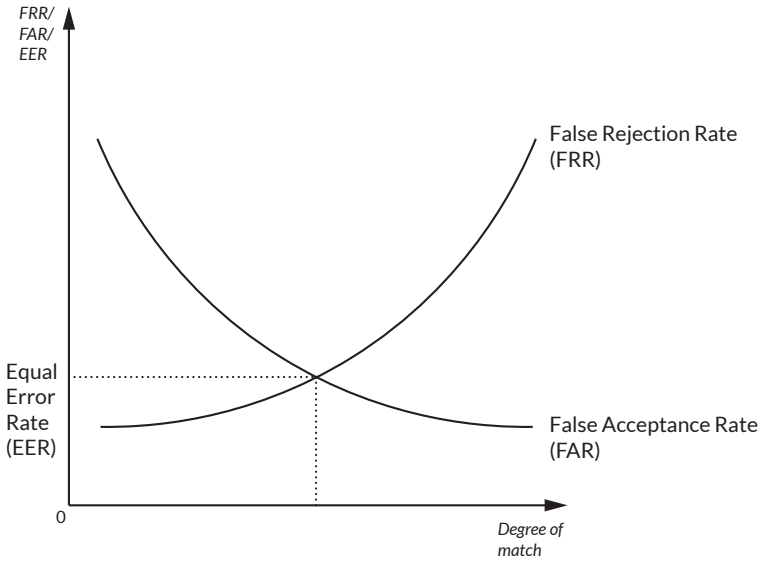


Figure 2 // FRR/FAR Tradeoff

Size of the Reference Storage For government agencies building reference storages for the purpose of identifying a data subject against all templates stored in the reference storage (1-to-N matching), the number of images in the reference storage is negatively correlated with the matching accuracy of an FRT algorithm.[48] Therefore, government agencies need to strategically confront the tradeoff between accuracy and size of the reference storage and potentially prioritize the enrollment of certain data subjects, for example, with a criminal conviction, over others.

02 //

POLICY ANALYSIS FRAMEWORK

02 //

POLICY ANALYSIS FRAMEWORK

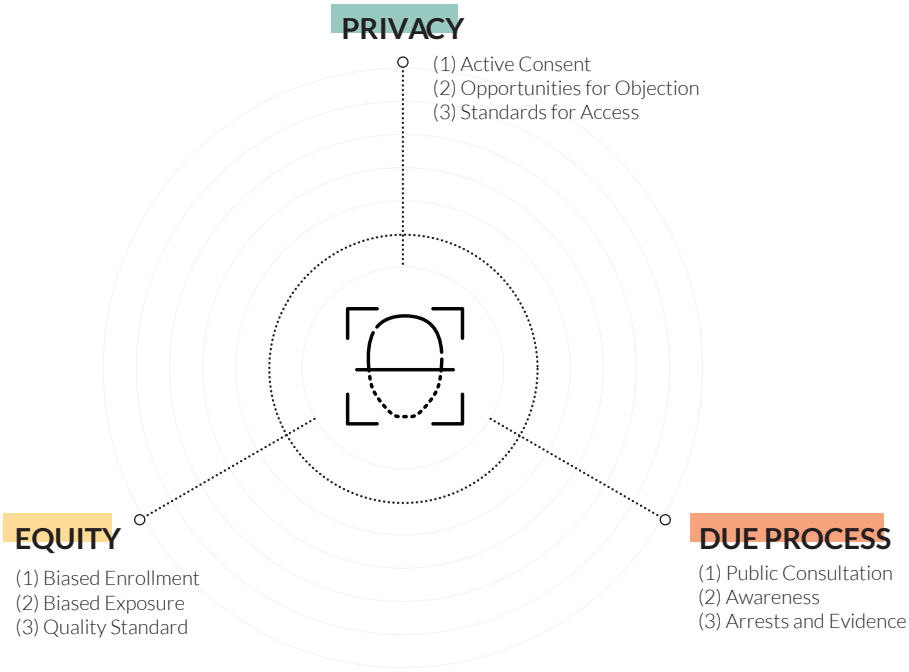


Figure 3 //
Policy Analysis Framework

The following framework allows assessing FRT policies across three dimensions of protected human rights norms: privacy, equity, and due process. The objective of the analysis is not to make a judgment or recommendation on the appropriate context of use for FRT, which should be determined in democratic discourse and the legislative process. Rather, the framework acts as guidance to evaluate whether, in the context of any given FRT use, safeguards are in place to protect human rights. For each human right or dimension, three sub-variables operationalize the broader concept in the context of FRT. The sub-variables are measured on a high-level scale to code observations ranging from the state that offers the least effective protection (1) to the state with the most effective protection (3) based on strategies that are common in the current policy discourse, for example, in policy recommendations or model legislation such as proposed by Garvie et al. (2016).[10] For each case study, the cumulative score attained in each category (additive, 1-9) is then plotted in a radar chart visualization.

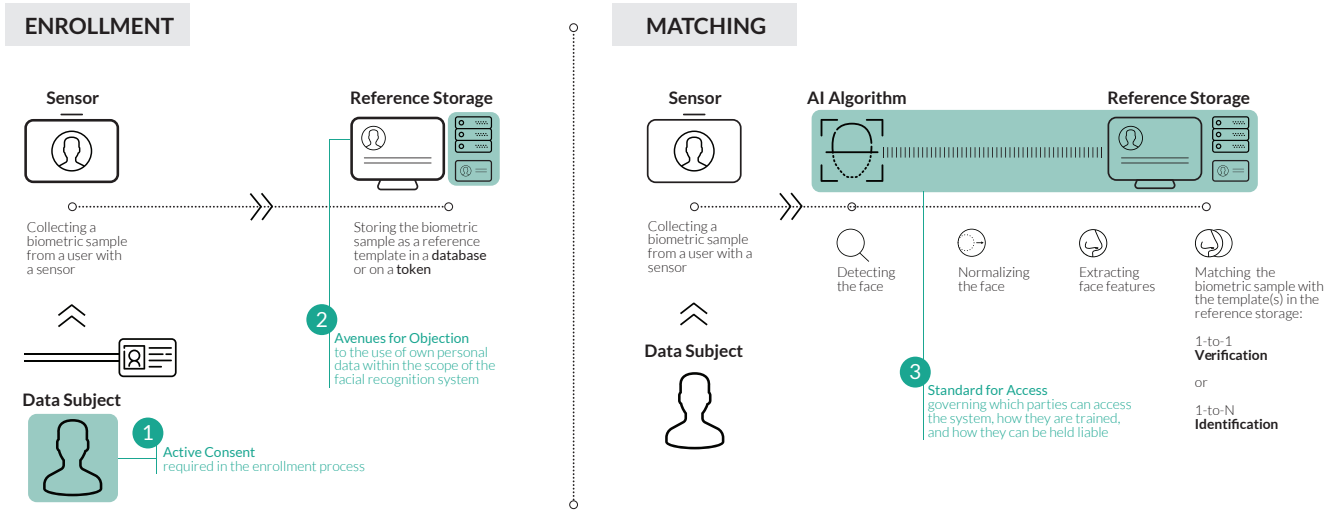


Figure 4 // Privacy Issues in FRT

PRIVACY

Article 17 ICCPR

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
2. *Everyone has the right to the protection of the law against such interference or attacks.*

The right to privacy is internationally recognized in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[49] Despite its status as a fundamental right, definitions of privacy in the academic and legal discourse have evolved continuously with technological advancements,[50] and was recently argued to be an essentially contested concept.[51] For the purpose of this analysis of FRT, policies are considered privacy enhancing if they allow individuals to make informed decisions on the level of exposure they are comfortable with given their preference for privacy. The right to privacy as guaranteed in Art. 17 ICCPR may conflict with other rights, which is why it is not an absolute but a qualified right, a right that inherently allows for the permissible restriction of the protection to “arbitrary or unlawful” interference.[52–55] Nevertheless, restrictions of the right to privacy must generally be lawful, have a legitimate aim, and be both necessary and proportionate.[55]

Specifically, the analysis will address the following privacy-related issues arising in the context of facial recognition systems: (1) active consent on the part of the data subject, (2) avenues for objection to the use of the data subject's personal data, and (3) the data subject's awareness that their biometric sample is being collected for matching purposes.

1 | Active Consent

Is active consent required for enrollment in a database used for the identification of individuals using FRT?

In comparison to capturing other biometric traits, using a camera as a sensor has advantages and disadvantages. On the one hand, cameras offer the advantage of being commonplace, cheap, contactless, and allow for identifying persons in proximity or at a distance, even if the data subject is not able to identify themselves, for example, due to limitations based on age or physical disabilities.[32,56] On the other hand, biometric samples can be collected overtly or covertly without the data subject's active consent. For example, the data subject may knowingly and voluntarily present herself with a biometric passport at a border, or unknowingly and without explicit consent have her image captured by a security camera. Facial images as biometric samples are particularly risky because they can be collected at a distance or repurposed from the use the data subject actively consented to.[32,57]

Both enrollment in training and testing data sets by private and public sector actors may prove problematic. On the one hand, training datasets, for example, IBM repurposed almost a million photos shared by users of the social media platform Flickr to train its facial recognition algorithms without effectively informed consent.[58] On the public sector side, practices by the National Institute of Standards and Technology (NIST), a government agency tasked among others with maintaining the Facial Recognition Vendor Testing (FRVT) program, the predominant validation system for facial recognition vendors to demonstrate the performance of their algorithms to private and public sector clients, were heavily criticized. To construct the vast datasets employed to assess the algorithms' performance, including the main dataset of 26.6 million portrait photos of 12.3 million individuals, NIST included the images of particularly vulnerable populations without their active consent, including abused children, visa applicants, deceased arrestees, and individuals booked on suspicion of criminal activity.[59] On the other hand, concerns arise related to the enrollment of individuals into the real-life testing datasets used by law enforcement agencies. Such public sector reference storage databases regularly include images of data

subjects who did not voluntarily provide their active consent. For example, in the US, the Federal Bureau of Investigation (FBI) has access to booking photo, as well as driver's license and ID photos.[10]

2 | Avenues for Objection

Are there meaningful options for individuals to object to the use of their data in the facial recognition system?

Given that FRT is among the least intrusive biometric matching technologies and that a facial image can be enrolled as a template in the reference storage without the knowledge of the data subject, only policy protections can ensure that the data subject can access their FRT data and object to its use. To this end, the data subject must be aware of the use of their data in an FRT system and an effective path must exist for the data voice their objection to the use and management of their data by the data controller. Where a formal de jure right exists, it is important to evaluate whether there is a de facto meaningful option for the data subject. For this determination a combination of the effective communication of the right (i.e., is only the legal community aware of it or does it feature prominently in outreach materials about the FRT use?), administrative obstacles (i.e., is a simple or involved process required to exercise the right which would place a burden on the data subject?), and, where available, information on how many data subjects regularly exercise their rights.

3 | Standard for Access

What are the standards for access (cause, training, liability, etc.) an entity must meet to gain access to the FRT data?

The users of FRT are the stewards of the system and the data included in or linked to the reference storage of facial images used as biometric FRT templates. Facial images capture a generally immutable and continuously publicly exposed personal trait, which means that linking them with other personally identifiable information creates a highly sensitive combination of personal data.[60] For this reason, the EU's GDPR, for example, considers biometric data a "special category of personal data" (Article 9 GDPR)[27] that merits more elevated standards of protection. To account for the sensitive nature of FRT data, policy strategies should place requirements on data controllers that are specific to the use of FRT and go beyond the protections in place for the processing of personal data in general. In the absence of policy intervention, granting access to FRT data would occur solely at

the discretion of the data controller. Ideally, such specific regulations may include who the data can be shared with, legitimate causes for sharing the data, administrative processes data sharing must comply with, and the legal obligations of data sub-stewards including training requirements and legal liability.

PRIVACY

Active Consent	Avenues for Objection	Standard for Access
1 No active consent required.	**1** There are no avenues for objection.	**1** Information is shared based solely on the discretion of the organization.
2 Active consent required from persons whose right to privacy is not potentially in conflict with other fundamental rights (e.g. images from convicted criminals).	**2** Individuals can effectively inquire about whether their face is part of an FRT reference storage which could allow them to object.	**2** Information is shared based solely on the discretion of the organization and in compliance with data protection legislation.
3 Active consent required from all persons.	**3** There is an effective and well-communicated avenue to object to data governance.	**3** Information is shared based on compliance with protocols established specifically for the sharing of sensitive FRT information.

Table 1 // Privacy Coding Table

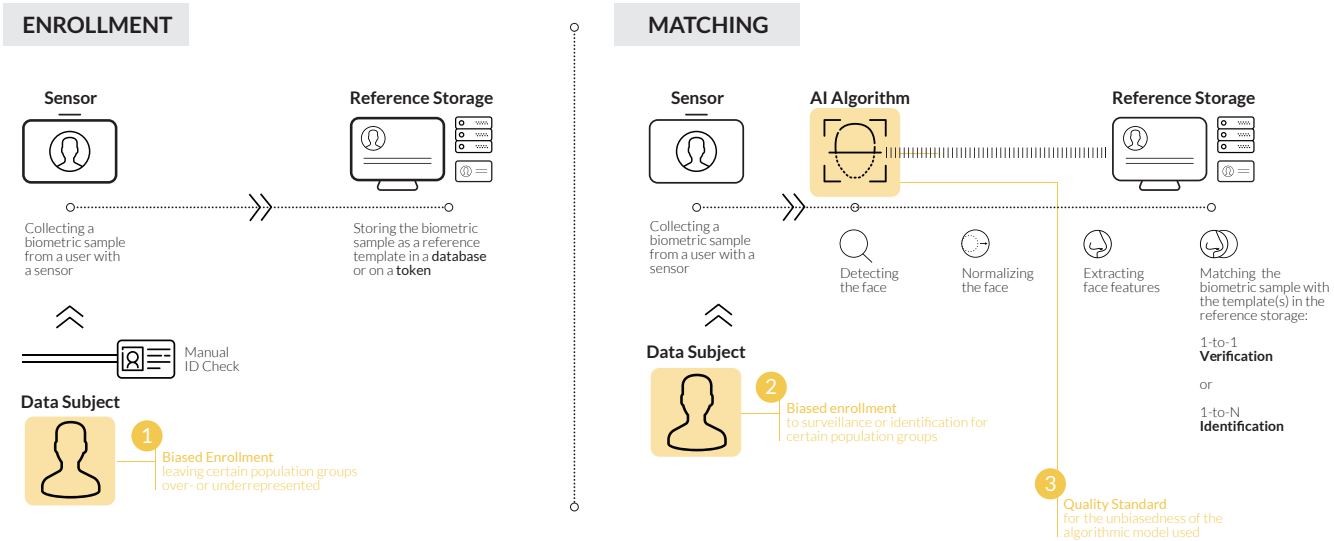


Figure 5 // Equity Issues in FRT

EQUITY

Article 26 ICCPR

> *All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*

Under the equity criterion, the analysis evaluates whether the benefits and risks of FRT equally affect different population groups. Policies around AI-enabled FRT must be measured against the standard of affording equal protection of the law and ensuring non-discrimination in accordance with Article 26 ICCPR.[49] Importantly, the ICCPR does not prohibit all distinctions in state action but allows for differentiation along "objective and reasonable criteria based on factual or legal distinctions," for which the burden of proof lies with the government.[61]

1 | Biased Enrollment

Are certain groups more or less likely to be enrolled and therefore over- or underrepresented in a database used for identification via FRT?

The operator of FRT technology must necessarily make choices on the enrollment of data subjects in the reference storage within the framework of existing policies. There are generally three options for enrollment practices. Firstly, the FRT operator can use a data collection specific to the purpose of acting as a reference storage for FRT. For example, databases of biometric passport photos are unambiguously used as FRT reference storages. Secondly, the FRT operator can use a data collection for which the main purpose is not the use as an FRT reference storage. For example, booking photo or driver's license image databases are databases not originally and explicitly intended to serve as FRT reference storages. Thirdly, the FRT operator can create a custom data collection drawing on various data collections to which they have access to create an FRT reference storage. For example, event-specific watchlists have been created and used by public[62] and private[63] entities.

Depending on the FRT operators enrollment practice, the probability of being enrolled in the system may be biased against populations with certain protected characteristics (i.e., any status enumerated in Article 26 ICCPR[49]) or unprotected characteristics (e.g., criminal history). Especially the exercise of discretion by the FRT operator by using a reference storage that was not intended to be used with FRT in its creation and custom reference storages elevate the risk of bias. For example, a collection of booking photos as reference storage necessarily reflects any existing bias in policing practices, for example, over-policing of ethnic minority communities.[62] Similarly, custom reference storages reflect implicit or explicit bias in the choices of the FRT operator, for example, against individuals with mental health challenges.[62]

A higher probability of being enrolled in the FRT reference storage may negatively impact individuals who are being enrolled, as well as individuals sharing their characteristics who are not being enrolled, who are more likely to be misidentified and forced to interact with law enforcement. In general, more templates in the reference storage, i.e. the testing dataset, imply more distractors leading to the FRT algorithm performing with lower accuracy.[64] Therefore, overrepresentation in the refernce storage or testing dataset leads to a higher chance of misidentification, which places a burden on individuals who have to prove that they have been misidentified.[65] Policies should mandate FRT operators to explicitly address any bias in the enrollment into FRT reference storage and prohibit biased practices unless

the FRT provider can provide a legitimate justification based on a tradeoff with other societal goods, i.e. "objective and reasonable criteria based on factual or legal distinctions."[61]

2 | Biased Exposure

Are certain groups more likely to be exposed to surveillance and identification via facial recognition?

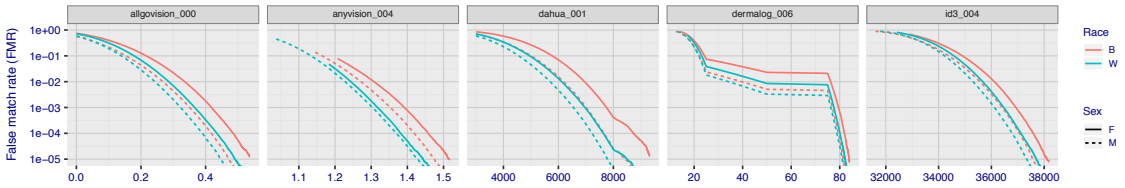
In addition to bias in enrollment, FRT systems may suffer from biased exposure, including both the physical presence of surveillance equipment using FRT and the algorithmic identification of a data subject. Firstly, the placement of surveillance equipment or sensors in the form of mobile camera vans, closed-circuit television (CCTV) cameras, or body-worn cameras may be prejudiced against certain communities[66] or attendants of certain events.[67] Secondly, the performance of FRT algorithms with respect to population groups who differ in their physical appearance is related to the representation of each group in the training data set used by the FRT developer, which is beyond the control of the FRT operator. However, the FRT operator bears responsibility for employing FRT software that is biased in its performance. Klare et al. (2012) describe the problem as "if a system was predominantly trained on white faces, and later operated on black faces, the learned representation may discard information useful for discerning black faces."[68] In a sense, FRT mirrors the deficits in human recognition capabilities in this regard as humans, who perform better at recognizing faces from their own racial group in comparison with other racial groups, well-documented as the "other-race-effect."[69–71] In their study, Klare et al. (2012) find consistently lower matching accuracies for female, black, and young data subjects in the age group 18-30.[68] Moreover, Buolamwini et al. (2018) find that the FRT software evaluated have an up to around 20% higher error rate for female faces and darker-skinned faces respectively and an up to 34.7% higher error rate for darker-skinned and female faces.[72] Phillips et al. (2009) report that in their comparison, an algorithm developed by Western engineers "recognized Caucasian faces more accurately than East Asian faces and the East Asian algorithm recognized East Asian faces more accurately than Caucasian faces."[73] Jennifer Lynch highlights that being misidentified as a false positive match places a burden on the individual because they have to prove that they were misidentified, which can have a severe impact on the individual's life.[74,75]

3 | Quality Standard

Is there a quality standard for the unbiasedness of the algorithm employed?

FRT algorithms vary by developer in their performance across demographic groups. To date, certain developers achieve nearly identical performance across race and gender whereas others lag behind. The most recent 2019 NIST FRVT 1-to-1 Identification Report (Figure 6) illustrates the discrepancies: The algorithm developed by the China Electronics Import-Export Corporation ("ceiec") performs equally well for females and males regardless of race whereas the algorithm developed by Aware has much higher false match rates for black individuals than for white and for females relative to males.[76] To prevent a disparate impact from the use of FRT on certain population groups, bias should be explicitly addressed and monitored and policies should require a quality standard for the unbiasedness of the FRT algorithm in the procurement process.

Figure 6 // Sex and Race Effects for Mugshot Images (Source: NIST (2019))



EQUITY

Biased Enrollment	Biased Exposure	Quality Standard
1 Population groups differing based on a protected category "such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status" (Article 26 ICCPR) are treated unequally.	**1** Population groups differing based on a protected category "such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status" (Article 26 ICCPR) are treated unequally.	**1** There is no regard for differential performance of FRT based on demographic differences.
2 Population groups differing based on a non-protected category such as criminal background are treated unequally.	**2** Population groups differing based on a non-protected category such as criminal background are treated unequally.	**2** FRT may exhibit differential performance based on demographic differences but it is critically addressed and monitored.
3 All individuals are treated equally.	**3** All individuals are treated equally.	**3** FRT exhibits no differential performance based on demographic differences.

Table 2 // Equity Coding Table

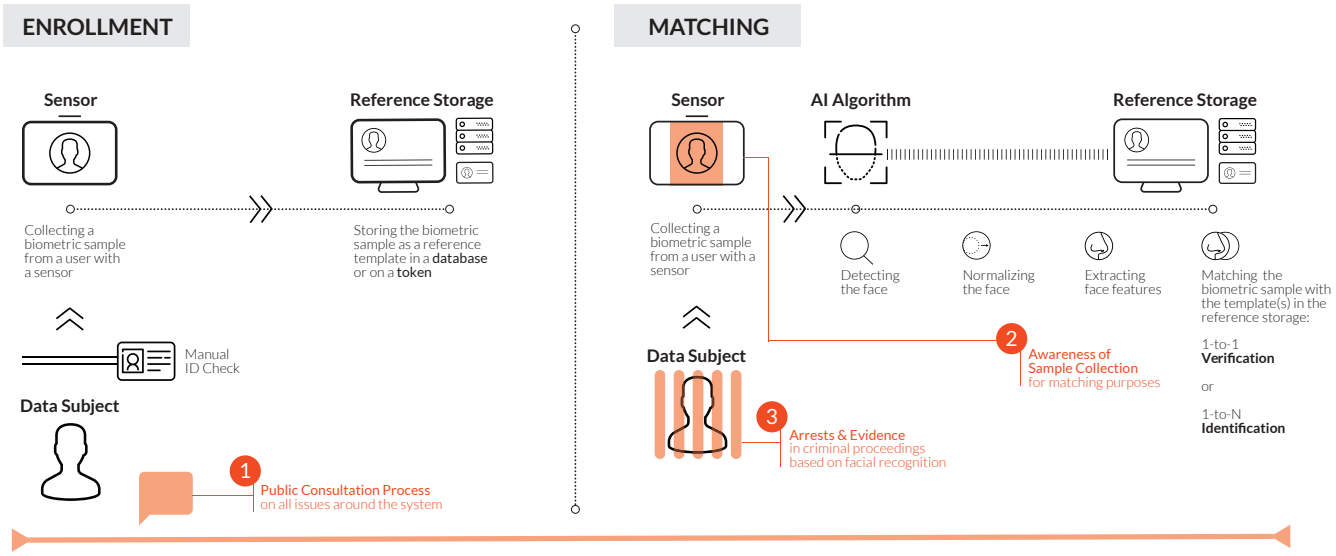


Figure 7 // Due Process Issues in FRT

DUE PROCESS

Article 9 ICCPR

1. *Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law. (...)*

Article 14 ICCPR

1. *All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. (...) Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law. (...)*

To the degree to which facial recognition is used in law enforcement, related policies must ensure the respect of the right to liberty and due process as recognized in Articles 9 and 14 ICCPR.[49] Both rights account for the possibility of limitations, for example, in the case of the right to liberty for arrests that are not "arbitrary" but "on such grounds and in accordance with such procedure as are established by law."[49]

1 | Public Consultation Process

Was there a public consultation process in designing the facial recognition system?

The use of FRT raises a number of ethical issues and tradeoffs from concerns around privacy and non-discrimination rights to a legitimate interest in public safety, that can only be resolved in public discourse. For this reason, it is imperative that both policies around and deployments of FRT are subject to a preliminary public consultation process that is effectively inclusive of any societal perspective. Ideally, a public consultation process should incorporate insights from organized stakeholder representatives, for example, representatives from multiple academic disciplines and representatives of diverse civil society organizations, and the general public. Policies can set a mandatory framework for public consultation processes that requires including stakeholder representatives and a public comment period or venue that is effectively advertised to the public.

2 | Awareness of Sample Collection

Are individuals made aware when their face is recorded for the purpose of identification using facial recognition?

FRT allows for non-intrusive and overt capture of a biometric sample, a facial image, not only for the purposes of enrollment but also for the purposes of matching. Technological breakthroughs which improve the capability to recognize data subjects from images with less and less information exacerbate this privacy concern. For example, NEC, a Japanese multinational information technology company, announced the technological capability to collect additional information on the data subject's appearance beyond the face, which may be collected from multiple cameras, to recognize persons whose face is partially concealed even when the images are taken at a side angle or from behind. [77] Therefore, it is necessary that the policy framework affords protections to the data subject. Most importantly, the FRT policy must clearly require that members of the public who move in a space subject to surveillance with FRT capability are effectively made aware of FRT use. Effective communication should include announcements via multiple channels. Notices could be published, for example, via announcements on the agency's website and across media channels before the deployment of FRT and via accessible signage and where possible personal outreach during the use of live FRT sensors.

3 | Arrests & Evidence

Can an individual be arrested on the basis of identification via facial recognition? To which extent can identification relying on facial recognition be used and challenged as evidence in court?

FRT is improving rapidly but will continue to provide system operators with matching rates of less than 100%, which means that no matching process can deliver an absolute, unambiguous result. For this reason, it is necessary that the policy framework accounts for technological inaccuracy and protects each individual's fundamental rights through procedural safeguards. FRT policies should prohibit that FRT matching rates in themselves can lead to legal consequences such as arrest or use as evidence in court. Instead, policies should require a two-step combination of machine and human matching for any use of FRT that can have a legal or other significant effect on the individual that is clearly transparent to all stakeholders, in particular in the context of judicial proceedings.

DUE PROCESS

Public Consultation	Awareness	Evidence
1 There was neither a stakeholder consultation process nor a public comment period.	**1** There is no communication that a sample is collected for the purposes of use in conjunction with FRT.	**1** There is no two-step process featuring human review of FRT matches before they develop legal consequences for the subject as evidence.
2 There was either a stakeholder consultation process or a public comment period.	**2** There is at least one form of communication that a sample is collected for the purposes of use in conjunction with FRT.	**2** There is a two-step process featuring human review but it is intransparent to the stakeholders involved in the criminal process (e.g. arrestee/defendant, police staff, defense attorney, jury, judge).
3 There was both a stakeholder consultation process and a public comment period.	**3** There are multiple forms of communication that a sample is collected for the purposes of use in conjunction with FRT.	**3** There is a two-step process featuring human review and it is fully transparent to the stakeholders involved in the criminal process (e.g. arrestee/defendant, police staff, defense attorney, jury, judge).

Table 3 // Due Process Coding Table

03 //
CASE STUDIES

03 //
CASE STUDIES

UNITED KINGDOM

Use Cases

In the UK, facial recognition technology was first deployed in trials by the London Metropolitan Police, the South Wales Police, the Leicestershire Police, and the Humberside Police.[62,78–80]

The earliest reports on the use of FRT in public date back to a trial of the Visionics FaceId system starting in 1998 in London's Newham borough although it was ineffective in detecting persons of interest according to the responsible Detective Inspector.[81] The Metropolitan Police[82] conducted a series of 10 trials testing FRT at large-scale public events (e.g. the Notting Hill Carnival) and transportation infrastructure between August 2016 and February 2019. Upon conclusion of its trials, the Metropolitan Police launched a "full independent evaluation" by the National Physical Laboratory and an independently assigned academic institute expected to conclude in April 2019.[83–85] The Metropolitan Police uses non-live FRT for general booking photo searches of approximately 2.9 million images through software provided by the vendor Safran Morpho, now Idemia, and live FRT through the NeoFace software developed by NEC.[83,85–87] In the practical deployment of live FRT, the police force follows a two-step process: Firstly, the software scans facial images, compares them against a "watch list" (selected images from the reference storage), and alerts the attending officer of a match. Secondly, the officer compares the camera and the watch list image before deciding whether to stop the individual.[83]

The South Wales Police deployed FRT 39 times since May 2017 at soccer games, racing events, concerts, and a royal visit supported by a £2.6 million government grant.[62] In total, 39 arrests have been informed by identification using FRT.[88] The South Wales Police frames its use of FRT as two functionalities, "Identify", a 'slow-time' application which compares still images of unknown persons of interest, against a database of circa 500,000 booking photos from South Wales and Gwent (the reference storage), and "Locate", a 'live-time' application which compares live camera feeds of faces against a predetermined event-specific watchlist of typically between 500 – 700 images.[89,90] The South Wales Police also deploy FRT NeoFace software developed by NEC.[91] In practice, the FRT also alerts the operator to a match who then manually compares the facial images.[92] The South Wales Police was criticized because they reported that 2,451 or 91% of their matches over a 12-month period were false positive identifications. As the reason for the high FAR, the South Wales Police states the fact that 2,297 of the matches resulted from their trial during the Union of European Football Associations (UEFA) Champions League final due to low image quality in the watchlist.[62]

The Leicestershire Police maintains a license for FRT software, began a six-month trial in 2014,[60,62] and deployed live FRT technology in a public space in one test at a festival in 2015, which led neither to stops nor arrests.[93] The Leicestershire Police's watchlist included both their 92,000 booking photos and images provided by Interpol.[62] The FRT software used, like other police departments, was developed by NEC. Moreover, the Leicestershire Police allows businesses wishing to report a crime to upload CCTV footage to an online reporting tool, a cloud-based platform that uses FRT to identify suspects provided by Facewatch, a private company.[94,95] The contract between the Leicestershire Police and Facewatch runs from September 2014 to 2019.[96]

No information on FRT use was disclosed by the Humberside Police on their website[97] and only a brief mention appeared in the August 2018 Force Management Statement Summary.[98]

Regulatory Policies

National Level

Researchers have criticized that FRT use in the UK has been operating in a legal vacuum.[62] Nick Hurd MP (Minister of State for Policing, for the Home Office) stated that "there is no legislation regulating the use of CCTV cameras with facial recognition".[67] The Home Office concedes that the current legislative and regulatory guidance on FRT use is insufficient as "policing in England and Wales do not have common standards for the capture, storage or exchange of facial image data."[18] The most generally applicable legal frameworks are human rights principles and the 2018 Data Protection Act,[99] which includes protections for the general processing of personal data. Moreover, data protection standards for the use of FRT in law enforcement are codified in the 1984 Police and Criminal Evidence Act (PACE), the Code of Practice on the Management of Police Information (MOPI), and guidance set out in the College of Policing's Authorised Professional Practice (APP). The PACE Act[100] determines the scope to which police are allowed to take and use biometric data. Passed in 1984, the PACE Act provides general protections for the purposes of and practical processing of biometric data; however, the law fails to account for the specificity of newly developed FRT technologies. Even the more recent revisions of the PACE Codes of Practice, in particular, the revised PACE Code D, the Code of Practice for the identification of persons by Police Officers most recently published in February 2017 failed to discuss specific challenges related to the use of FRT.[101] Also applicable is the Home Office's 2013 Surveillance Camera Code of Practice,[102,103] which lays down 12 general principles of practice, and the Information Commissioner's Office's Code of Practice for Surveillance Cameras.[103] The Home Office's Code mandates that "any use of facial recognition (...) systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated" and that adverse decisions must involve human intervention, which is seconded by the Information Commissioner's Code.[102] Additionally, the Biometrics and Forensics Ethics Group (BFEG), which is responsible for the governance of FRT use in law enforcement,[18] published a set of broader ethical principles.[104] Regulatory oversight is exercised by the Information Commissioner's Office and the Surveillance Camera Commissioner's Codes of Practice, and the Biometrics Commissioner.[18] In its entirety, researchers have criticized that the piecemeal legal framework negatively impacts the foreseeability and accessibility of FRT policy.[62]

To fill the legal vacuum and develop an effective and cohesive future policy strategy, the Home Office published its 2018 Biometrics Strategy.* As part of the strategy, the Home Office is planning to establish a new oversight and advisory board tasked with producing policy and oversight solutions for law enforcement's use of facial images and facial recognition systems. The goal in establishing a new body is to coordinate approaches by police, the Home Office, the Surveillance Camera Commissioner, the Biometrics Commissioner, the Information Commissioner, and the Forensic Science Regulator, and BFEG. Moreover, the Home Office is planning to expand the use of Data Protection Impact Assessments (DPIAs) for new applications of new or existing biometric technologies "inviting scrutiny from an independent ethics panel, regulators and commissioners,"[18] coordinated by the new oversight and advisory board for law enforcement and Home Office Data Board for immigration use. The overarching goal is to create effective and transparent policies or policy recommendations around the use, retention, and deletion of images.[18]

EU Level

At the EU level, the 2016 GDPR is currently the most prominent legislative act related to the processing of personal data, including biometric facial images. Article 9 GDPR on special categories of personal data prohibits the processing of biometric data, including facial images. The provision provides for ten exclusions, including for use cases where the collection of biometric data is necessary "for reasons of substantial public interest."[27] Furthermore, Article 35 GDPR mandates the use of a DPIA whenever data processing is likely to result in "high risk to the rights and freedoms of natural persons," which includes the use of new technology based on Recital 91 of the preamble and the Article 29 Working Party guidelines.[105] Articles 16, 17, and 21 GDPR furthermore grant the rights to rectification, erasure, and objection of personal data.[27] Nevertheless, the European Parliamentary Research Service (EPRS) emphasizes that the scope and interpretation of many clauses in the GDPR remains to be operationalized through legal challenges and emerging jurisprudence by the European Court of Justice.[106] Moreover, the 2016 Data Protection Directive specifically outlines principles for the processing of data by law enforcement agencies in criminal matters, which does not include more substantive guidance on FRT technology.[107] At present, there is no more comprehensive legislation on the use of FRT at EU level.

---

* Big Brother Watch criticized the government for publishing its Biometrics Strategy five years after its promised publication showing a lack of concern for the severity of the issue.

Policy Design Choices

Privacy

Active Consent The South Wales Police watchlists include images of individuals with outstanding warrants, suspects for offenses in the area, and individuals previously arrested at a certain event.[108] The Metropolitan Police state that images that may be included in their watchlist include booking photos, as well as images taken by the police or the Fixated Threat Assessment Centre, a joint police/mental health unit, with the knowledge of the individual.[109] With regard to booking photos, the Metropolitan Police argues in their Privacy Impact Assessment that the right to privacy in Article 8(1) European Convention on Human Rights (ECHR) provides "limited protection to the criminal and it is not intended to bar lawful and proportionate law enforcement activities." The South Wales Police similarly emphasizes in their Privacy Impact Assessment that the right to privacy guaranteed in Article 8(1) ECHR is a limited right.[110] However, the custody imaging database presently includes both images of convicted criminals and individuals taken into custody but not convicted. Individuals who were not convicted have the right to take the initiative to apply for deletion of their image and the police retain the image if there is an exceptional reason.[19] According to research by the Press Association, the number of such deletion requests (up to October 2017) was small at 67 with 14 refusals.[19] Moreover, Big Brother Watch criticized that no police force was able to state how many innocent individuals feature in the custody imaging database.[67] This data retention policy the Home Office conceded upholds a lower standard than the more advanced systems storing DNA and fingerprints data.[19] To remedy the situation, the Home Office committed to linking booking photos to conviction outcomes to facilitate their deletion in the future.[18] Moreover, the Metropolitan Police was criticized for including individuals with mental health challenges who are "fixated" on public figures but not wanted for a particular offense in their Remembrance Sunday 2017 trial.[62] Overall, researchers furthermore criticized that for the purpose of creating watch lists, there is "no legal prohibition on police forces taking images from the internet or public facing social media."[62] Moreover, there is no indication that any of the individuals in the reference storage have been specifically made aware that their images are being used in FRT trials.*

The private company Facewatch proclaims that it holds the "only shared national facial recognition watchlist."[95] The watchlist is composed of indi-

* No such information is included in the Fair Processing Notice.

viduals Facewatch refers to as Subjects of Interest (SOIs). Both businesses who acquire the services of Facewatch's FRT tool for surveillance of their retail space and the police contribute images and basic data (date of the offense or suspected offense, picture of the SOI face, SOI name if known, short summary of what happened) on individuals "reasonably suspected to have committed crime or disorder." Facewatch considers that confirming the authenticity of this information provided by third parties with a disclaimer effectively deters the parties from submitting erroneous or malicious information. Moreover, Facewatch itself augments this watchlist with images posted on police websites and on the Crimestoppers website. Facewatch explicitly states that it cannot ask for the consent of the individuals because it "would prejudice the purposes of the processing."[112]

Avenues for Objection With regard to biometric data processing, individuals have the right to access their data under the provisions of GDPR and the Data Protection Act 2018. Aside from an access request, individuals have the option to file a complaint regarding the processing of data by a data controller with the Information Commissioner's Office.[99] Facewatch also offers members of the public a specific tool to submit a Subject Access Request on their website to obtain information on whether they are featured on the Facewatch watchlist after providing proof of identity and potentially a photo.[113]

Standards for Access The Metropolitan and South Wales Police* system deletes all images captured immediately, except for facial images matching the watch list, which are stored for 30 days.[83-89] The Leicestershire Police maintained none of the data generated as part of the FRT and did not operate with an explicit policy governing who is able to view positive or false matches from the FRT test.[114] The Metropolitan Police is ambiguous in its statements on access to the recorded images, stating in one Freedom of Information (FOI) request that only police officers and staff assigned to the live FRT deployment have access to the recorded footage and alert images[115] and in another that such images are shared with other police forces.[85] In the Privacy Impact Assessment, the Metropolitan Police note that there is "no intention of the [Metropolitan Police] to provide wide access to this data corporately."[116] Moreover, in their Privacy Notice on the handling of personal data in general, the Metropolitan Police reserves the right to share data with other law enforcement agencies, both nationally and internationally, partner agencies working on crime reduction and prevention initiatives, and other bodies such as the press, service providers, employ-

* The South Wales Police maintains a data sharing agreement with the Universities Police Science Institute attached to the University of South Wales.

ers, voluntary sector organisations, financial institutions, and regulatory bodies. However, the Metropolitan Police qualifies that all personal data including data relevant to FRT is handled in compliance with the 2018 Data Protection Act and the EU GDPR and disclosures are always "necessary and proportionate" and on a case-by-case basis. Furthermore, the Privacy Notice highlights that data is shared, in addition to discretionary data sharing, "when required to (...) by, or under, any act of legislation, by any rule of law, and by court order."[117]

Facewatch states with regard to data retention that "every incident is deleted from our live system after a maximum of 24 months and is then backed up for 30 days (but not available to data subjects) after which it is permanently deleted." Furthermore, Facewatch proclaims that the company will not share "personal data with third-parties nor will we transfer it out of the EU."[118] However, in an extended privacy notice, Facewatch specifies a more detailed list of parties with access to its watchlists, which are "only available to businesses (...) and to police forces and crime prevention organisations which have entered into legal agreements with (Facewatch)."[112]

Equity

Biased Enrollment In 2017 to 2018, black individuals were three times more likely to be arrested in the UK than white individuals.[119] Researchers criticize that given the over-policing of minority communities and the use of booking photos in FRT watchlists, the enrollment process for law enforcement use is thus biased against ethnic minorities.[62] Moreover, the fact that both individuals convicted of a crime and not convicted of a crime are included on watchlists creates a discriminatory impact on individuals who have unwarrantedly been taken into custody by police. The Metropolitan Police was furthermore subject to criticism for their inclusion of "fixated individuals", referring to individuals known to be fixated on public figures, in their Remembrance Day 2017 trial, which biased their enrollment practice against individuals with mental health conditions.[62]

Biased Exposure Based on the most recent edition of the NIST 1-to-1 FRVT, a series started in 2017, Idemia's algorithms exhibit substantial demographic differences in the false match rates, which are higher for black than for white individuals, and higher for females than for males (see Figure 8).[76] In 2010, NEC's algorithms, in general, have performed reasonably well in comparison to other FRT vendors in terms of the difference in accuracy between races and gender, but perform substantially on older subjects.[120] The specific NEC NeoFace FRT in use by police departments has not been

tested for bias based on demographic characteristics[121] and no information is available on the performance of the system in use by Facewatch.

Quality Standard Big Brother Watch criticizes police departments for not publishing detailed information on FRT performance relative to protected categories such as gender, race, and age.[62] In response to a FOI question on gender or racial bias in the FRT software, the Metropolitan Police refers to the assessment of the US National Institute of Standards and Technology that 1:N systems are "largely untested for demographic effects".[122] The South Wales Police merely stated in response to inquiries regarding gender or racial bias that in their 18 months of deployment no bias became evident without providing evidence or documentation.[89]

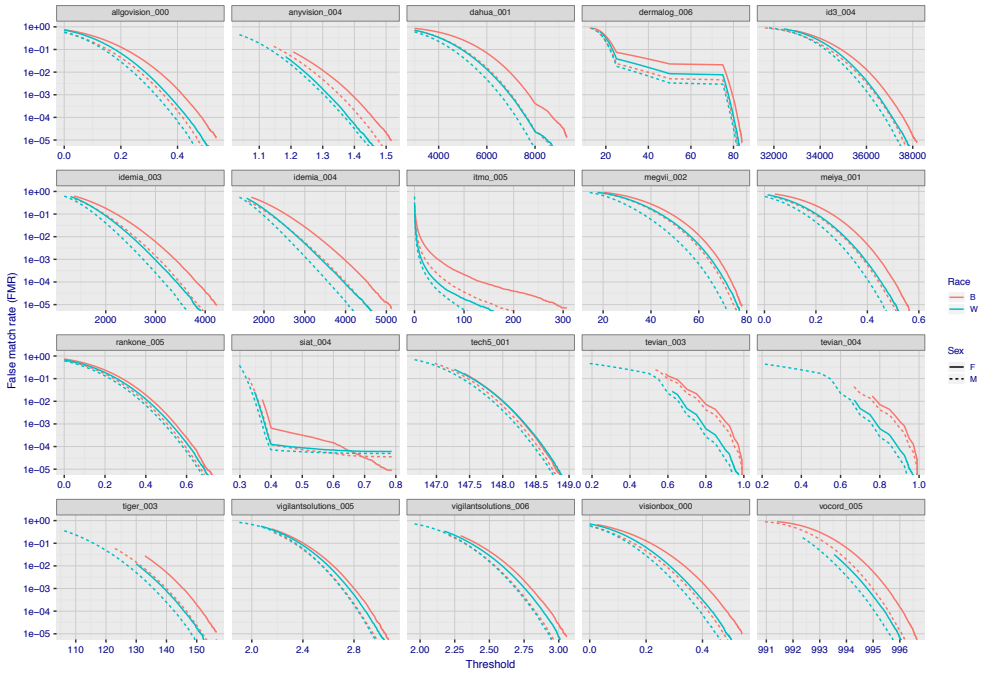


Figure 8 // False Match Rates for various FRT algorithms (Source: NIST (2019))

Due Process

Public Consultation Process FOI requests to the Metropolitan Police reveal that the procedure preceding the FRT trial included a consultation with the Biometrics Commissioner, Surveillance Camera Commissioner, Information Commissioner and via liaison the non-profit organization Big Brother Watch, and the completion of a Privacy Impact Assessment (PIA) in April 2017.[115,123] Moreover, the Metropolitan Police invites sporadic feedback from the public on the FRT trials through a link on the leaflets distributed at FRT sites.[116] The South Wales Police has and continues to consult at least 13 stakeholders in the process of its FRT deployments, including government agencies such as the Information Commissioner's Office, the Surveillance Camera Commissioner, the Biometrics Commissioner, and the Home Office, an academic institute, and various police departments or organizations.[110] However, the South Wales Police does not reference inviting feedback from the public and in its Privacy Impact Assessment states that public consultation for the "Locate" functionality is difficult because it is deployed at "high risk, high profile" events.[110] Accompanying the use of FRT by the South Wales Police, ethical issues were discussed in five South Wales Police Independent Ethics Committee meetings, in which both police officers and independent members of the committee participate.[124,125] Furthermore, the South Wales Police sought advice from the Surveillance Camera Commissioner's Advisory Counsel held in May 2018 with representatives from Liberty and Big Brother Watch.[90] The Leicestershire Police did not conduct a Privacy Impact Assessment.[114] Overall, none of the police departments published information on an opportunity for the general public to comment on the plans for the trials during a public comment period before the beginning of the trials.

Awareness of Sample Collection The Metropolitan Police notifies the public of FRT trials via announcements through the news section on its website,[126] information leaflets handed out to the public, posters placed in and around the FRT trial site, and officer engagement with the public at the FRT trial site.[83] However, the Privacy Impact Assessment raises concerns as to whether the signage was always explicit with regard to the fact that FRT was used - example language included in the impact assessment refers only to "Police Operation - Cameras in Use".[116] Furthermore, the Metropolitan Police proclaims that "Anyone can refuse to be scanned; it's not an offence or considered 'obstruction' to actively avoid being scanned".[83] However, media reports state that individuals have been stopped and fined for covering their face to avoid scanning during the Metropolitan Police trials.[127] The South Wales Police notifies the public of live FRT use via announcements on its social media channels and signage at the FRT deployment site.[89] With regard to the opportunity to object to scanning, the South

Wales Police states that “avoidance of [...] cameras in isolation does not in itself constitute grounds for search or arrest”.[89] Members of the public entering a space subject to Facewatch surveillance will be alerted to the use of the system by signage as the company states.[118]

Arrests & Evidence To the author’s knowledge, there are no court cases in which the transparent use of FRT in a two-step technical human review process have been the subject of concern.

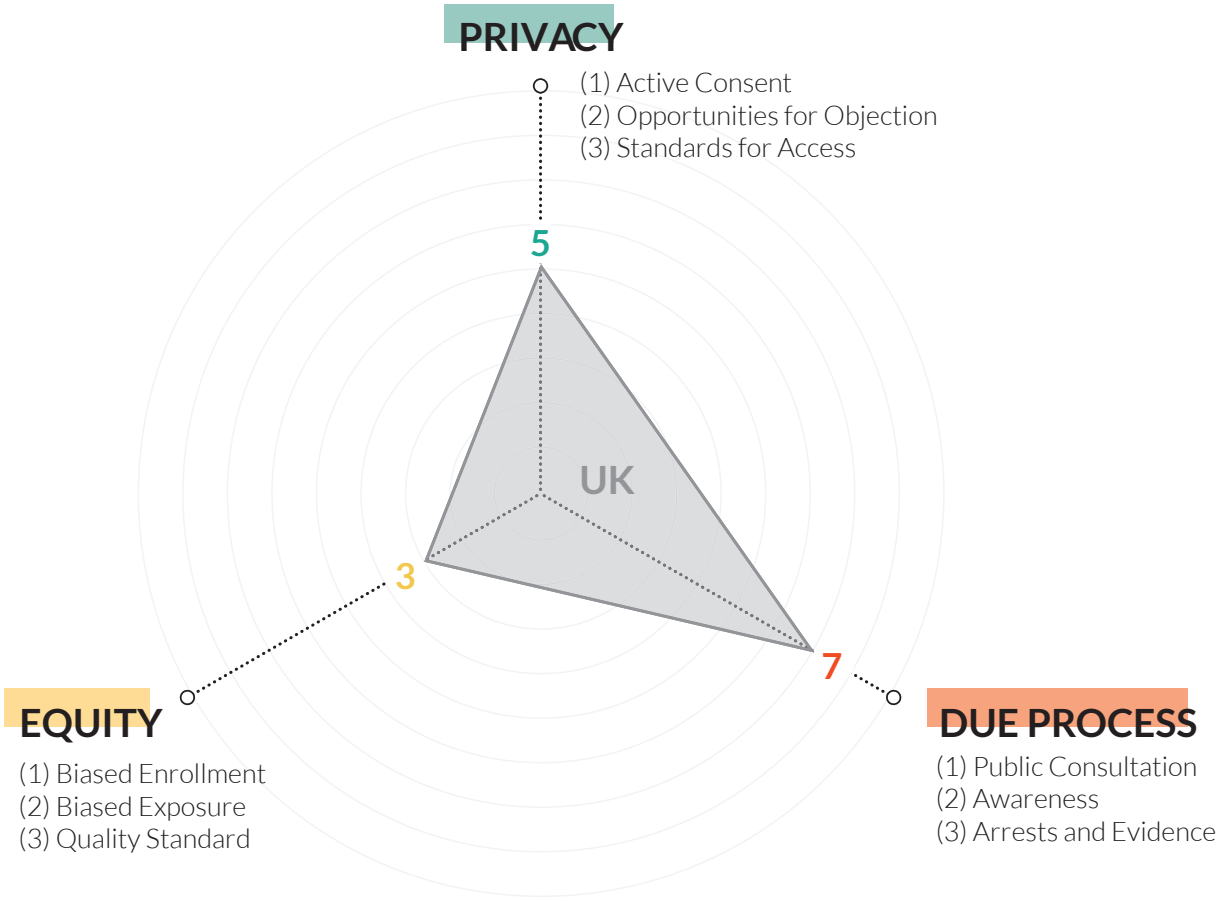


Figure 9 // UK Policy Framework Scoring

PRIVACY

Active Consent	Avenues for Objection	Standard for Access
1 **No active consent required.** Both watchlists held by police and the private company Facewatch include templates obtained from individuals who did not explicitly and actively consent to being included in an FRT reference storage because their image is a booking photo, uploaded by a business based on their CCTV footage. Booking photos remain included even for individuals not charged with or convicted if a crime unless they apply for removal.	**2** **Individuals can effectively inquire about whether their face is part of an FRT reference storage which could allow them to object.** All systems surveyed include a path to request information about the inclusion of one's data on an FRT watchlist, via an FOI request in the case of watchlists maintained by public institutions and via a Subject Access Request with Facewatch. However, no institution clearly publicizes a path to remove one's data from such watchlists.	**2** **Information is shared based solely on the discretion of the organization and in compliance with data protection legislation.** Information sharing occurs largely based on the discretion of the police forces within the framework of the Data Protection Act 2018 and the GDPR.

EQUITY

Biased Enrollment	Biased Exposure	Quality Standard
1 **Population groups differing based on a protected category (Article 26 ICCPR) are treated unequally.** FRT policy did not prohibit the enrollment of individuals based on their mental health condition.	**1** **Population groups differing based on a protected category (Article 26 ICCPR) are treated unequally.** Based on the bias in policing practices and the enrollment process due to the inclusion of booking photos an overrepresentation of images of individuals from overpoliced ethnic minorities, are at a higher risk of (mis-)identification.	**1** **There is no regard for differential performance of FRT based on demographic differences.** None of the police forces trialing FRT have publicly addressed potential bias in the software employed.

DUE PROCESS

Public Consultation	Awareness	Evidence
2 **There was either a stakeholder consultation process or a public comment period.** Police forces conducted only a formal consultation process of stakeholders, not the general public.	**2** **There is at least one form of communication that a sample is collected for the purposes of use in conjunction with FRT.** At least in one application case, the Facewatch tool, individuals are only apprised of the use of FRT via one channel of communication, signage in the area. The most advanced FRT deployments by police departments, however, feature at least two outreach methods.	**3** **There is a two-step process featuring human review and it is fully transparent to the stakeholders involved in the criminal process (e.g. arrestee/defendant, police staff, defense attorney, jury, judge).** There are no known incidents of arrests or FRT identifications being used as evidence in court.

Table 4 // UK Policy Framework Scoring

United States

Use Cases

Federal Level

The FBI's Criminal Justice Information Services (CJIS) Division, the FBI's largest division, began building the Next Generation Identification (NGI) database which for the first time included FRT in the form of the Interstate Photo System (IPS) at a cost of around $1.2 million in 2010.[65,128] The NGI-IPS system was piloted in 2012 and became fully operational in 2014.[129,130] The NGI-IPS contains three categories of photos: criminal booking photos, civil photos submitted as part of background checks or state licensing requirements,[74] and probe photos connected to a felony investigation that did not produce a candidate for matching which the submitting law enforcement agency wishes to retain in the system's Unsolved Photo File (UPF). UPF photos are retained while the criminal investigation to which they are connected remains active, which the contributor must verify after a year. Mugshot images are automatically searched against the UPF.[131] Authorized law enforcement users can search the database of around 51 million criminal booking photos and additionally request a search against the UPF.[65,132,133] Law enforcement users are not permitted to search against the collection of civil photos.[131] In 2016, the NGI-IPS contained around 84% criminal and 16% non-criminal photos.[10] The FBI uses FRT systems developed by the Microsoft Azure web services suite and the NEC Integra ID 5 biometric solution software which offer facial recognition capabilities and has run pilots with Amazon Web Services' Rekognition software according to media reports.[134]

The FBI states that searches with a "probe" photo against the NGI-IPS firstly produce a ranking of potential matches with the caveat that "the response should only be used as an investigative lead".[129] In a second step, the results are further investigated for positive identification.[65] Furthermore, the NGI-IPS allows text-based search for certain biographic or demographic characteristics including sex, race, age, and hair color, which is intended to help create photo lineups.[131] The photos that are part of the NGI-IPS have a standard retention period until "subjects attain 110 years of age or seven years after notification of death with biometric confirmation".[131] According to the FBI, in 2017, 11 states were connected to the NGI.[135] Regarding the overall accuracy of FRT searches against the NGI-IPS, the FBI states that

a "correct candidate [is returned] a minimum of 85 percent of the time* within the top 50 candidates."[135] However, the Government Accountability Office (GAO) criticizes the FBI's accuracy standard pointing out that in the practical application, investigators often only generate "the top handful of images".[65] The critique moreover states that the FBI does not test its false positive rates, which hinder investigative efficiency.[65] Additionally, the Electronic Frontier Foundation (EFF) warns that the median quality of photos included in the NGI-IPS database is "well below" the necessary quality for maintaining adequate FRT accuracy.[65] Finally, the GAO criticizes that accuracy tests apply to FRT used by the FBI and not external partners searching against its database.[65]

The FBI CJIS has operated a Facial Analysis, Comparison, and Evaluation (FACE) Services Unit since 2011, which provides investigative support by comparing "probe" photos against federal and state databases, with potential access to over 411 million images, which include criminal booking, visa, driver's license, and ID photos.[10,135],** The FACE Units FRT network in 2016 contained around 8% criminal, 80% non-criminal, and 12% photos for which the classification is unknown.[10] For this purpose, the FBI entered into memorandums of understanding that allow it to access photo databases of currently at least 18 states.[65,136] After entering a probe photo into the system generating a list of possible candidates, the FACE unit in a second step "generally confirms with the record owner[5] that the record is valid and active and requests permission to disseminate the information"[137], and provides a photo of the most likely candidate to the investigating staff for further analysis before deleting all other photos.[65] In the first four years of the FACE units deployment, it employed FRT for 214,920 searches of which only 4% produced likely matches.[10]

The Department of Justice (DOJ) through its research, development, and evaluation agency the National Institute of Justice (NIJ) supported a project with the objective to develop binoculars with integrated FRT capabilities for law enforcement purposes in cooperation with the vendor StereoVision Imaging, Inc. with $1.4 million between 2010 and 2012.[129,138]

Furthermore, the U.S. Secret Service (USSS) published a PIA in November 2018 announcing an FRT pilot to test the technology as part of an enhanced security architecture around the White House complex with volun-

---

* Currently the FBI FRT's accuracy is at 86% for a match within the 50 top candidates.

** FBI's NGI, other federal databases (e.g., Department of State's Visa Photo File, Department of Defense's Automated Biometric Identification System, Department of State's Passport Photo File), and state photo repositories (e.g., select state Departments of Motor Vehicles)

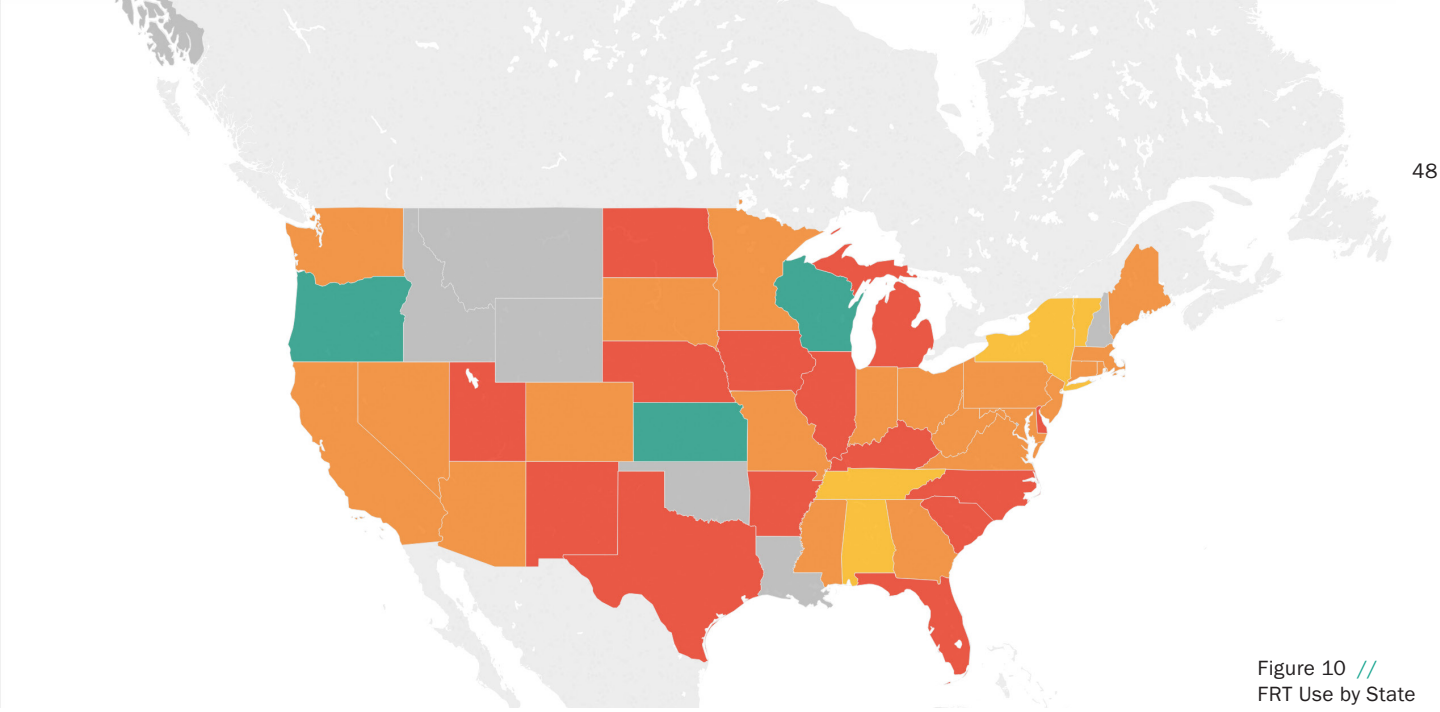


Figure 10 //
FRT Use by State

40
States provide or have provided federal, state, and/or local law enforcement agencies access to FRT databases

14
States provide or have provided access to the FBI **and** state or local law enforcement agencies

22
States provide or have provided access **only** to state or local law enforcement agencies

4
States provide or have provided access **only** to the FBI

3
States provide or have provided access **only** to the DMV

teer employees.[139]

State & Local Level

At least 40 states use or have used FRT either within their driver's license administration or for the purposes of law enforcement in the context of criminal investigations or corrections facilities (see Appendix).[10,140] At least 26 or 65% of these states that use FRT allow law enforcement searches against driver's license or ID photo databases.[10] In addition to the FBI, some state and local jurisdictions open their FRT systems to a number of other federal agencies, including the Department of Defense, the Drug Enforcement Administration, Immigration and Customs Enforcement, the Internal Revenue Service, the Social Security Administration, the U.S. Air Force Office of Special Investigations, and the U.S. Marshals Service.[10] State and local jurisdictions vary in the rate at which they make use of their FRT capabilities with a range of around 350 to 8,000 searches per month.[10] Moreover, in at least 36 states, state or local law enforcement agencies have run or actively run FRT searches.[10] 29 state and local jurisdictions limit their FRT searches to the context of stops, arrests, and investigations in which a probe photo is compared against a booking photo database.[10] Another 19 agencies in eight states allow and expand such FRT search activity to the driver's license and ID databases which they have access to.[10] Moreover, at least 5 state or local law enforcement agencies made plans to establish real-time live FRT capabilities including the Los Angeles Police Department, which claims to have such a system in use.[10] Jurisdictions vary substantially in the requirements for accuracy they establish in the FRT procurement process ranging from no requirements, for example, in Los Angeles County or Ohio, to a specific set of minimum thresholds and required documentation, for example, in San Francisco.[10]

The following three case studies highlight the variety of FRT use practices at the state, county, and city level:

State Level: Florida

Florida maintains the Face Analysis Comparison & Examination System (FACES), an FRT network which 243 state, local, and federal law enforcement agencies have access to.[10,141,142] The FACES system was initiated and continues to be hosted as one of the first FRT systems nationwide in 2001 by the Pinellas County Sheriff's Office (PCSO).[10,141,143] The number of searches run against the system, recorded at almost 8,000 searches per month in 2016, places the FACES system at the top end of the spectrum across the nation.[10] Jennifer Lynch, a privacy advocate with the EFF who testified twice in congressional hearings on facial recognition technology, states that the FACES system is "the most advanced face recognition system of any state in the country" and describes it as "the longest-running and most robust."[144] Included in the FACES system are over 11 million law enforcement and 22 million Florida driver's license and ID photos.[10,142] To run searches against its extensive database, the FACES system used to employ software developed by Viisage and now switched to the use of MorphoTrust's FRT software.[10,145] Moreover, Tampa, FL, drew criticism for a month-long public trial of FRT software at the 2001 Super Bowl and with around 36 cameras as part of the infrastructure in the Ybor City district.[146–149] The FRT used was provided by Visionics Corporation free of charge for a year.[149]

County Level: Maricopa County

Among the earlier adopters, the Maricopa County Sheriff's Office (MCSO) began using FRT in 2006 according to public records requests.[10,150] Media reports suggest that pilot programs started as early as 2002 for use in jails and schools for the purpose of missing children investigations, which was heavily criticized by the American Civil Liberties Union (ACLU).[151,152] The MCSO actively enrolls individuals booked into jail into the FRT-searchable database.[153] In addition to a total of at least 3.2 million Arizona booking photos and 1.5 million booking photos from the DOJ's Federal Joint Automated Booking System, the FRT database contains at least 14.5 million driver's license photos as every Arizona driver who is issued a driver's li-

cense is automatically enrolled.[10] Additionally, in 2007, the MCSO obtained booking photos and all driver's license photos from the Honduran government, a major source country of immigration to Arizona,[154] which were subsequently enrolled in the FRT database.[10*] An internal MCSO memo states that the "Honduran Federal Police have advised that they will also attempt to secure at least the criminal booking records of the other Central American nations of El Salvador, Nicaragua, and Guatemala."[150,158] In exchange, the Maricopa Chief Deputy County Attorney who pledged $60,000** in addition to MCSO funds for the expansion of the Arizona and the construction of a Honduran FRT unit.[150] Moreover, according to a practice notice, "the FBI, [Department of Homeland Security] DHS, the US Marshals Service, and several other federal agencies contributed photographs from the various criminal most wanted lists that they maintain."[159] In compiling the FRT database, MCSO has cooperated with the Arizona Counter-Terrorism Information Center (ACTIC).[159] Public records requests and media reports reveal that initially, the FRT in use by the MCSO was provided by Hummingbird Defense Systems, potentially donated free of charge for pilots, but the records do not confirm which system is currently in use.[10,151,160] The software and algorithm employed by Hummingbird Defense Systems were, to the author's knowledge, never evaluated by NIST and are reported to perform at a level far below the standards set by competitors[160] and were described as very difficult to use effectively by the MCSO staff.[161] An internal memo states that in the first four years of the FRT system's operation resulted in only around 15 to 20 identifications.[161] To operate its FRT system, the MCSO maintains a Facial Recognition Unit similar to the FBI's FACE Unit, that is specifically tasked with running FRT searches upon request, review the results, and with supervisor approval return leads to investigators.[10]

City Level: Seattle

The Seattle Police Department (PD) launched its FRT system, the Booking Photo Comparison Software (BPCS), in 2014 in cooperation with South Sound 911, a local intergovernmental organization connecting five 911 agencies.[10,162] The collective FRT database contains at least 350,000

* Then Maricopa County Sheriff Joe Arpaio gained notoriety due to his extreme positions on law enforcement and immigration. His leadership of the MCSO resulted in a 2011 DOJ investigation concluding that Maricopa County shows the worst pattern of racial discrimination by law enforcement in US history and his 2017 conviction for contempt of court for refusing to follow court orders to stop racial profiling practices for hwhich he was later pardoned by President Donald Trump.

** The funding was stated to be derived from grants awarded under the Racketeering Influenced and Corrupt Organizations Act (RICO).

booking photos from three counties, Snohomish, King, and Pierce, and is accessible to at least eight local law enforcement agencies.[10,163] Underlying the BPCS system's FRT capability is software procured from NEC.[164] For comparisons against the BPCS database, staff download a probe photo into the system, compare it against photos in the database, and "present the images of any possible suspect(s) to the investigating officer/detective."[164] Contracts obtained by researchers showed that South Sound 911 likely purchased a software capable of real-time recognition from live-feed video footage but the Seattle PD has prohibited this application.[10] However, probe photos submitted to the system may include screenshots from video footage captured by body-worn cameras that all front-line Seattle PD police officers are equipped with since 2017.[165] The Seattle PD Police Manual mandates that any data related to such BPCS searches may only be retained for 42 months.[164] Importantly, the Seattle City Council takes an effective interest in the deployment of the system in accordance with societal values and made the FRT program funding conditional on a policy review and approval by the ACLU of Washington.[10] In 2014, after recommending changes to the BPCS use policy, the ACLU of Washington confirmed its approval of the FRT system.[166]

Regulatory Policies

Federal Level

Legislation

The FBI states that its mandate as described in the US Code and the Code of Federal Regulations justifies the activities of its FACE Unit,*[135] and additionally references the USA PATRIOT Act and several executive orders as the legal basis for the operation of the NGI-IPS system.**[131] All federal agencies collecting, using, and storing personal information need to comply with the 1974 Privacy Act and the 2002 E-Government Act.[130] The Privacy Act[167] governs the government use of general systems of records for personal

* The FBI in its privacy impact assessment for the FACE Unit specifically references United States Code (U.S.C) Sections 533 and 534; Title 28, Code of Federal Regulations Section 0.85; Title 42, U.S.C. Section 3771; and Title 18, U.S.C. Chapter 123.

** The FBI in its privacy impact assessment for the NGI-IPS system specifically references 28 U.S.C. §§ 533, 534; 42 U.S.C. § 3771; 44 U.S.C. §3301; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), Executive Orders 8781, 8914, and 10450, 28 CFR 0.85, 20.31, 20.33.

information linking, for example, biometric information with the identity of a person and mandates that the public is informed about the use of such systems via Systems of Records Notices (SORN). However, it only applies to federal agencies and US citizens and permanent residents.[168] Moreover, the Privacy act features a general exemption for criminal law enforcement records.[168] In 2016, the FBI successfully sought a specific exemption for the NGI from the Privacy Act, justified as "necessary to avoid interference with the Department's law enforcement and national security functions and responsibilities of the FBI."[169,170,169,171] Specifically, the rule changes prevent individuals from accessing information pertaining to them in the NGI, for example, to correct erroneous entries.[171] Along with over 100 public comments on the rule change invited by the DOJ,[169,170] 45 organizations rights advocacy and private sector organizations addressed a letter to the DOJ expressed their concern with regard to the proposed exemption and criticize the rule change as "an extraordinarily broad proposal, and the system it affects is extraordinarily sensitive –particularly for the communities it may affect the most."[171] Nevertheless, the proposed rule change came into effect in August 2017.[170,172] More specifically, the 2002 E-Government Act[173] pertains to the management of personal information through information technology and requires that before the procurement or development of new technology, the public must be informed via a PIA.[130] The White House Office of Management and Budget (OMB) oversees enforcement, which has been referenced as "extremely deferential to agencies exercising their powers of exemption."[168]

Furthermore, in the area of regulating identification modalities, which are closely related to issues around FRT, the 1994 Driver's Privacy Protection Act (DPPA) mandates that state departments may only disclose personal information connected to driver's license and ID cards for use "by any government agency, including any court or law enforcement agency, in carrying out its functions." This exception to a general ban on sharing personal information applies especially facial images, which meet DPPA's definition of "highly restricted personal information."[140,174] Moreover, the 2005 REAL ID Act governs the issuance of driver's licenses and ID cards establishing a federal standard for documents that are accepted for "official purposes", including entering federal facilities or boarding commercial aircrafts.[175] Part of the federal minimum standard established in the REAL ID Act is the requirement of a facial image for each application, which prevents states from granting exceptions to individuals with religious objections or physical disabilities, as 32 states have done in the past.[140]

With regard to a future-facing strategy to address the challenges raised by emerging technologies such as AI-enabled FRT, the U.S. House of Representatives Subcommittee on Information Technology of the Committee on

Oversight and Government Reform published a report on the impact of AI on US policy.[176] The policymakers recommend that "federal agencies review federal privacy laws and regulations to determine how they may already apply to AI technologies within their jurisdiction, and, where necessary, update existing regulations to account for the addition of AI.[176] Moreover, the report calls on government agencies to engage in "discussions on how to identify bias in the use of AI systems, how best to eliminate bias through technology, and how to account for bias."[176] Two bills pertaining to the use of FRT by government agencies have been introduced in Congress and are currently in committee. In November 2017, Rep. Eleanor Norton (D-DC) introduced the Federal Police Camera and Accountability Act of 2018 (H.R.7156) which was last referred to the House Committee on the Judiciary. The bill would create a mandate for body and dashboard cameras but prohibit the use of FRT for these cameras and only allow the use of FRT on video footage with a specific warrant or court order.[177] In January 2019, Rep. Steve Cohen (D-TN) introduced the Police CAMERA Act of 2019 (H.R.120), which would allow DOJ grantmaking for the purchase of body cameras and place limitations on the use of FRT in conjunction with such cameras, and was referred to the Subcommittee on Crime, Terrorism, and Homeland Security.[178]

Jurisprudence

To date, no judicial case has addressed how fundamental rights protections apply to the use of FRT and the new risks it creates. While legal research highlights that at the federal level, there exists no explicit right to privacy in the US,[179] the Fourth Amendment to the US Constitution provides the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[180] Jurisprudence has yet to establish if certain use cases of FRT by government agencies constitute a "search" and whether that search is to be considered "unreasonable."[179] A series of cases have established case law around issues that are tangential to FRT and delimit the space in which jurisprudence on the use of FRT in law enforcement will likely develop:

Katz v. US (1967)[181] In the case, the question at issue was whether an external wiretap on a public pay phone constitutes a search protected by the Fourth Amendment. Justice Harlan introduced the concept of a "reasonable expectation of privacy" that may exist even with no intrusion into physical space, and that a violation which constitutes unconstitutional "search and seizure" under the Fourth Amendment, "which protects "people, not places."[181]

Terry v. Ohio (1968)[182] In deciding whether a stop-and-frisk search on the street is in violation of the Fourth Amendment, the US Supreme Court held that a reasonable suspicion of past, present, or future criminal activity suffices to justify the search under the Fourth Amendment.[182]

United States v. Dionisio (1973)[183] In Dionisio, the US Supreme Court decided whether a grand jury subpoena for the production of voice exemplars violates Fourth Amendment rights. In its decision against such a violation, the court stated that "like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."[183]

US v. Knotts (1983)[184] Knotts addressed the question of whether a tracking beeper installed on an item sold to an individual violates their Fourth Amendment rights. The US Supreme Court held that there can be no reasonable expectation of privacy for movements in public* that would be visible to an observer, and that "nothing in the Fourth Amendment prohibited the police from augmenting their sensory faculties with such enhancement as science and technology afforded them in this case."[184]

Kyllo v. United States (2001)[186] The US Supreme Court in Kyllo deliberated whether using a thermal imaging device to detect heat signatures emanating from a private home is in violation of the Fourth Amendment. The court held that for government use of devices "not in general public use," gaining information on the home "that would previously have been unknowable without physical intrusion" constitutes a search.[186]

Hiibel v. Sixth Judicial District Court (2004)[187] In Hiibel, the US Supreme Court addressed whether the refusal to identify oneself to a police officer is protected by the Fourth and Fifth Amendment, the right to refrain from self-incrimination. The court's holding affirms that demanding to identify oneself upon reasonable suspicion of criminal conduct is minimally intrusive and does not violate Fourth Amendment rights.[187,188]

Illinois v. Caballes (2005)[189] Caballes required the US Supreme Court to address the question of whether reasonable suspicion is necessary for a canine sniff during a routine traffic stop to be constitutional under the Fourth Amendment. The court held that a legitimate interest in privacy was not at risk because a canine sniff could only reveal illegal substances.[189]

---

* In the court's argument, the distinction between public and private space is key as their US v. Karo (1984) decision highlights, in which a beeper was installed in a private home. Similarly, the US Supreme Court held in several cases that aerial surveillance of what a private citizen could see from air space does not constitute a Fourth Amendment violation. The US Tenth Circuit Court held this arguments for surveillance cameras mounted on poles covering an area visible to passersby.

US v. Jones (2012)[190] In US v. Jones, the US Supreme Court discussed whether a GPS tracking device installed in a car is a Fourth Amendment search. In speaking for the majority, Justice Scalia affirmed that placing the GPS tracker constituted trespass and in combination with gathering information on the car's location, a Fourth Amendment search.[191]

Maryland v. King (2013)[192] The US Supreme Court in Maryland v. King debated whether collecting DNA samples from individuals arrested for but not convicted of serious crimes was in violation of the Fourth Amendment. The court held that "analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."

Carpenter v. US (2018)[193] At issue in Carpenter was the question whether obtaining cell phone records revealing location and movements of an individual violates the Fourth Amendment. According to the US Supreme Court's holding, analyzing cell phone records constitutes a search because while an individual may be aware of the fact that a third party maintains such records, the information is not affirmatively disclosed.[193] Amendment prohibited the police from augmenting their sensory faculties with such enhancement as science and technology afforded them in this case."[184]

Current case law therefore gives indications for characteristics of intervention that are critical to the question whether or not the activity is in violation of the Fourth Amendment, including whether the information collected was in a public or private space, on a single movement or all movements over an extended timeframe, or how intrusive the collection of information was. However, in a 2012 hearing on FRT in front of the Senate Judiciary Committee, Sen Al Franken highlighted one of the underlying conundrums in applying Fourth Amendment case law to FRT: "Current Fourth Amendment case law generally says that we have no reasonable expectation of privacy in what we voluntarily expose to the public; yet we can hardly leave our houses in the morning without exposing our faces to the public."[129]

Policies

In 2016, researchers found that of a sample of 52 government agencies using FRT, only 10% had a publicly available use policy.[10] In 2017, with a grant from the DOJ's Bureau of Justice Assistance and DHS, "state, local, and federal law enforcement, privacy, and criminal justice partners, practitioners, and subject-matter experts" in a Face Recognition Policy Group have developed a policy template with best practices for the use of FRT in

law enforcement absent regulation.[56] In its structure, the template broadly adheres to the internationally recognized Fair Information Practice Principles (FIPPs), as formulated by the DHS.[56] The template emphasizes the importance of an FRT use policy as part of an "ongoing entity privacy program cycle."[56] Stages of the cycle include (1) raising awareness for and (2) assessing risks to privacy, civil rights, and civil liberties, (3) creating a policy, (4) evaluate the policy in a community engagement process, (5) train personnel, (6) conduct an annual review, and (7) audit the FRT system.[56] The template strongly encourages agencies to make their FRT policy available to the public.[56] Moreover, the recommended language in the template extends the FRT policy to third parties, establishes training requirements and accountability for governance and oversight, and procedures to ensure the protection of data against security breaches.[56] With regard to the deployment of mobile FRT in public, the group and template take the position that "the individual has no reasonable expectation of privacy."[56] Moreover, the policy template recommends specifying a policy for disclosure or corrections requests and for the retention of FRT-related information.[56]

State & Local Level

Beyond the federal level, states and local jurisdictions may elevate the standard of rights protections if they so choose. Some states grant an explicit right to privacy, including California (California Constitution Art. I §1),[194] Florida (Florida Constitution Art. I §23),[195] and Montana (Montana Constitution Art. II §10),[196] and less than a third of states have own privacy laws.[179] In 24 states, "stop and identify" laws require lawfully detained individuals to identify themselves.[140] At present, however, no state has passed comprehensive legislation regulating the governmental use of facial recognition technology (see Appendix). Wisconsin has prohibited the use of driver's license and ID photos from the DMV database in a photo lineup or array (WI Stat Ann § 343.237 & 165.8287 (2018)).[197,198] Legislation specific to the use of body-worn cameras effectively banning the use of FRT on body-worn camera footage has been enacted in two states,* New Hampshire (NH Rev Stat § 105-D:2 (2016))[201] and Oregon (OR Rev Stat § 133.741 (2017)).[202,203] Moreover, Maine (ME Rev Stat 25 § 4501 (2015))[204] and Vermont (VT Stat Ann 20 § 4622 (2018))[205] restrict the use of FRT in drones. Michigan (MI Compiled Laws Section 28.243 (2018))[206] mandates that biometric data is destroyed for individuals not charged or found innocent. Moreover, in four states lawmakers introduced bills on the use of FRT by law enforcement agencies**:

---

* Three states, Illinois, Texas, and Washington have passed Biometric Information Privacy Legislation which is, however, only applicable to commercial applications.[199,200]

** Related bills that are currently discussed include proposals to regulate the use of FRT

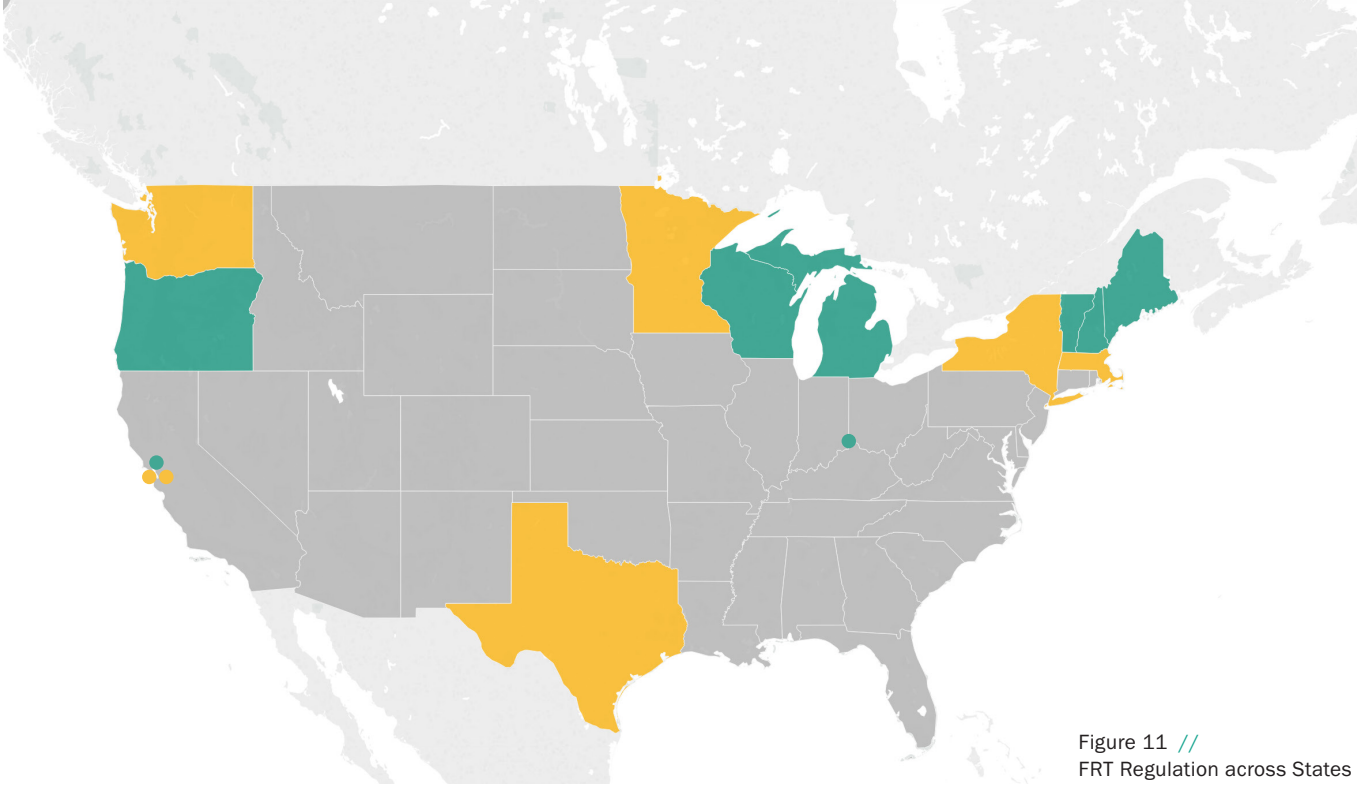


Figure 11 //
FRT Regulation across States

6
States have passed legislation regulating the use of FRT by law enforcement agencies

5
States are debating legislation regulating the use of FRT by law enforcement agencies in the state legislature

Comprehensive Bills In Massachusetts, S 1385 would ban FRT without statutory authorization.[214] New York legislators are debating Assembly Bill A1692, which would ban FRT without legal authorization issued by a court of competent jurisdiction.[215] Texas' Senate Bill SB 485 would require a warrant, arrest or proximity to the national border for law enforcement agencies to collect biometric identifiers.[216] In Washington, Senate Bill SB 5376 and SB 5528 address the issue of regulating FRT more comprehensively. Senate Bill SB 5376 would establish protections for personal data, including prohibiting the use of FRT by government agencies for surveillance in public spaces except for law enforcement or in an emergency and with an analysis by the Office of Privacy and Data Protection.[217] SB 5528 would more specifically prohibit the government use of an FRT system.[218] Michigan furthermore operates FRT with a policy safeguards against misuse and their policy of removing anyone who hasn't been convicted of a crime from an FRT database.[65]

Body-Worn Camera Bills and Drone Camera Bills In California Assembly Bill AB 1215[219] and in Massachusetts House Bill HB 2120[220] would prohibit the use of FRT in connection with officer cameras. Moreover, Massachusetts (SB 1447),[221] New York (A 4030),[222] and Minnesota (SF 1430)[223] debate prohibiting the use of FRT in drones.

---

or collection of biometric information by schools in New York (A 6787)[205] and Missouri (HB 783),[206] or private parties such as retailers or employers in California (AB 1281),[207] Connecticut (HB 5333),[208] New Hampshire (HB 536),[209] and Oregon (SB 284).[210] Moreover, Washington is considering wide-ranging legislation on automated decision making (HB 1655).[211]

Transparency Bills Massachusetts legislators are currently debating Senate Bill SB 1429 that would require the Department of Motor Vehicles (DMV) to post notices at all driver licensing offices, make written information available, and provide information on the department web site regarding investigative or law enforcement officers' searches of driver's license and ID photos through targeted FRT.[224] Moreover, Vermont in House Bill H470 considers requiring specific authorization from the General Assembly prior to law enforcement using technology such as FRT.[225]

At the local level, cities have moved faster on the issue of regulating FRT than states. In California, Berkeley has passed the 2018 Surveillance Technology Use and Community Safety Ordinance mandates that the purchase of surveillance technology including FRT requires approval by the city council.[226] Similarly, San Francisco and Oakland are in the process of passing laws regulating the use of FRT. San Francisco's Stop Secret Surveillance Ordinance, which is about to be passed, places restrictions on the collection and use of biometric data by city departments and bans the use of FRT.[227–230] Oakland, a similar ban on the use of FRT passed the city's Privacy Commission and is now transferred to the Public Safety Committee and the Oakland City Council.[231] Moreover, Cincinnati has a policy banning the use of FRT on stored body-worn camera footage, with no explicit provisions for live video, however,[232] and Seattle made funding for FRT use in law enforcement conditional on approval by the ACLU.[10]

Policy Design Choices

Privacy

Active Consent For an individual to give active consent the individual must have (1) received notice of an intervention and (2), given that notice, consented to their involvement in the intervention. FRT systems in use by law enforcement agencies in the US include both criminal images, such as booking photos, and non-criminal or civil images, such as driver's license or ID photos. In the US, booking photos are subject to limited data privacy protections: In 49 states, booking photos are part of the public record and even the reposting of other individuals' booking photos is generally considered protected by the right to freedom of speech under the first amendment.[233–235] However, while an argument may be constructed that in balancing the public interest and the privacy rights of convicted criminals these privacy rights may reasonably be limited, it is important to emphasize that booking photos include a substantial number of images of individuals

who were arrested but not found guilty of any offense.[236] Only the Michigan State Police deletes booking photos for individuals not charged with or convicted of a crime.[10] EFF's Jennifer Lynch states that at the federal level, "at least 50 percent of FBI's arrest records fail to include information on the final disposition of the case—whether a person was convicted, acquitted, or if charges against them were dropped."[65] It is problematic that the fact that an individual is arrested, which is highly related to policing practices and may be found to be unwarranted at later stages in the criminal process, creates a risk to the full enjoyment of the individual's privacy rights, for example, in the context of an FRT system. Similarly, individuals registering for a driver's license or ID should in no way be restricted in their exercise of privacy rights. Nlets, a private not for profit interstate justice and public safety network created by the 50 state law enforcement agencies and owned by the States, included a statement in its Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies that raises doubt with regard to the commitment to protecting privacy rights even for civil photos:

> *"Nevertheless, there may be drawbacks to providing the public with notice that facial images will be collected in the field and can be submitted to a state DMV for comparison by a facial recognition system. Such notice may add to the controversy surrounding the REAL ID Act. It may also increase public scrutiny of police-citizen interactions. A notice might also inform the public that long range lens photos might also be used to identify people who have not been detained by law enforcement officers."*[140]

At the agency level, available evidence suggests that effective requirements for active consent for the enrollment of individuals in FRT databases are lacking beginning with a lack of notice to the individual. The FBI states in the privacy impact assessment for the NGI-IPS states that notice is given broadly in the SORN and PIA and specifically in a Privacy Act statement to individuals with civil photo entries but not to individuals with criminal photo entries "because notice is not generally provided to subjects of mugshots" (see Table 5).[131] The FBI's FACE unit also states that no notice is provided to the data subjects because "probe photos are potential subjects, victims, or witnesses of/to federal crimes that have been collected pursuant to authorized FBI investigations."[137]

Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. Further notice will be provided by this PIA.	
X	Yes, notice is provided by other means.	Specify how: Civil applicants whose photos are submitted to NGI will be provided with notice via a Privacy Act statement on a hard copy or electronic form. Notice is also given by the publication of this PIA.

Table 5 //
FBI NGI-IPS Notice Policy I
(Source: FBI (2016))

X	No, notice is not provided.	Specify why not: Individuals in the Criminal Identity Group will not receive additional notice because notice is not generally provided to subjects of mugshots.

Indicate whether and how individuals have the opportunity to decline to provide information.

Moreover, the FBI states that arrested individuals so not have the opportunity to object to the enrollment in the FRT system "because arrested individuals do not have the opportunity to decline mugshots." With regard to individuals in civil photos, the FBI recognizes a right to refuse enrollment, however, the FBI qualifies that the refusal may limit the individual's access to other benefits, for example, when submitting a photo is required for employment or licensing (see Table 6).[131]

Table 6 //
FBI NGI-IPS Notice Policy II
(Source: FBI (2016))

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Civil applicants may decline to submit photos; however, agencies may require photos as a prerequisite for employment and licensing.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Individuals in the Criminal Identity Group cannot decline to submit photos because arrested individuals do not have the opportunity to decline mugshots.

At the state and local level, notice and active consent are similarly problematic. In Florida, for example, the Department of Highway Safety and Motor Vehicles has not provided notice to drivers issued a driver's license that their facial image is automatically enrolled in an FRT network.[141] In Maricopa County, AZ, and Seattle, WA, notice is provided through a policy statement on the website.[153,164] However, in the case of Maricopa County, it is unclear whether the notice was timely at the beginning of the FRT program in 2006 - the current policy number DO-3 from 2011, in which the use of FRT is mentioned supersedes an earlier version of the policy from the year 2000. There is furthermore no evidence that Maricopa County provided notice to Honduran individuals whose images were enrolled in the FRT database in 2007. Seattle, however, has been actively establishing procedures to increase transparency in the handling of personal information in the framework of its Privacy Program. In particular, the city's 2017 Surveillance Ordinance 125376 makes information on surveillance technologies including FRT and the review processes easily accessible to the public.[237,238]

However, even effective notice is only a necessary but not sufficient part of obtaining active consent. The Federal Trade Commission in a hearing before the Senate Judiciary Committee emphasized that data subjects must have a meaningful choice regarding the personal information collected from them, which "at a minimum [...] means [...] that a disclosure has to

be provided very clearly outside the privacy policy."[129] Jurisdictions may require photos not only in the criminal justice process but also in the context of driver's license and ID applications, especially in states complying with the REAL ID Act. Even assuming that an individual received notice, this circumstance may make active consent to FRT the prize for due process rights, as well as the privilege of obtaining an ID, driving, or even voting.[10]

Avenues for Objection No legislative protections safeguard the rights of data subjects to access and correct their personal information because the applicable 1974 Privacy Act applies only to federal agencies and the FBI's NGI-IPS system has been granted a specific exemption. Therefore, rights to object to the governance of personal data are currently largely subject to agency policies. The FBI provides a procedure for individuals to access their personal information under the Freedom of Information Act, and correct information under the Code of Federal Regulations (28 C.F.R. part 16, subpart D) pursuant to the Privacy Act. The procedural steps involve an application directly to the agency that contributed the questioned information, either directly or forwarded by the FBI's CJIS Division, requesting that agency to verify or correct the challenged entry. However, verification or correction does not necessarily imply that individuals can object to the use of their data for FRT purposes. Moreover, biometrics in the FBI's NGI-IPS "may be removed from NGI earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction."[131] At the state and local level, it may be possible for an individual, depending on the context of their situation, to seek an expungement of their criminal record pursuant to state law.[239]

Standards for Access Given the lack of more comprehensive regulation, the number and type of agencies granted access to FRT systems varies by jurisdiction (see Appendix). The FBI's exemption of the NGI-IPS system from the Privacy Act includes the requirement to use of FRT has been exempt from the states the following general information sharing policy for NGI-IPS: "Criminal Identity face and SMT photos will also be shared with federal, local, state, tribal, foreign, international, and joint agencies for criminal justice initiatives and national security matters as permitted by federal and state statutes, federal and state executive orders, or regulation or order by the Attorney General" (see Table 7).[131] Moreover, the FBI emphasizes that "agencies requesting and receiving photos [from the IPS] will be subject to training and audit requirements by the applicable CJIS Systems Agency (CSA) and periodic FBI audits.[131] In particular, "agencies requesting and receiving biometric identifications will be trained by the CJIS Systems Agency, which has overall responsibility for the administration and usage of the CJIS programs that operate in a particular state."[131] Moreover, the FBI states that "access to NGI is controlled through extensive, long-standing

user identification and authentication procedures."[131] Florida, to train the over 5,300 officials with access to the FACES system,[10] online user training was made available within the user interface.[142] No information on training requirements in Maricopa County, AZ, or Seattle was available.

Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Table 7 //
FBI NGI-IPS Notice Policy III
(Source: FBI (2016))

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components			X	
Federal entities			X	
State, local, tribal gov't entities			X	
Public				
Private sector				
Foreign governments			X	Canada
Foreign entities	X			
Other (specify):				

The EFF furthermore highlights the substantial number of attacks on and breaches of government agency data storage, which is highly problematic considering the sensitive nature of the information stored in FRT databases.[65] Media reports suggest that, for example, the MCSO has in the past struggled with data protection provisions. ProPublica and the Center for Investigative Reporting revealed a possible data breach in 2007 as a Chinese national who had not passed a vetting process before working for ACTIC with sweeping access to the FRT database left to return for China potentially with protected information. Moreover, ProPublica's research suggests that there have been deliberate efforts within the MCSO to cover up instead of communicating the potential data breach.[160]

Equity

Biased Enrollment Policing practices in the US disproportionately affect minority communities.[240] Research shows that individuals from racial minority groups are substantially more likely to be pulled over,[241,242] searched,[242–244] arrested,[245–247] incarcerated,[248] and wrongfully convicted[249] than white individuals.[247] In 2017, 27.2% of individuals arrested in the US were black despite the fact that only around 13.4% of the population is black.[250,251] In Florida, black arrestees made up 34% percent of arrestees, with 16.9% of black individuals as a share of the total population.[252,253] Maricopa County, AZ, access all of Arizona's booking photos, black individuals constitute

5% of the total population but 12.5% of arrestees.[254,255] In King County, which Seattle is a part of, 26.0% of booked individuals are black whereas only 6.8% of the population is black.[256,257] Regardless of whether such policing activity results in findings of wrongdoing, and numerous studies[247] show that searches of minority groups are less likely to result in finding contraband,[241,242,244,258,259] police contact negatively impacts every aspect of an individual's life. In particular, at least 30% of arrests never lead to a charge or conviction.[74] In the context of enrollment in FRT systems, higher rates of arrests, including wrongful arrests, lead to an overrepresentation of minorities in FRT databases.[10] Moreover, the blanket enrollment of Honduran driver's and arrestees in Maricopa County's, AZ, FRT database has caused overrepresentation specifically of Hispanic individuals in the database. Outside the law enforcement use context, NIST, the agency hosting the Facial Recognition Vendor Test (FRVT) has been heavily criticized for its practice of enrolling images from vulnerable populations in its vast test datasets, including "images of children who have been exploited for child pornography; U.S. visa applicants, especially those from Mexico; and people who have been arrested and are now deceased."[59]

Biased Exposure In the US, the FRT algorithm developed by MorphoTrust USA, now Idemia, dominates the public use market and is employed by the majority of state driver's license databases, federal and state law enforcement agencies, including the FBI and Florida's FRT systems.[74] Based on the most recent edition of the NIST 1-to-1 FRVT, a series started in 2017, Idemia's algorithms exhibit substantial demographic differences in the false match rates, which are higher for black than for white individuals, and higher for females than for males (see Figure 8).[76] NEC's algorithm in use in Seattle has not yet been tested for its performance across demographic groups.[121] The Hummingbird system that used to and may still be in use in Maricopa County, AZ, is particularly problematic - to the best of the author's knowledge, it has never participated in a NIST FRVT and was heavily criticized for its inaccuracy by police staff.[160, 161] Research shows that the algorithms in use by other law enforcement agencies, including Los Angeles County Sheriff, the Maryland Department of Public Safety, the Michigan State Police, the Pennsylvania Justice Network, and the San Diego Association of Governments (SANDAG) that were tested in Klare et al. (2012) were found to perform 5 to 10% less accurate on black than on white individuals and also systematically worse for female and younger individuals.[10,68,72] To address the need for more accurate data on FRT algorithms' bias, 52 organizations formed a coalition calling on the DOJ to investigate the issue in the context of law enforcement use.[260]

Quality Standard In addition to a lack of testing for demographic biases with the goal to establish standards for the unbiasedness of FRT in use by

law enforcement, both public officials and industry representatives show a lack of understanding of or concern for bias. For example, Kimberly DelGreco, Deputy Assistant Director of the Information Services Branch in the FBI's CJIS Division, stated in the 2017 congressional hearing that their "requirement when [the FBI] developed the Interstate Photo System did not include tone or ethnicity. It was based on the mathematical computation only."[65] It is important to note that especially in the context of the FBI's use of FRT, misidentification due to bias in the FRT employed has consequences beyond the criminal realm when employed for employment background checks.[74] Similarly, a system's analyst for a Florida Sheriff's office stated that "[the software] is oblivious to things like a person's hairstyle, gender, race or age" in a media interview and the Seattle PD claimed in their FAQ section that their system "does not see race, sex, orientation or age."[65] Moreover, in interviews representatives for leading FRT vendors have failed to establish that tests for racial bias were used instead relying on the assumption that diverse training datasets automatically produced unbiased algorithms.[10]

Due Process

Public Consultation Process The FBI was in fact severely criticized by policymakers and the GAO for failing to inform the public of its use of FRT. Specifically, the GAO finds that the FBI did not update an initial PIA for the start of the NGI-IPS development in a timely manner when it began to pilot the system with 20,000 searches and did not publish a PIA before the FACE unit began its operations. Furthermore, the GAO highlights that a SORN was not filed until after it first reviewed the systems in 2016. Overall, the FBI was using FRT for around five years before informing the public by publishing the PIAs on its activities in 2015.[65,131] Moreover, the FBI's CJIS unit manages and reviews compliance with regulation of access to the FBI's FRT-relevant systems through an audit program, however, the GAO found that the audit program did not meet its objectives in achieving a timely audit, which is in conflict with the GAO's Standards for Internal Control in the Federal Government (also referred to as the Green Book).[130,261] While some state and local jurisdictions have established requirements for consultations with stakeholders or for public comment periods, such requirements remain the exception rather than the norm. Florida, for example, has been criticized for trialing FRT technology with little or no public consultation, in particular in the context of the Super Bowl 2001 in Tampa.[148] Similarly, no evidence was found of a public consultation in Maricopa County, AZ. Seattle is making strides in involving the community in the use of surveillance technologies: The 2017 Surveillance Ordinance makes a public meeting and comments a requirement for each new technology.[262] Moreover, the

process also includes a Surveillance Advisory Working Group composed of community representatives with the task to create privacy and civil liberties impact assessment for each new technology[263] The Seattle City Council also specifically ran a community engagement program on body-worn cameras that addressed questions regarding FRT capabilities.[264]

Awareness of Sample Collection Not all law enforcement agencies make information available to the public regarding when, where, and how biometric samples are collected for the purpose of FRT processing. Research has revealed that in 2016, out of 52 agencies surveyed only 10% had a use policy that was accessible to the public.[10] The FBI provides limited information about its FRT programs in the required PIAs, although they were not published in a timely manner.[130,131,137,265] The PCSO, which hosts Florida's FACES system, published mentions of its facial recognition capabilities on its website only in the history section and auxiliary documents including job descriptions, internal memos, and the jail inmate handbook.[266] During the live FRT trial in Tampa's Ybor City, police have erected signs stating "Smart CCTV is in use," which is a step in the right direction but may not be understood by the public as referencing an FRT system. In fact, interviews have revealed that the signs were not visible from all areas and passersby did not know what they meant.[149] The only notice the MCSO provides of its use of FRT through its website is hidden in a procedure's manual for the identification process.[153] The Seattle PD provides transparent information about its use of FRT in its publicly available Police Manual online.[164] Moreover, researchers at Georgetown Law in their survey found that no law enforcement agency had a policy that required a warrant to scan and "search" a data subject's face and around 80% of agencies do not require reasonable suspicion of criminal activity.[65] There is no evidence that agencies rely on any communication channel other than public documents on their websites to make the public aware in which context their biometric sample is collected for FRT identification.

Arrests & Evidence To date, the question of how FRT identifications can feature as evidence in the judicial process has been addressed in one case, Willie Allen Lynch v. State of Florida.[267,268] The defendant Willie Allen Lynch was identified by FRT as the only suspect identified with a star out of four suggested suspects for a 2015 case of a crack cocaine sale witnessed by undercover agents who were not able to identify the offender.[144] The use of the system was not disclosed in the police report but revealed to the defendant in a pretrial disposition of the crime analyst who operated the FRT.[144] The defendant's defense was built around the claim that he had been misidentified which raised the question of how the still imperfect FRT was employed and whether the defendant had a right to see the photos of

other defendants identified by the FRT as Brady evidence.*[144] The appellate court, the First District Court of Appeals held that the defendant could not prove the similarity between his and the photos of other possible suspects identified by the FRT, even though the defense team had no access to them, and upheld the conviction.[144] In reaction EFF, ACLU, Georgetown Law's Center on Privacy & Technology, and Innocence Project filed an amicus brief with the Florida Supreme Court to draw attention to and challenge the lower court's holding based on the fact that no information around the procedural use of FRT was revealed.[267] The case highlights the problems emerging from the fact that, according to the state attorney, there is no policy regarding the role of FRT evidence in criminal proceedings.[270] Although the identification process involved a two-step human review including the FRT identification and the confirmation by the undercover agents, the process was deliberately made intransparent to the defendant and the defense counsel.[270]

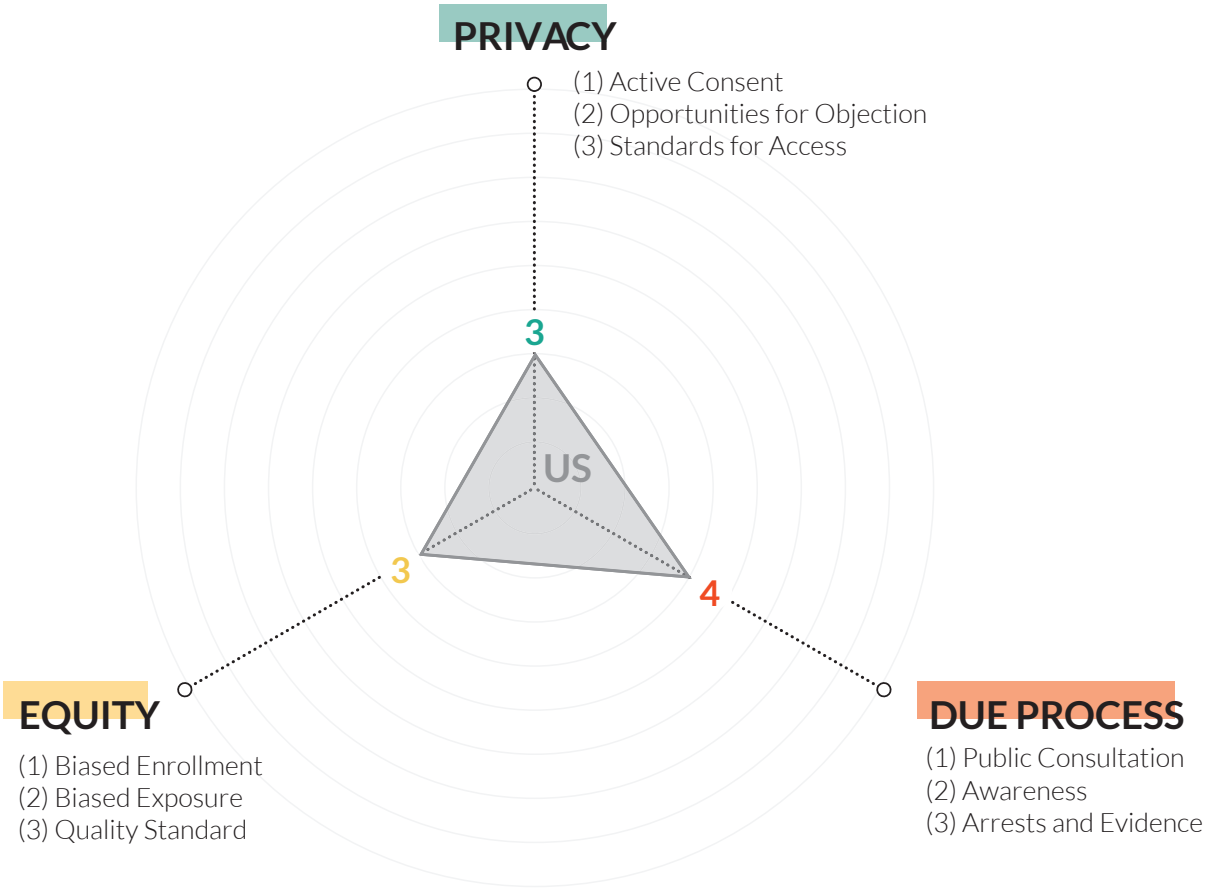


Figure 12 // US Policy Framework Scoring

*Based on the case Brady v. Maryland, 373 U.S. 83 (1963), the Brady Rule requires that all available materially exculpatory evidence be disclosed to the defense.

PRIVACY

Active Consent	Avenues for Objection	Standard for Access
1 **No active consent required.** Governmental agencies at the federal (e.g. FBI), state (e.g. Florida), and at the local level (e.g. Maricopa County, AZ) perform facial recognition on driver's license photos for which the data subjects did not actively consent to being part of an FRT system. Moreover, booking photo databases likely incude individuals not charged with or convicted of a crime.	**1** **There are no avenues for objection.** Although the 1974 Privacy Act explicitly provides individuals with the opportunity to inquire about and request corrections of their data used by government agencies, the FBI and DOJ moved to exclude the NGI system from the provisions of the Privacy Act. The Privacy Act does not apply to government agencies at the state or local level.	**1** **Information is shared based solely on the discretion of the organization.** State agencies are not subject to and the FBI's NGI-IPS system has been exempt from the 1974 Privacy Act that governs the sharing of personal information by government agencies.

EQUITY

Biased Enrollment	Biased Exposure	Quality Standard
1 **Population groups differing based on a protected category (Article 26 ICCPR) are treated unequally.** Bias in policing creates overrepresentation of ethnic minorities in booking photo databases. In Maricopa County, AZ, all driver's license and booking photos available to the government of Honduras were added to the FRT system in 2007.	**1** **Population groups differing based on a protected category (Article 26 ICCPR) are treated unequally.** Based on the bias in the enrollment process and unaddressed algorithmic bias, ethnic minorities are at a higher risk of (mis-)identification.	**1** **There is no regard for differential performance of FRT based on demographic differences.** None of the government agencies employing FRT have publicly addressed potential bias in the software employed.

DUE PROCESS

Public Consultation	Awareness	Evidence
1 **There was neither a stakeholder consultation process nor a public comment period.** The FBI began its FRT pilot and deployment before publishing a privacy impact assessment alerting the public to the use of the system.	**1** **There is no communication that a sample is collected for the purposes of use in conjunction with FRT.** Many state and local agencies do not provide information on their collection of samples to be run through FRT systems on their website.	**2** **There is a two-step process featuring human review but it is intransparent to the stakeholders involved in the criminal process (e.g. arrestee/defendant, police staff, defense attorney, jury, judge).** In materials made available to the public by agencies the agencies describe a two-step process involving human review, however, the Willie Allen Lynch v State of Florida case illustrates that there is insufficient transparency about the extent to which FRT is part of the investigation.

Table 8 // US Policy Framework Scoring

04 //

DISCUSSION OF EMERGING ISSUES

04 //

DISCUSSION OF EMERGING ISSUES

The analysis of current FRT applications in domestic law enforcement and their regulation highlights a broader problem across technology policy: Highly complex emerging technological innovations emerge from academia and the private sector and promise gains in the effectiveness and efficiency of processes, for example, in the area of law enforcement. In the area of surveillance technology, gains from such technological innovation promise returns for their users, law enforcement agencies, and their developers. However, in the pursuit of these gains, the fast-paced innovation process risks to evolve without a focus on societal needs.

Complex technologies such as FRT often engender information asymmetry between the public and private Sector and pose a unique challenge to democratically organized societies because effective public discourse and policymaking require both the sovereign electorate and their elected representatives to fully understand the capabilities and limitations of technological innovation. However, the case of FRT use in law enforcement illustrates that this understanding is lacking. Several agency representatives have revealed a lack of understanding of how the technology works. In the UK, for example, the South Wales Police stated in a response to a FOI request:

> *"South Wales Police do not currently employ any Artificial Intelligence, machine learning or deep learning technology. South Wales Police currently use Automatic Facial Recognition technology provided by NEC. (...) The algorithm has been "trained" using AI technology during its development by NEC, however no machine learning element is present when the system is used by South Wales Police."*[271]

FRT and machine learning applications pass training data through a learning algorithm to generate a machine learning model. The machine learning model acts as a learned algorithm that new data is passed through to arrive at the desired answer, for example, a classification. The statement, therefore, shows a lack of understanding or avoidance of public inquiry in representing the use of a machine learning model as separate from the machine learning process.[40] Moreover, in the US, Pinellas County, FL, Captain Jim Main stated that:

> *"The more images you get, the greater chance you have of making a match."* [145]

However, increasing the number of images in the reference storage also increases the number of distractors the machine learning model could misclassify on, which increases the probability of useless false positive classifications, which makes the FRT as a whole less effective.[40,64] This argument has been advanced to lend further weight to the case against including driver's license and ID photos. Similarly, law enforcement officials at the FBI, the PCSO and the Seattle Police Department have claimed that their FRT "does not see race," demonstrating a lack of understanding for the challenges that remain for calibrating FRT for unbiasedness.[10, 65]

Both in the US and in Europe around half the adult population had not heard about AI in 2017 and marginalized population groups on average had even less awareness.[16,17] With such limited knowledge transfer from innovating sectors to civil society, informed political participation in discussions of technology regulation becomes impossible for large shares of the population. One line of reasoning may argue that in a representative democracy, the electorate should through its votes determine the general political direction, so that the technicalities of policymaking can remain to be addressed by elected legislators. However, parliamentarians face challenges in keeping up with rapid progress across many areas that require regulation. In the US, for example, the challenge has grown since in-house expertise in the Office of Technology Assessment fell victim to budget cuts over 25 years ago.[272] As a result, legislators struggle to keep up with technical details relying on expert testimonies and lobbyists, which Rep. Adam Kinzinger from Illinois illustrated by stating "I can understand about 50 percent of the things you say" during a technical testimony.[272–274]

In an interesting evolution of regulatory dynamics, private sector developers of FRT have acknowledged the risks that their technology poses to the exercise of human rights and not only joined researchers and advocates in a call for regulation but also engaged in self-regulation. Microsoft published suggestions for FRT regulation and committed to upholding six principles, from notice and consent to non-discrimination, in its development and sale of the technology.[11,13] Moreover, Microsoft is lobbying in support of Washington State's Senate Bill SB 5376 would establish protections for personal data, and establish strict conditions for the use of FRT by government agencies for surveillance in public spaces.[275] Most recently, Microsoft rejected a government contract with a California law enforcement agency seeking to install FRT in police cars and body-worn cameras due to risks to human rights.[276,277] Similarly, Google has formulated principles governing their development of AI and taken a public "not to offer general-purpose facial recognition [application programming interfaces] APIs before working through important technology and policy questions."[278–280] Riding on the momentum of private sector self-regulation, the Algorithmic Justice League and the Center on Technology & Privacy at Georgetown Law have drafted the SafeFace Pledge, through which companies can openly commit to not (1) "contribute to applications that risk human life," (2) "facilitate secret and discriminatory government surveillance," and actively (3) "mitigate law enforcement abuse," and "ensure [the developer's] rules are being followed."[281]

05 //
CONCLUSION

05 //
CONCLUSION

FRT is a formidable technological innovation that allows us to connect a part of us that is inherently private, our identity, with a part of us that is inherently public, our face. Relative to other biometric technologies, FRT stands out because our face is one of our most immutable features and one of the parts of our body that we most identify with. Moreover, in most cultural contexts, our face is always exposed to the public making it difficult to participate in societal life without revealing one's face. For these reasons, the use of FRT creates risks for our exercise of human rights which demand caution as we apply it to serve legitimate societal goals such as enforcing the law. In the interest of offering structure for the necessary societal discourse and social innovation engendered by the adoption of FRT as an emerging technology, this work developed a policy analysis framework. The three-dimensional framework centers on the three human rights principles most relevant in the context of FRT, namely privacy, equity or non-discrimation, and due process, which are almost universally accepted at the international level and codified, in the ICCPR. As an analytical guide, the policy analysis framework operationalizes the broader concept of each human rights principle in the context of FRT in three sub-variables to compare different jurisdictions' safeguarding of human rights.

The case studies from both the UK and the US demonstrate that even in mature democracies with a strong commitment to protecting civil liberties, establishing policy safeguards for the use of FRT in law enforcement in accordance with human rights remains challenging. In the UK, the policy environment is effective at deploying FRT with due process considerations. In general, law enforcement agencies consulted stakeholders in the development of their FRT program development and communicated program details via at least one if not more communication channels. Relatively more problematic is the area of privacy: There is no requirement for notice of and active consent to the enrollment in an FRT database, which raises concerns with respect to individuals arrested for but never charged with or convicted of a crime, and public-private collaborations. Data access and rights of the data subject, for example, to object to the use and management of the data, are not protected by legislation specific to FRT but rigorous standards for the protection of personal data in general through the EU GDPR. The most concerning area is equity, in which a lack of understand-

ing and concern for algorithmic bias, as well as bias in real-life enrollment practices, create a disparate impact for minorities.

In the US, jurisdictions vary greatly in the law enforcement use of FRT and the policy response. Some jurisdictions stand out in setting a positive example of issues around the use of FRT can be addressed with innovative policy solutions such as Seattle, which established a collaboration with the ACLU to develop an FRT use policy that is aligned with civil liberty protections. Other jurisdictions raise concerns due to their lack of critical engagement with the technology's risks. Overall, examples from these jurisdictions show that the there is insufficient regulation in the area of due process rights, as programs are rolled out without effective communication with the public before or during FRT deployment, including the FBI's delayed publication of a PIA around five years after the program launch. The current Willie Allen Lynch v State of Florida case, however, will be an interesting opportunity to grapple with procedural safeguards and transparency around the use of FRT. More concerning are the areas of equity and privacy. Jurisdictions, in general, fail to critically address algorithmic bias and bias from the disproportionate enrollment of overpoliced minorities or ethnically homogenous foreign citizens, as Maricopa County's enrollment of Honduran booking and driver's license and ID photos demonstrated. In the area of privacy, the automatic enrollment of civil driver's license and ID photos without notice or an effective path to opt-out without forgoing other public benefits is very problematic. Moreover, the lack of FRT-specific or even general data protection regulation that applies to all law enforcement agencies without allowing for exceptions such as the one granted to the FBI's FRT system, jeopardized the rights of the data subjects.

For an informed societal discourse on benefits and risks of FRT use in law enforcement, it is necessary to conduct further research, for example, in quasi-experimental research designs, on the effectiveness of FRT in solving and preventing crimes. Therefore, it is important to develop effective ways to communicate academic knowledge on the technology's capabilities and limitations and raise public awareness for the trade-off between benefits and risks of its applications. As the democratic sovereign, the people, as well as their elected representatives, need to understand that an emerging technology is in use, how it is used, how it works, and what its impact is. Given the unique vulnerability of leveraging our face for establishing our identity, FRT creates specific risks to protected human rights. For this reason, it is necessary to establish a regulatory framework specific to the challenges of FRT before rights violations need to be litigated in a slow-moving judicial process. Technological innovation redefines the architecture of the social world, and social innovation is necessary to ensure the respect of our existing human rights protections in an evolving socio-technical system.

REFERENCES

1. PTI. Delhi: Facial recognition system helps trace 3,000 missing children in 4 days - Times of India. The Times of India (2018). Available at: https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms. (Accessed: 21st January 2019)

2. The Brussels Times. The man in the hat identified thanks to FBI software. (2016). Available at: http://www.brusselstimes.com/brussels/5445/the-man-in-the-hat-identified-thanks-to-fbi-software. (Accessed: 21st January 2019)

3. Aravindan, A. & Geddie, J. Singapore to test facial recognition on lampposts, stoking privacy fears. Reuters (2018).

4. South Wales Police. Facial Recognition Technology. South Wales Police Available at: https://www.south-wales.police.uk/en/advice/facial-recognition-technology/. (Accessed: 22nd January 2019)

5. Joseph, G. & Lipp, K. IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color. The Intercept (2018). Available at: https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/. (Accessed: 29th January 2019)

6. Sanchez del Rio, J., Moctezuma, D., Conde, C., Martin de Diego, I. & Cabello, E. Automated border control e-gates and facial recognition systems. Comput. Secur. 62, 49–72 (2016).

7. Mason, M. Biometric Breakthrough - How CBP is Meeting its Mandate and Keeping America Safe. U.S. Customs and Border Protection (2016). Available at: https://www.cbp.gov/frontline/cbp-biometric-testing. (Accessed: 21st January 2019)

8. Reilly, C. Welcome to the airport of the future, where your face is your passport. CNET (2018). Available at: https://www.cnet.com/news/welcome-to-the-airport-of-the-future-where-your-face-is-your-passport/. (Accessed: 22nd January 2019)

9. Lohr, S. Facial Recognition Is Accurate, if You're a White Guy. The New York Times (2018).

10. Garvie, C., Bedoya, A. & Frankle, J. The Perpetual Line-Up. (Center on Privacy & Technology at Georgetown Law, 2016).

11. Smith, B. Facial recognition: It's time for action - Microsoft on the Issues. Microsoft on the Issues (2018). Available at: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/. (Accessed: 21st January 2019)

12. Smith, B. Facial recognition technology: The need for public regulation and corporate responsibility - Microsoft on the Issues. Microsoft on the Issues (2018). Available at: https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/. (Accessed: 21st January 2019)

13. Sauer, R. Six principles to guide Microsoft's facial recognition work - Microsoft on the Issues. Microsoft on the Issues (2018). Available at: https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/. (Accessed: 21st January 2019)

14. Shoham, Y. et al. The AI Index 2018 Annual Report. (AI Index Steering Committee, Human-Centered AI Initiative, Stanford University, 2018).

15. Dutton, T. An Overview of National AI Strategies – Politics + AI – Medium. Medium (2018). Available at: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd. (Accessed: 6th March 2019)

16. Directorate-General for Communications Networks, Content and Technology of the European Commission. Special Eurobarometer 460 - Attitudes towards the impact of digitisation and automation on daily life. (European Commission, 2017).

17. Consult, M. National Tracking Poll #170401. (Morning Consult, March-April, 2017).

18. Home Office. Biometrics Strategy - Better public services, maintaining public trust. (Home Office, 2018).

19. House of Commons Science and Technology Committee. Biometrics strategy and forensic services - Fifth Report of Session 2017–19. (House of Commons , 2018).

20. Zhang, B. & Dafoe, A. Artificial Intelligence: American Attitudes and Trends. (Center for the Governance of AI, Future of Humanity Institute, University of Oxford, 2019).

21. Castro, D. Survey: Few Americans Want Government to Limit Use of Facial Recognition Technology, Particularly for Public Safety or Airport Screening. Center for Data Innovation (2019). Available at: https://www.datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/. (Accessed: 19th February 2019)

22. World Economic Forum. The Global Risks Report 2018 - 13th Edition. (World Economic Forum, 2018).

23. Sandberg, A. & Bostrom, N. Global Catastrophic Risks Survey. (Future of Humanity Institute, Oxford University, 2008).

24. Whittaker, M. et al. AI Now Report 2018. (AI Now Institute, 2018).

25. United Nations General Assembly. Universal Declaration of Human Rights. (1948).

26. Warren, S. D. & Brandeis, L. D. The Right to Privacy. Harv. Law Rev. V.IV, (1890).

27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)). 2016/679 (2016).

28. The United States Bill of Rights. (1791).

29. Charter of Fundamental Rights of the European Union. (2012).

30. Consolidated version of the Treaty on European Union (TEU). (2012).

31. Consolidated version of the Treaty on the Functioning of the European Union (TFEU). (2012).

32. Fairhurst, M. Biometrics: a Very Short Introduction. (Oxford University Press, 2018).

33. Ashbourn, J. Practical Biometrics: From Aspiration to Implementation. 1–10 (Springer London, 2015).

34. Information Security: Foundations, Technologies and Applications. (IET Digital Library, 2018).

35. Riggan, B. S., Short, N. J. & Hu, S. Thermal to Visible Synthesis of Face Images using Multiple Regions. arXiv [cs.CV] (2018).

36. Scherhag, U. et al. On the vulnerability of face recognition systems towards morphed face attacks. in 2017 5th International Workshop on Biometrics and Forensics (IWBF) 1–6 (2017).

37. Vielhauer, C. User-Centric Privacy and Security in Biometrics. (Institution of Engineering and Technology, 2017).

38. Thomas, E. How to hack your face to dodge the rise of facial recognition tech. WIRED UK (2019). Available at: https://www.wired.co.uk/article/avoid-facial-recognition-software. (Accessed: 1st February 2019)

39. Harvey, A. CV Dazzle: Camouflage from Face Detection. Available at: https://cvdazzle.com/. (Accessed: 7th May 2019)

40. Kohli, N. (2019).

41. Dwiyantoro, A. P. J. The Evolution of Computer Vision Techniques on Face Detection, Part 1. Medium (2018). Available at: https://medium.com/nodeflux/the-evolution-of-computer-vision-techniques-on-face-detection-part-1-7fb5896aaac0. (Accessed: 31st March 2019)

42. Viola, P. & Jones, M. Rapid object detection using a boosted cascade of simple features. CVPR (1) (2001).

43. Dalal, N. & Triggs, B. Histograms of oriented gradients for human detection. in international Conference on computer vision & Pattern Recognition (CVPR'05) 1, 886–893 (IEEE Computer Society, 2005).

44. Kroll, J. A. Face Recognition: A Technology Primer Prepared for the National Association of Criminal Defense Attorneys. (1 March, 2019).

45. Li, H., Lin, Z., Shen, X., Brandt, J. & Hua, G. A convolutional neural network cascade for face detection. in Proceedings of the IEEE conference on computer vision and pattern recognition 5325–5334 (2015).

46. Zhang, K., Zhang, Z., Li, Z. & Qiao, Y. Joint Face Detection and Alignment using Multitask Cascaded Convolutional Networks. arXiv [cs.CV] (2016).

47. Lei, Z. & Li, S. Z. Face Recognition Models: Computational Approaches. in International Encyclopedia of the Social & Behavioral Sciences (Second Edition) (ed. Wright, J. D.) 658–662 (Elsevier, 2015).

48. Langston, J. How well do facial recognition algorithms cope with a million strangers? UW News (2016). Available at: https://www.washington.edu/news/2016/06/23/how-well-do-facial-recognition-algorithms-cope-with-a-million-strangers/. (Accessed: 20th April 2019)

49. International Covenant on Civil and Political Rights (ICCPR). (1976).

50. Solove, D. J. A brief history of information privacy law. Proskauer on privacy, PLI (2016).

51. Mulligan Deirdre K., Koopman Colin & Doty Nick. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 374, 20160118 (2016).

52. The Bingham Centre for the Rule of Law. Building Human Rights into Practice - A Training Manual on International Human Rights Law. (The Bingham Centre for the Rule of Law , 2012).

53. Çalı, B. Balancing human rights? Methodological problems with weights, scales and proportions. Hum. Rights Q. 251–270 (2007).

54. Scottish Human Rights Commission. Equality & Human Rights Impact Assessment. Convention Rights Available at: http://eqhria.scottishhumanrights.com/eqhriatrainingconrightsheader.html. (Accessed: 7th May 2019)

55. Liberty -The National Council for Civil Liberties. A Parliamentarian's Guide to the Human Rights Act. (Liberty - The National Council for Civil Liberties, 2010).

56. Bureau of Justice Assistance. Face Recognition Policy Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities. (US Department of Justice, 2017).

57. Financial Times. Privacy is under threat from the facial recognition revolution. Financial Times (2017).

58. Liao, S. IBM didn't inform people when it used their Flickr photos for facial recognition training. The Verge (2019). Available at: https://www.theverge.

com/2019/3/12/18262646/ibm-didnt-inform-people-when-it-used-their-flickr-photos-for-facial-recognition-training. (Accessed: 3rd April 2019)

59. Keyes, O., Stevens, N. & Wernimont, J. The Government Uses Images of Abused Children and Dead People to Test Facial Recognition Tech. Slate Magazine (2019). Available at: https://slate.com/technology/2019/03/facial-recognition-nist-verification-testing-data-sets-children-immigrants-consent.html. (Accessed: 26th March 2019)

60. House of Commons. Current and future uses of biometric data and technologies. (House of Commons, 2015).

61. The Westminster Consortium. Human Rights and Parliaments: Handbook for Members and Staff. (The Westminster Consortium, 2011).

62. Purshouse, J. & Campbell, L. Privacy, Crime Control and Police Use of Automated Facial Recognition Technology. Crim. Law Rev. 2019, (2018).

63. Snapes, L. Taylor Swift used facial recognition software to detect stalkers at LA concert. The Guardian (2018).

64. Kemelmacher-Shlizerman, I., Seitz, S. M., Miller, D. & Brossard, E. The MegaFace Benchmark: 1 Million Faces for Recognition at Scale. in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 4873–4882 (2016).

65. House Of Representatives. Hearing Before The Committee On Oversight And Government Reform House Of Representatives. (House Of Representatives, 2017).

66. Robitzski, D. Americans Built Tech for China's Sinister 'Re-Education Camps'. Futurism (2019). Available at: https://futurism.com/americans-developed-tech-china-reeducation-camps. (Accessed: 26th March 2019)

67. Big Brother Watch. Face Off - The lawless growth of facial recognition in UK policing. (Big Brother Watch, 2018).

68. Klare, B. F., Burge, M. J., Klontz, J. C., Vorder Bruegge, R. W. & Jain, A. K. Face Recognition Performance: Role of Demographic Information. IEEE Trans. Inf. Forensics Secur. 7, 1789–1801 (2012).

69. Meissner, C. A. & Brigham, J. C. Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review. Psychol. Public Policy Law 7, 3–35 (2001).

70. Kelly, D. J. et al. The other-race effect develops during infancy: evidence of perceptual narrowing. Psychol. Sci. 18, 1084–1089 (2007).

71. Lindsay, D. S., Jack, P. C., Jr & Christian, M. A. Other-race face perception. J. Appl. Psychol. 76, 587–589 (1991).

72. Buolamwini, J. & Gebru, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. in Proceedings of the 1st Conference on Fairness, Accountability and Transparency (eds. Friedler, S. A. & Wilson, C.) 81, 77–91 (PMLR, 2018).

73. Jonathan Phillips, P., O'Toole, A. J., Jiang, F., Narvekar, A. & Ayadd, J. An Other-Race Effect for Face Recognition Algorithms. ACM Transactions on Applied Perception (2009).

74. Lynch, J. Face Off: Law Enforcement Use of Face Recognition Technology. Electronic Frontier Foundation (2018). Available at: https://www.eff.org/wp/law-enforcement-use-face-recognition. (Accessed: 6th May 2019)

75. Kofman, A. How a Facial Recognition Mismatch Can Ruin Your Life. The Intercept (2016). Available at: https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/. (Accessed: 6th May 2019)

76. Grother, P., Ngan, M. & Hanaoka, K. Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification. (National Institute of Standards and Technology, 2019).

77. NEC. NEC technology recognizes people based on partial images. NEC (2019). Available at: https://www.nec.com/en/press/201902/global_20190208_01.html. (Accessed:

9th March 2019)

78. Biometrics and Forensics Ethics Group Facial Recognition Working Group. Ethical issues arising from the police use of live facial recognition technology -. (UK Government, 2019).

79. Nilsson, P. How UK police are using facial recognition software. Financial Times (2018).

80. Metropolitan Police. Information Rights Unit - Use and discussion of live automated facial recognition trails deployment. (Metropolitan Police, 2018).

81. Meek, J. Robo cop. The Guardian (2002).

82. Metropolitan Police. Live Facial Recognition, (LFR) MPS Legal Mandate. (Metropolitan Police, 2018).

83. Metropolitan Police. Live Facial Recognition trial. The Met Available at: https://www.met.police.uk/live-facial-recognition-trial/. (Accessed: 16th April 2019)

84. Metropolitan Police. UPDATE: Facial recognition deployment in Romford. The Met (2019). Available at: http://news.met.police.uk/news/update-facial-recognition-deployment-in-romford-358866. (Accessed: 16th April 2019)

85. Metropolitan Police. Information Rights Unit - 'Real time' automatic facial recognition technology at the Notting Hill Carnival 2017. (Metropolitan Police, 2018).

86. Metropolitan Police. Information Rights Unit – MPS use of facial recognition technology. (Metropolitan Police, 2018).

87. Metropolitan Police. Information Rights Unit – Facial recognition or face scanning software used by the MPS. (Metropolitan Police, 2017).

88. South Wales Police. All Deployments. (Smarter Recognition Safer Community).

89. South Wales Police. What is AFR? AFR | South Wales Police Available at: http://afr.south-wales.police.uk/. (Accessed: 16th April 2019)

90. Lloyd, S. South Wales Police Data Protection Impact Assessment. (South Wales Police, 2018).

91. South Wales Police. Introduction of Facial Recognition into South Wales Police - South Wales Police. South Wales Police Available at: https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/. (Accessed: 16th April 2019)

92. South Wales Police. South Wales Police to use facial recognition at Biggest Weekend in Swansea. South Wales Police (2018). Available at: https://www.south-wales.police.uk/en/newsroom/facial-recognition-biggest-weekend-swansea/. (Accessed: 16th April 2019)

93. Leicestershire Police. Freedom of Information Act 2000 - 003690/18. (Leicestershire Police, 2018).

94. Leicestershire Police. Facewatch. Leicestershire Police Available at: https://leics.police.uk/advice-and-information/crime-prevention/business-crime/facewatch. (Accessed: 17th April 2019)

95. Facewatch. Facewatch – Facewatch, the greatest advance in security since the introduction of CCTV. Facewatch Available at: https://www.facewatch.co.uk/. (Accessed: 17th April 2019)

96. Leicestershire Police. Freedom of Information Act 2000 - 002688/18. (Leicestershire Police, 2018).

97. Humberside Police. Search: 'face'. Humberside Police Available at: https://www.humberside.police.uk/search?keywords=facial&op=Submit&form_build_id=form-226LdfwWC8oJzXC7T2Yvv8CWPXOrovMjQeLEGxZflgI&form_id=hp_secondary_search_form. (Accessed: 16th April 2019)

98. Humberside Police. Humberside Police Force Management Statement Summary. (Humberside Police , 2018).

99. Data Protection Act 2018. 2018 c. 12, (2018).

100. Police and Criminal Evidence Act 1984. 1984 c. 60, (1984).

101. Home Office. PACE Code D - Revised Code of Practice for the identification of persons by Police Officers. (Home Office, 2017).

102. Home Office. Surveillance Camera Code of Practice. (Home Office, 2013).

103. Information Commissioner's Office. In the picture: A data protection code of practice for surveillance cameras and personal information. (Information Commissioner's Office, 2017).

104. Biometrics & Forensics Ethics Group. Biometrics & Forensics Ethics Group - Ethical Principles. (Biometrics & Forensics Ethics Group, 2018).

105. Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679. (Article 29 Data Protection Working Party, 2017).

106. Koene, A. et al. A governance framework for algorithmic accountability and transparency. (European Parliamentary Research Service, 2019).

107. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. L 119/89, (2016).

108. South Wales Police. Freedom of Information Request 397-18. (South Wales Police, 2019).

109. Metropolitan Police. Information Rights Unit – Information about facial recognition used on Remembrance Sunday at the Cenotaph in 2017. (Metropolitan Police, 2018).

110. Lloyd, S. South Wales Police Privacy Impact Assessment. (South Wales Police , 2018).

111. Metropolitan Police. Metropolitan Police Service Fair Processing Notice (FPN). (Metropolitan Police, 2016).

112. Facewatch. Subjects of Interest (SOIs) – Detailed Privacy Notice to be read in conjunction with our General Privacy Notice. (Facewatch, 2019).

113. Facewatch. Subject Access Request. Facewatch Available at: https://www.facewatch.co.uk/privacy/subject-access-request/. (Accessed: 17th April 2019)

114. Leicestershire Police. Freedom of Information Act 2000 - 001507/18. (Leicestershire Police, 2018).

115. Metropolitan Police. Information Rights Unit – MPS policies on automated facial recognition(AFR) technology. (Metropolitan Police, 2018).

116. Metropolitan Police. Metropolitan Police Service Privacy Impact Assessment. (Metropolitan Police, 2018).

117. Metropolitan Police. MPS Privacy Notice. (Metropolitan Police, 2018).

118. Facewatch. Privacy. Facewatch Available at: https://www.facewatch.co.uk/privacy/. (Accessed: 17th April 2019)

119. Home Office. Arrests. Home Office (2019). Available at: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest. (Accessed: 29th April 2019)

120. Grother, P. J., Quinn, G. W. & Phillips, P. J. Report on the Evaluation of 2D Still-Image

Face Recognition Algorithms. (2010). doi:10.1002/https://dx.doi.org/10.6028/NIST.IR.7709

121. Karp, P. Facial matching system risks racial bias, Human Rights Law Centre warns. The Guardian (2018).

122. Metropolitan Police. Information Rights Unit – Automated facial recognition technology used on Remembrance Sunday in 2017 and the Notting Hill Carnival in 2016 & 2017. (Metropolitan Police, 2018).

123. Metropolitan Police. Information Rights Unit – Facial recognition systems used within the MPS. (Metropolitan Police, 2017).

124. South Wales Police. Safer Community. AFR | South Wales Police Available at: http://afr.south-wales.police.uk/safer-community. (Accessed: 16th April 2019)

125. South Wales Police. Heddlu De Cymru - Our Vision, Values and Ethics. South Wales Police Available at: https://www.south-wales.police.uk/en/about-us/visonvaluesandethics/. (Accessed: 17th April 2019)

126. Metropolitan Police. Live facial technology to be deployed in Romford. The Met (2019). Available at: http://news.met.police.uk/news/live-facial-technology-to-be-deployed-in-romford-356772. (Accessed: 16th April 2019)

127. Dearden, L. Man fined £90 after covering face during facial recognition trial in London. The Independent (2019).

128. Maurer, D. GAO-16-267, FACE Recognition Technology: FBI Should Better Ensure Privacy and Accuracy [Reissued on August 3, 2016]. (Government Accountability Office, 2016).

129. United States Senate. What Facial Recognition Technology Means For Privacy And Civil Liberties - Hearing before the Subcommittee on Privacy, Technology, and the Law of the Committee on the Judiciary United States Senate. (United States Senate, 2012).

130. Maurer, D. GAO-17-489T, FACE RECOGNITION TECHNOLOGY: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy. (Government Accountability Office, 2017).

131. Babcock, E. J. Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System. Federal Bureau of Investigation (2016). Available at: https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/interstate-photo-system. (Accessed: 3rd April 2019)

132. FBI. Next Generation Identification (NGI). Federal Bureau of Investigation (2016). Available at: https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi. (Accessed: 11th February 2019)

133. Criminal Justice Information Services. CJIS Annual Report 2016. (Federal Bureau of Investigation, 2016).

134. American Civil Liberties Union. Freedom of Information Act Request on Facial Recognition. (American Civil Liberties Union, 2019).

135. Del Greco, K. J. Law Enforcement's Use of Facial Recognition Technology. Federal Bureau of Investigation (2017). Available at: https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology. (Accessed: 11th February 2019)

136. Jouvenal, J. Police used facial-recognition software to identify suspect in newspaper shooting. The Washington Post (2018).

137. Federal Bureau of Investigation. Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit. Federal Bureau of Investigation (2016). Available at: https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit. (Accessed: 28th April 2019)

138. Steinthal, G. Image Stabilized Binoculars with Integrated 3D Facial Recognition Imaging

Capabilities - Final Technical Report. (StereoVision Imaging, Inc., 2013).

139. Scott, T. DHS/USSS/PIA-024 - Privacy Impact Assessment for the Facial Recognition Pilot. (U.S. Secret Service, 2018).

140. Nlets-International Justice and Public Safety Network. Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field. (2011).

141. Williams, E. Are you a target? Bonita Spring Florida Weekly (2016). Available at: https://bonitasprings.floridaweekly.com/articles/are-you-a-target/. (Accessed: 29th April 2019)

142. Taylor, L. Interagency Use of Facial Recognition... Does it work? (2013).

143. Pinellas County Sheriff's Office. History. Pinellas County Sheriff's Office Available at: https://www.pcsoweb.com/history. (Accessed: 29th April 2019)

144. Mak, A. What Crimes Actually Justify the Use of Facial Recognition Technology to Nab Suspects? Slate Magazine (2019). Available at: https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html. (Accessed: 30th April 2019)

145. National Law Enforcement and Corrections Technology Center. Florida Facial Recognition System Unmasks Identity, Boosts Arrests. National Law Enforcement and Corrections Technology Center - TECH Beat (2010).

146. Rogers, K. That Time the Super Bowl Secretly Used Facial Recognition Software on Fans. Vice (2016). Available at: https://www.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans. (Accessed: 6th May 2019)

147. Hamann, K. & Smith, R. Facial Recognition Technology: Where Will It Take Us? American Bar Association Available at: https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/. (Accessed: 6th May 2019)

148. American Civil Liberties Union. ACLU Calls for Public Hearings on Tampa's. American Civil Liberties Union (2001). Available at: https://www.aclu.org/news/aclu-calls-public-hearings-tampas. (Accessed: 6th May 2019)

149. Canedy, D. Tampa Scans the Faces in Its Crowds for Criminals. The New York Times (2001).

150. Churay, R. Purchase of Equipment to Enhance the MCSO Facial Recognition Unit at the ACTIC. (Maricopa County Sheriff's Office, 2017).

151. Brown, J. A Face in the Crowd. (2004). Available at: https://www.govtech.com/public-safety/A-Face-in-the-Crowd.html. (Accessed: 29th April 2019)

152. Eisenberg, E. & Steinhardt, B. Letter to Arizona School Officials on School Face Recognition. American Civil Liberties Union Available at: https://www.aclu.org/letter/letter-arizona-school-officials-school-face-recognition. (Accessed: 29th April 2019)

153. Maricopa County Sheriff's Office. Policy and Procedures - Identification Process. (Maricopa County Sheriff's Office, 2001).

154. Timberg, C. Racial profiling, by a computer? Police facial-ID tech raises civil rights concerns. The Washington Post (2016).

155. Perez, T. Maricopa County Sheriff's Office Findings Letter - December 15, 2011. (Department of Justice, 2011).

156. Stern, R. Sheriff Joe Arpaio's Office Commits Worst Racial Profiling in U.S. History, Concludes DOJ Investigation. Phoenix New Times (2011). Available at: https://www.phoenixnewtimes.com/news/sheriff-joe-arpaios-office-commits-worst-racial-profiling-in-us-history-concludes-doj-investigation-6655328. (Accessed: 29th April 2019)

157. Wong, J. C. & Gambino, L. Donald Trump pardons Joe Arpaio, former sheriff convicted in racial profiling case. The Guardian (2017).

158. Maricopa County Sheriff's Office. MCSO Investigation No. M081710. Internet Archive (2011). Available at: https://archive.org/details/89087-issueno17/page/n1. (Accessed: 29th April 2019)

159. Lessons Learned Information Sharing (LLIS). Facial Recognition Tools: Arizona Counter-Terrorism Information Center's Facial Recognition Database. (Department of Homeland Security).

160. Gabrielson, R. Intelligence Gap: How a Chinese National Gained Access to Arizona's Terror Center — ProPublica. ProPublica (2014). Available at: https://www.propublica.org/article/lizhong-fan. (Accessed: 29th April 2019)

161. Munnell, F. Recommend the Arizona Department of Public Safety Conduct a Formal Investigation Regarding Allegations of Serious Misconduct, Mismanagement, Unlawful Acts, and Hostile Work Environment Against Chief Deputy David A. Henderschott. (Maricopa County Sheriff's Office, 2010).

162. South Sound 911. About South Sound 911 - South Sound 911. South Sound 911 Available at: https://southsound911.org/about/. (Accessed: 29th April 2019)

163. Lucia, B. SPD is marrying mug shots with high tech. Crosscut (2014). Available at: https://crosscut.com/2014/02/seattle-police-facial-recognition-software-policy. (Accessed: 29th April 2019)

164. Best, C. 12.045 - Booking Photo Comparison Software. Seattle Police Department Manual Available at: https://www.seattle.gov/police-manual/title-12---department-information-systems/12045---booking-photo-comparison-software. (Accessed: 29th April 2019)

165. Best, C. Body Worn Video. Police | seattle.gov Available at: https://www.seattle.gov/police/about-us/body-worn-video. (Accessed: 29th April 2019)

166. The ACLU-WA and Seattle's Booking Photo Comparison Software. ACLU of Washington (2014). Available at: https://www.aclu-wa.org/blog/aclu-wa-and-seattle-s-booking-photo-comparison-software. (Accessed: 29th April 2019)

167. The Privacy Act of 1974. 5 U.S.C. § 552a (2012) (1974).

168. Donohue, L. Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age. (2012).

169. Cramer, H. The Face of Surveillance. The Century Foundation (2017). Available at: https://tcf.org/content/commentary/the-face-of-surveillance/?session=1&agreed=1. (Accessed: 28th April 2019)

170. Justice Department. Privacy Act of 1974; Implementation. Federal Register 82, 35651–35654 (2017).

171. Letter to FBI Requesting More Time to Respond to Proposed Privacy Act Exemptions for Next Generation Identification. Electronic Frontier Foundation (2016). Available at: https://www.eff.org/document/2016-letter-fbi-re-NGI. (Accessed: 28th April 2019)

172. Whittaker, Z. FBI can keep secret who's in its biometrics 'mega database,' says Justice Dept. | ZDNet. ZDNet (2017). Available at: https://www.zdnet.com/article/fbi-to-keep-secret-biometrics-database-justice-department/. (Accessed: 29th April 2019)

173. The E-Government Act of 2002. 116 STAT. 2900 PUBLIC LAW 107–347—DEC. 17 2002 (2002).

174. 18 U.S. Code § 2721 - Prohibition on release and use of certain personal information from State motor vehicle records. U.S. Code 18 U.S. Code § 2721, (1994).

175. REAL ID. Department of Homeland Security (2014). Available at: https://www.dhs.gov/real-id. (Accessed: 29th April 2019)

176. Hurd, W. & Kelly, R. Rise of the Machines Artificial Intelligence and its Growing Impact on U.S. Policy. (US House of Representatives, 2018).

177. Norton, E. H. Federal Police Camera and Accountability Act of 2018. (2018).

178. Cohen, S. Police CAMERA Act of 2019. (2019).

179. Lillo, C. Open Face: Striking the Balance Between Privacy and Security With The FBI's Next Generation Identification System. J. Legis. (2014).

180. LII Staff. Fourth Amendment. LII / Legal Information Institute (2010). Available at: https://www.law.cornell.edu/constitution/fourth_amendment. (Accessed: 2nd May 2019)

181. Katz v. United States, 389 U.S. 347 (1967). (1967).

182. Terry v. Ohio, 392 U.S. 1 (1968). (1968).

183. United States v. Dionisio, 410 U.S. 1 (1973). (1973).

184. United States v. Knotts, 460 U.S. 276 (1983). (1983).

185. United States v Karo, 468 U.S. 705 (1984). (1984).

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

187. Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty., 542 U.S. 177 (2004). (2004).

188. Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County. Oyez Available at: https://www.oyez.org/cases/2003/03-5554. (Accessed: 2nd May 2019)

189. Illinois v. Caballes, 543 U.S. 405 (2005). (2005).

190. United States v. Jones, 565 U.S. 400 (2012). (2012).

191. Colb, S. F. The Supreme Court Decides the GPS Case, United States v. Jones, and the Fourth Amendment Evolves: Part Two in a Two-Part Series of Columns. (2012). Available at: https://verdict.justia.com/2012/02/15/the-supreme-court-decides-the-gps-case-united-states-v-jones-and-the-fourth-amendment-evolves-2. (Accessed: 2nd May 2019)

192. Maryland v. King, 569 U.S. 435 (2013). (2013).

193. Carpenter v. United States, 585 U.S. ___ (2018). (2018).

194. California Constitution. (1879).

195. Florida Constitution. (1968).

196. Montana Constitution. (1972).

197. Wisconsin Legislature: 343.237. Wisconsin Statutes and Annotations 343.237,

198. Wisconsin Legislature: 165.8287. Wisconsin Statutes and Annotations 165.8287,

199. Thakkar, D. Biometric Regulations in the U.S. States. Bayometric (2018). Available at: https://www.bayometric.com/biometric-regulations-us-states/. (Accessed: 30th April 2019)

200. Geiger, H. Seeing Is IDing: Facial Recognition & Privacy. (Center for Democracy & Technology, 2012).

201. 2016 New Hampshire Revised Statutes :: Title VII - SHERIFFS, CONSTABLES, AND POLICE OFFICERS :: Chapter 105-D - BODY-WORN CAMERAS :: Section 105-D:2 - Use of Body-Worn Cameras. 2016 New Hampshire Revised Statutes Title VII - SHERIFFS, CONSTABLES, AND POLICE OFFICERS :: Chapter 105-D - BODY-WORN CAMERAS, (2016).

202. 2017 Oregon Revised Statutes :: Volume : 04 - Criminal Procedure, Crimes :: Chapter 133 - Arrest and Related Procedures; Search and Seizure; Extradition :: Section 133.741 - Law enforcement agency policies and procedures regarding video and audio

recordings; requirements; exceptions. 2017 Oregon Revised Statutes : 04 - Criminal Procedure, Crimes :: Chapter 133 - Arrest and Related Procedures; Search and Seizure; Extradition, (2015).

203. Ringrose, K. Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. Virginia Law Review Online 105, (2019).

204. 25 M.R.S. §4501 - Regulation of unmanned aerial vehicles. Maine Revised Statutes 25,

205. 20 V.S.A. § 4622 - Law enforcement use of drones. Vermont Statutes Annotated 20,

206. Michigan Compiled Laws Section 28.243. Michigan Compiled Laws

207. Wallace, M. P. A 6787 - Directs the commissioner of education to conduct a study on the use of biometric identifying technology; prevents the use of biometric identifying technology in schools. (2019).

208. Pogue, J. HB 783 - Prohibits school districts from collecting biometric information on students without the express written consent of parents or legal guardians. (2019).

209. Chau, E. AB 1281 - Privacy: facial recognition technology: disclosure. (2019).

210. Zawistowski, T. HB 5333 - An Act Prohibiting Retailers From Using Facial Recognition Software For Marketing Purposes. (2019).

211. Luneau, D. HB 536 - Adding biometric information to the consumer protection act. (2019).

212. Anderson, M. SB 284 - Relating to the collection of biometric data from employees. (2019).

213. Hudgins, Z. HB 1655 - 2019-20 Establishing guidelines for government procurement and use of automated decision systems in order to protect consumers, improve transparency, and create more market predictability. (2019).

214. Creem, C. S. S.1385 - An Act establishing a moratorium on face recognition and other remote biometric surveillance systems. (2019).

215. Abinanti, T. J. A1692. (2019).

216. Hughes, B. SB485. (2019).

217. Washington State Legislature. SB 5376 - 2019-20 Protecting consumer data. Washington State Legislature Available at: https://app.leg.wa.gov/billsummary?BillNumber=5376&Year=2019&Initiative=false. (Accessed: 11th February 2019)

218. Hasegawa, B. SB 5528 - Concerning the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology. (2019).

219. Ting, P. AB 1215 - Law enforcement: facial recognition and other biometric surveillance. (2019).

220. Provost, D. HB 2120 - An Act to establish a taskforce to develop a uniform code for police body-worn cameras and their recordings. (2019).

221. O'Connor, P. M. SB 1447 - An Act to regulate the use of unmanned aerial vehicles. (2019).

222. Englebright, S. A 4030 - Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof. (2019).

223. Dibble, S. SF 1430 - Unmanned aerial vehicles (drones) use by law enforcement agencies regulation. (2019).

224. Montigny, M. C. SB 1429 - An Act to promote transparency of facial recognition and driver's license photos. (2019).

225. Rachelson, B. H 470 - An act relating to requiring approval of the General Assembly prior to using certain law enforcement technology or information obtained from such technology. (2019).

226. Ordinance No. 7,592–n.S. - Adding Chapter 2.99 To The Berkeley Municipal Code, Acquisition And Use Of Surveillance Technology. Berkeley Municipal Code Ordinance No. 7,592, (2018).

227. San Francisco Board of Supervisors. [Administrative Code - Acquisition of Surveillance Technology].

228. Fussell, S. San Francisco Wants to Ban Government Face Recognition. The Atlantic (2019).

229. Engardio, J. P. Open Forum: San Francisco legislation would limit ability to fight crime with video cameras. San Francisco Chronicle (2019).

230. Tarantola, A. San Francisco could be the first US city to ban facial recognition tech. Engadget (2019). Available at: https://live.engadget.com/2019/04/24/san-francisco-first-us-city-ban-facial-recognition/. (Accessed: 4th May 2019)

231. Oakland's Facial Recognition Ban Passes First Administrative Hurdle. CBS San Francisco (2019). Available at: https://sanfrancisco.cbslocal.com/2019/05/03/oaklands-facial-recognition-ban-passes-first-administrative-hurdle/. (Accessed: 4th May 2019)

232. Knight, C. Cincinnati ranked second in country for body cam system, ahead of Louisville, Columbus, Cleveland. Cincinnati.com (2017). Available at: https://www.cincinnati.com/story/news/2017/11/14/cincinnati-ranked-second-country-body-cam-system-ahead-louisville-columbus-cleveland/862116001/. (Accessed: 4th May 2019)

233. Kravets, D. There's now only one US state where mug shots aren't public records. Ars Technica (2017). Available at: https://arstechnica.com/tech-policy/2017/03/theres-now-only-one-us-state-where-mugshots-arent-public-records/. (Accessed: 4th May 2019)

234. Feldman, A. E. What rights do people have to their own mug shots online? National Constitution Center – constitutioncenter.org (2013). Available at: https://constitutioncenter.org/blog/what-rights-do-people-have-to-their-own-mug-shots-online. (Accessed: 5th May 2019)

235. Duffin, K. The Business Of Posting Mugshots Online And Charging People To Take Them Down. NPR (2018).

236. Bidgood, J. After Arrests, Quandary for Police on Posting Booking Photos. The New York Times (2015).

237. Bashir, S. Surveillance Technologies. Tech | seattle.gov Available at: http://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies. (Accessed: 5th May 2019)

238. City of Seattle. Surveillance Technologies. City of Seattle Open Data Portal (Updated April 26, 2019). Available at: https://data.seattle.gov/City-Business/Surveillance-Technologies/ky9n-n26c. (Accessed: 5th May 2019)

239. Collateral Consequences Resource Center. 50-State Comparison Judicial Expungement, Sealing, and Set-aside. Restoration of Rights Project (2019). Available at: https://ccresourcecenter.org/state-restoration-profiles/50-state-comparisonjudicial-expungement-sealing-and-set-aside/. (Accessed: 5th May 2019)

240. The Stanford Open Policing Project. The Stanford Open Policing Project. openpolicing.stanford.edu (2019). Available at: https://openpolicing.stanford.edu/findings/. (Accessed: 5th May 2019)

241. Baumgartner, F. R., Epp, D. A. & Shoub, K. Suspect Citizens: What 20 Million Traffic Stops Tell Us About Policing and Race. (Cambridge University Press, 2018).

242. Choudhury, N. New Data Reveals Milwaukee Police Stops Are About Race and Ethnicity. American Civil Liberties Union (2018). Available at: https://www.aclu.org/blog/crim-

inal-law-reform/reforming-police-practices/new-data-reveals-milwaukee-police-stops-are. (Accessed: 5th May 2019)

243. Langton, L. & Durose, M. R. Police behavior during traffic and street stops, 2011. (US Department of Justice, Office of Justice Programs, Bureau of Justice ..., 2013).

244. Simoiu, C., Corbett-Davies, S. & Goel, S. The problem of infra-marginality in outcome tests for discrimination. Ann. Appl. Stat. 11, 1193–1216 (2017).

245. NAACP. Criminal Justice Fact Sheet. NAACP (2019). Available at: https://www.naacp.org/criminal-justice-fact-sheet/. (Accessed: 5th May 2019)

246. Stevenson, M. T. & Mayson, S. G. The Scale of Misdemeanor Justice. Boston Univ. Law Rev. 98, (2018).

247. Balko, R. Opinion - There's overwhelming evidence that the criminal-justice system is racist. Here's the proof. The Washington Post (2018).

248. Nellis, A. The Color of Justice: Racial and Ethnic Disparity in State Prisons. (The Sentencing Project, 2016).

249. Gross, S. R., Editor, S., Possley, M. & Stephens, S. R. K. Race and Wrongful Convictions in the United States. (2017).

250. FBI. Table 43 - Arrests by Race and Ethnicity, 2017 [12,599 agencies; 2017 estimated population 253,405,839]. 2017 Crime in the United States Available at: https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/tables/table-43. (Accessed: 6th May 2019)

251. U.S. Census Bureau. U.S. Census Bureau QuickFacts: UNITED STATES. Census Bureau QuickFacts Available at: https://www.census.gov/quickfacts/fact/table/US/PST045218. (Accessed: 6th May 2019)

252. Swearingen, R. FDLE - UCR Arrest Data. Florida Department of Law Enforcement Available at: https://www.fdle.state.fl.us/FSAC/Data-Statistics/UCR-Arrest-Data.aspx. (Accessed: 6th May 2019)

253. U.S. Census Bureau. U.S. Census Bureau QuickFacts: Florida. Census Bureau QuickFacts Available at: https://www.census.gov/quickfacts/fl. (Accessed: 6th May 2019)

254. Arizona Department of Public Safety. Crime in Arizona 2017. (Arizona Department of Public Safety , 2018).

255. U.S. Census Bureau. U.S. Census Bureau QuickFacts: Arizona. Census Bureau QuickFacts Available at: https://www.census.gov/quickfacts/az. (Accessed: 6th May 2019)

256. King County Department of Adult and Juvenile Detention. DAJD Statistics - King County. King County (2018). Available at: https://www.kingcounty.gov/depts/jails/about/dajd-stats.aspx. (Accessed: 6th May 2019)

257. U.S. Census Bureau. U.S. Census Bureau QuickFacts: King County, Washington. Census Bureau QuickFacts Available at: https://www.census.gov/quickfacts/kingcountywashington. (Accessed: 6th May 2019)

258. Balko, R. Opinion - How municipalities in St. Louis County, Mo., profit from poverty. The Washington Post (2014).

259. Gideon's Army. Driving While Black - A Report on Racial Profiling in Metro Nashville Police Department Traffic Stops. (Gideon's Army, 2016).

260. American Civil Liberties Union. Coalition Letter to the Department of Justice Civil Rights Division Calling for an Investigation of the Disparate Impact of Face Recognition on Communities of Color. American Civil Liberties Union (2016). Available at: https://www.aclu.org/letter/coalition-letter-department-justice-civil-rights-division-calling-investigation-disparate. (Accessed: 6th May 2019)

261. Comptroller General of the United States. Standards for Internal Control in the Federal Government. (Government Accountability Office, 2014).

262. Bashir, S. About the Surveillance Ordinance. Tech | seattle.gov Available at: https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-ordinance. (Accessed: 6th May 2019)

263. Bashir, S. Surveillance Advisory Working Group. Tech | seattle.gov Available at: https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/surveillance-advisory-working-group. (Accessed: 29th April 2019)

264. Seattle City Council. Body-Worn Video Program Community Engagement - Proviso Response Final Report. (Seattle City Council, 2017).

265. Federal Bureau of Investigation. Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Phase II System. Federal Bureau of Investigation (2018). Available at: https://www.fbi.gov/file-repository/pia-face-phase-2-system.pdf/view. (Accessed: 28th April 2019)

266. Pinellas County Sheriff's Office. Pinellas County Sheriff's Office. Pinellas County Sheriff's Office Available at: https://www.pcsoweb.com/. (Accessed: 29th April 2019)

267. Gullo, K. When Facial Recognition Is Used to Identify Defendants, They Have a Right to Obtain Information About the Algorithms Used on Them, EFF Tells Court. Electronic Frontier Foundation (2019). Available at: https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain. (Accessed: 26th March 2019)

268. Lynch v. Florida amicus brief. Electronic Frontier Foundation (2019). Available at: https://www.eff.org/document/lynch-v-florida-amicus-brief. (Accessed: 6th May 2019)

269. Ryan, M. M. Brady Rule. LII / Legal Information Institute (2009). Available at: https://www.law.cornell.edu/wex/brady_rule. (Accessed: 6th May 2019)

270. Conarck, B. Florida Courts Could Decide How Police Use Facial Recognition Tech. GovTech (2018). Available at: https://www.govtech.com/public-safety/Florida-Courts-Could-Decide-How-Police-Use-Facial-Recognition-Tech.html. (Accessed: 6th May 2019)

271. South Wales Police. Freedom of Information Request 1404-18. (2019).

272. Zetter, K. Of Course Congress Is Clueless About Tech—It Killed Its Tutor. Wired (2016).

273. Romm, T. 'I can understand about 50 percent of the things you say': How Congress is struggling to get smart on tech. The Washington Post (2018).

274. Kelly, L. & Bjarnason, R. Our 'modern' Congress doesn't understand 21st century technology. TechCrunch (2018).

275. Bass, D. Microsoft backs Washington state's facial recognition bill as Amazon mulls support. The Seattle Times (2019). Available at: https://www.seattletimes.com/business/microsoft-backs-washington-states-facial-recognition-bill-as-amazon-mulls-support/. (Accessed: 11th February 2019)

276. Menn, J. Microsoft turned down facial-recognition sales on human rights concerns. Reuters (2019).

277. Vincent, J. Microsoft denied police facial recognition tech over human rights concerns. The Verge (2019). Available at: https://www.theverge.com/2019/4/17/18411757/microsoft-facial-recognition-sales-refused-police-access. (Accessed: 23rd April 2019)

278. Pichai, S. AI at Google: our principles. Google (2018). Available at: https://www.blog.google/technology/ai/ai-principles/. (Accessed: 11th February 2019)

279. Locklear, M. Google pledges to hold off on selling facial recognition technology. Engadget (2018). Available at: https://www.engadget.com/2018/12/13/google-hold-off-selling-facial-recognition-technology/. (Accessed: 23rd April 2019)

280. Walker, K. AI for Social Good in Asia Pacific. Google (2018). Available at: https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/amp/. (Accessed: 7th May 2019)

APPENDIX

State	FRT Use	DMV	State/Local	FBI	Agency (current or former use)	Notable Legislation
Alabama	X		X	X	FBI	
Alaska						
Arizona	X		X		Arizona Department of Public Safety, Maricopa County Sheriff	
Arkansas	X	X	X	X	FBI, Arkansas Office of Driver Services, Arkansas Crime Information Center	
California	X		X		Los Angeles County Sheriff, San Diego Association of Governments, San Diego County Sheriff, Auburn PD, Los Angeles PD, Carlsbad PD, Chula Vista PD, Lincoln PD, San Diego PD, San Francisco PD, San Jose PD	**Constitutional Right to Privacy** **Proposed:** AB 1215, prohibiting the use of FRT in connection with officer cameras
Colorado	X		X		State law enforcement	
Connecticut	X	X	X		DMV, state law enforcement	
D.C.	-					
Delaware	X		X	X	FBI, state law enforcement	
Florida	X	X	X	X	FBI, Department of Highway Safety and Motor Vehicles, Department of Corrections, Jacksonville County Sheriff, Palm Beach County Sheriff, Pinellas County Sheriff, Miami Dade PD, Daytona Beach PD, Tampa PD, and many others (244 agencies total)	**Constitutional Right to Privacy**
Georgia	X		X		Georgia Bureau of Investigation	
Hawaii	X		X		Hawaii Criminal Justice Data Center, Honolulu PD	
Idaho						

281. Pledge - Safe Face Pledge. Safe Face Pledge Available at: https://www.safefacepledge.org/pledge. (Accessed: 7th May 2019)

Regulation and Use (present and former) of FRT across States

State	FRT Use	DMV	State/Local	FBI	Agency (current or former use)	Notable Legislation
Illinois	X		X	X	FBI, Illinois Secretary of State's Office, Illinois State Police, Chicago PD	*
Indiana	X	X	X		DMV, state law enforcement	
Iowa	X		X	X	FBI, Iowa Department of Public Safety	
Kansas	X	X			DMV	
Kentucky	X		X	X	FBI, Kentucky State Police	
Louisiana	-					
Maine	X		X		Maine State Police, Cumberland County Sheriff	**Passed:** ME Rev Stat 25 § 4501 (2015), restricting FRT in drones
Maryland	X		X		Department of Public Safety and Corrections, Maryland State Police, Montgomery County Police, Baltimore PD, Prince George's County PD	
Massachusetts	X		X		State law enforcement, Plymouth County Sheriff, New Bedford PD	**Proposed:** **S1385**, banning FRT without statutory authorization; **HB 2120**, prohibiting the use of FRT in connection with officer cameras; **SB 1447**, prohibiting FRT in drones; **SB 1429**, requiring FRT notices at the DMV
Michigan	X		X	X	FBI, Michigan State Police, DOJ, Detroit PD, Department of Corrections, Detroit and Southeast Michigan Information and Intelligence Center	**Passed:** **MI Compiled Laws Section 28.243 (2018)**, destruction of biometric data for individuals found innocent
Minnesota	X	X	X		Department of Public Safety Bureau of Criminal Apprehension, Department of Public Safety Driver Vehicle Services	**Proposed:** **SF1430**, prohibiting FRT in drones
Mississippi	X	X	X		Driver Services Division and Criminal Information Center of Mississippi Dept of Public Safety	
Missouri	X		X		Kansas City PD	
Montana						**Constitutional Right to Privacy**

State	FRT Use	DMV	State/Local	FBI	Agency (current or former use)	Notable Legislation
Nebraska	X	X	X	X	FBI, DMV, Nebraska Criminal Justice Information System, Nebraska State Patrol, Lincoln PD, Omaha PD	
Nevada	X	X	X		DMV, state law enforcement	
New Hampshire	-					**Passed:** **NH Rev Stat § 105-D:2 (2016)**, banning FRT in body-worn cameras
New Jersey	X		X		New Jersey State Police Regional Operations Intelligence Center	
New Mexico	X	X	X	X	FBI, state law enforcement, DMV, Albuquerque PD	
New York	X	X	X	X	FBI, DMV	**Proposed:** **A1692**, banning FRT without legal authorization issued by a court of competent jurisdiction; **A4030**, prohibiting FRT in drones
North Carolina	X	X	X	X	FBI, state law enforcement, DMV, Cumberland County Sheriff	
North Dakota	X		X	X	FBI, Bureau of Criminal Investigation	
Ohio	X		X		Ohio Attorney General's Office Bureau of Criminal Identification and Investigation, Ohio Department of Public Safety, other agencies (500+ total)	
Oklahoma	-					
Oregon	X	X			DMV	**Passed:** **OR Rev Stat § 133.741 (2017)**, banning FRT in body-worn cameras
Pennsylvania	X		X		Any law enforcement agency in the state (500+ total)	
Rhode Island	X	X	X		DMV, Rhode Island State Police, Rhode Island Corrections	
South Carolina	X		X	X	FBI, State Police	
South Dakota	X		X		State law enforcement	
Tennessee	X		X	X	FBI	

State	FRT Use	DMV	State/Local	FBI	Agency (current or former use)	Notable Legislation
Texas	X		X	X	FBI, Texas Department of Public Safety	* **Proposed:** **SB 485**, requiring a warrant, arrest or proximity to national border for law enforcement agencies to collect biometric identifiers
Utah	X		X	X	FBI, Department of Public Safety	
Vermont	X		X	X	FBI	**Passed:** **VT Stat Ann 20 § 4622 (2018)**, restricting FRT in drones; **Proposed:** **H470**, requiring General Assembly authorization before FRT use
Virginia	X		X		Northern Virginia Regional Information System, Virginia State Police, Fairfax County PD	
Washington	X		X		South Sound 911, King County Sheriff, Pierce County Sheriff, Snohomish County Sheriff, Seattle PD	* **Proposed:** **SB 5376**, establishing protections for personal data, including prohibiting the use of FRT by government agencies for surveillance in public spaces except for law enforcement or in an emergency and with an analysis by the Office of Privacy and Data Protection; **SB 5528**, prohibiting the government use of a FRT system
West Virginia	X		X		State law enforcement, West Virginia Intelligence Fusion Center	
Wisconsin	X	X	-		DMV	**Passed:** **WI Stat Ann § 343.237 & 165.8287 (2018)**, limit use of driver photos including "The photograph shall not be used as part of a photo lineup or photo array."
Wyoming	-					
TOTAL	43	15	40	18		**Passed:** 6 **Proposed:** 5

Sources: Nlets (2011), Geiger (2012), Garvie et al. (2016), GAO (2017)