Facial Recognition Technology: Conflict of Interest and Human Rights Implications

by

Kseniia Guliaeva

Submitted to

Central European University

Department of Legal Studies

In partial fulfillment of the requirements for the LLM degree

Supervisor: Professor Judit Sandor

Vienna, Austria

2024

ABSTRACT

This thesis explores a complex relationship between the deployment and use of Facial Recognition Technology (FRT) by law enforcement, the commercial interests of private FRT developers, and the protection of individual human rights.

Through a comparative analysis of case law as well as existing and emerging regulatory frameworks in the European Union and the United States, this study outlines, that the rapid advancement and adoption of FRT have resulted in significant governance and legal challenges, especially with regard to right to privacy and non-discrimination. It also highlights how a drive for profit and law enforcement objectives often overshadow human rights considerations, resulting in uncontrolled expansion of FRT and impairing the establishment of stringent legal frameworks that prioritize human rights. The findings suggest that existing regulatory approaches display numerous deficiencies, particularly related to the lack of transparency, oversight, and broad discretion granted to law enforcement authorities in using FRT.

The thesis then offers initial recommendations for improving existing legal frameworks. Stressing the need for greater transparency and accountability, it calls for adopting new approaches that further restrict the discretionary use of FRT by law enforcement and promote broader societal engagement in governance processes. This strategy aims to prevent further degradation of the rights in question and ensure alignment of FRT use and deployment with core human rights principles.

TABLE OF CONTENTS

1. INTRODUCTION

In the modern digital era, technology advances at an unprecedented pace, intertwining with our daily lives and redefining the scope of privacy, security, and freedom. Facial Recognition Technology (FRT) is no exception. While millions, if not billions of people use facial recognition technologies to unlock their phones, apply Instagram filters, or categorize their photos, the technology is also widely used by Big Tech companies to develop comprehensive marketing strategies and law enforcement authorities to identify potential suspects, find missing individuals, and otherwise protect public order and safety. Facial recognition technology is currently at the forefront of its development, with technological innovations rapidly outpacing the existing regulatory frameworks and posing numerous threats to individual human rights.

A prominent example of human rights violations linked to FRT is the Clearview AI case. Clearview AI amassed billions of images from social media and various websites without obtaining users' consent, creating a facial recognition database heavily utilized by law enforcement agencies. This lack of consent and transparency raised serious concerns about privacy and unauthorized surveillance and ended up in court. In May 2022, Clearview AI settled a lawsuit by agreeing to stop selling its database to private persons and business entities across the United States, while still allowing its use by federal authorities and state agencies outside of Illinois.

Thus, the selection of the topic is grounded in the rapid development and expansion of the use of FRT by law enforcement authorities and private companies and an urgent need to examine its interplay with the human rights frameworks. The current transitional legal frameworks governing FRT are displaying significant governance and legal gaps that the governments are now seeking to eliminate. This evolving legal landscape presents a ripe area for scholarly research in understanding what are the main challenges and how they are

approached in the emerging legislation. The thesis aims to contribute to the identification of existing legal, and governance gaps and the development of balanced and informed legal frameworks and policies that foster innovation without undermining human rights protection.

The thesis explores and analyses the legal, political, and ethical dimensions of the use by law enforcement authorities of FRT developed by private companies. It examines the interplay between technological advancements and human rights, particularly focusing on the right to privacy and non-discrimination. It methodically explores the definition and technical capabilities of facial recognition technology, scrutinizes the legal frameworks and upcoming legislation governing its use, and examines the diverse human rights implications.

Through a comparative analysis of existing international and national case law, with a special focus on jurisdictions such as the United States and the European Union, the thesis identifies the existing governance gap by conducting a critical evaluation of the current landscape of FRT usage and its far-reaching implications for privacy and other human rights. The thesis also explores an existing conflict of interest among the private companies producing FRT software and databases, law enforcement authorities that are often the primary beneficiaries of the FRT developed by the private sector, and the human rights of individuals affected by the use of FRT.

This study aims to broadly analyze the legal and political dimensions of the utilization of FRT by law enforcement authorities, particularly focusing on technologies developed by private companies. The primary objective is to assess the implications of such usage on human rights, identify prevailing challenges, and propose potential pathways for the future. Governments and private companies have increasingly collaborated in the market for digital surveillance tools, including FRT.[1] These collaborations often occur at global and regional trade shows designed to connect government needs with private sector solutions, however, the extent

[1] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, (28 May 2019) A/HRC/41/35, para 15-20.

to which these companies are subjected to human rights due diligence remains largely unknown.[2]

The analysis will focus on existing legal regulations (relevant international law instruments, EU regulatory framework, and relevant laws in the United States) and the public statements of political actors that are relevant to the topic.

The regulatory acts and the relevant case law will be analyzed with the use of qualitative analysis, including content analysis of legal texts and case study analysis, comparative legal analysis methods designed to understand different approaches to the use and regulation of FRT in different jurisdictions. An interdisciplinary approach incorporating technological, political, legal, and ethical insights will be employed to interpretation and implementation of legal frameworks.

The anticipated limitations of this analysis derive from the fast-paced development of the FRT and the dynamic nature of related legal frameworks. The analysis may face challenges in keeping pace with rapidly changing laws and emerging technologies, potentially resulting in an incomplete or outdated representation of applicable regulations. Additionally, access to resources may be challenging, as comprehensive and up-to-date information on facial recognition technology regulations and case law across various jurisdictions may not be readily available or easily accessible.

It is important to stress, that the legal frameworks analyzed herein do not address all legal acts relevant to regulating the FRT in the selected jurisdictions and do not expressly and in detail name all relevant rights and obligations, as this would be impossible within the framework of the current thesis. Rather, the thesis aims to provide a general overview, and the legal acts and bills presented here have been chosen as illustrative examples of specific legislation that can give a general idea about the existing trends, approaches, and issues,

[2] Id.

prevalent in the chosen jurisdictions. The thesis also does not aim to address the use of FRT in the military sector and the regulations that relate to the export of dual-use technologies, both of which could form the basis for separate studies.

Firstly, the thesis delves into technology's technical capabilities and potential applications, with the view to establishing a viable definition of FRT. Subsequently, the study briefly explores the existing normative and legal framework governing the use and deployment of FRT with a focus on the regulation addressing enforcement authorities. Moving forward, the thesis undertakes an examination of human rights impacted by the use of facial recognition technology. In this context, the thesis conducts an analysis of existing case law at both international and national levels, with a specific emphasis on the legal landscapes of the United States. Finally, the study addresses identified governance gaps and explores identified legal and ethical constraints associated with the FRT. Specific deficiencies where current legislation and policies may fall short in safeguarding human rights are pinpointed. The study then discusses potential strategies to minimize human rights violations and develop recommendations or frameworks to fill these governance gaps. The conclusion summarizes the findings of the research and underscores the importance of developing robust legal frameworks to balance technological advancements with human rights protections.

2. DEFINITION AND APPLICATIONS OF FRT

The emergence of FRT dates back to the 1960s when Woodrow Willson Bledsoe came up with a way to manually record coordinates of persons' facial features and upload this data into a computer.[3] The system was slow and rarely rendered any useful results, however, demonstrated that faces could indeed be used for identification and picked the interest of law enforcement authorities.[4] Significant technological developments in the area have been made between the 1970s and 1990s, substantially automating the process of face detection and recognition and improving accuracy.[5] A large portion of these developments was based on the rapid advancement of digital photography and the introduction of Adobe Photoshop in the 1980s.[6] 1996 US FERET Program is claimed to have been the first facial database.[7] The first testing of the FRT that became widely known to the public took place during the 2001 Super Bowl in the United States when law enforcement officials used FRT to scan the crowd at the stadium and identified 19 wanted criminals.[8] The next breakthrough occurred in the 2010s, with computers getting powerful enough to train neural networks necessary for a smooth operation of the FRT.[9] In 2011, FRT was used to "confirm the identity of Osama bin Laden" killed in the course of the US operation.[10] President Trump issued an executive order prescribing the use of FRT at the top 20 airports in the United States to ensure identity verification of individuals crossing US borders.[11]

[3] Klosowski, Thorin. "Facial Recognition Is Everywhere. Here's What We Can Do About It." Wirecutter: Reviews for the Real World, July 15, 2020, available at - https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/; Candriam, *Facial Recognition and Human Rights:Investor Guidance*, March 2021, 5; Smith, Marcus, and Seumas Miller. 2021. *Biometric Identification, Law and Ethics*. 1st ed. Cham, Switzerland: Springer Nature, 21.
[4] Id.
[5] Candriam, 5; Dauvergne, Peter. 2022. *Identified, Tracked, and Profiled: The Politics of Resisting Facial Recognition Technology*. Cheltenham, England: Edward Elgar Publishing, 3.
[6] I. Berle, FACE RECOGNITION TECHNOLOGY, Law, Governance and Technology Series 41, Springer Nature Switzerland AG 2020, p.1-2.
[7] Candriam, 5; Dauvergne, 3.
[8] Id.
[9] Id.
[10] Id.
[11] Id; Smith, Marcus, and Seumas Miller, 23.

All major Big Tech companies also rolled out different tools employing FRT. In 2014, Facebook introduced its DeepFace software using FRT for tagging individuals on photos. In 2014, Google introduced Android's Trusted Face to unlock smartphones (which was later pulled out),[12] and in 2015 publicly revealed analogous "FaceNet" FRT used by Google Photos to automatically categorize pictures by person and tag individuals.[13] The same year Microsoft launched its Windows Hello biometric identification for Windows 10 devices.[14] On 30 November 2016, Amazon launched its FRT 'Rekognition', a cloud-based software as a service (SaaS) platform, that allows its users to "identify people, activities, objects, text, and scenes in images and videos".[15] Apple introduced its 'FaceID' FRT in 2017 with the release of the iPhone X and has incorporated it in almost all of the following models since (except for SE).[16] FaceID scans your face, runs it against the database, and depending on the result of the search, decides whether to deny or grant you access to your iPhone.[17]

The above evolution of the FRT from its inception to the present day is a remarkable story of significant transformation. Having started as a manual method of categorization, the FRT rapidly evolved into a comprehensive automated algorithm that each of us interacts with daily. Its widespread use in a range of domains, from law enforcement to marketing and consumer electronics, demonstrates its exceptional utility and impact. This progression is not only a testament to a huge potential for further advancement but also a signal to urgently consider legal, ethical, privacy, and other concerns associated with its use.[18]

[12] Khoury, Rita El. *Trusted Face Smart Unlock Method Has Been Removed from Android Devices*, Android Police, September 4, 2019, available at - https://www.androidpolice.com/2019/09/04/trusted-face-smart-unlock-method-has-been-removed-from-android-devices/.
[13] Schroff, Florian, Dmitry Kalenichenko, and James Philbin. *FaceNet: A Unified Embedding for Face Recognition and Clustering*, June 1, 2015, available at - https://doi.org/10.1109/cvpr.2015.7298682.
[14] Statt, Nick, *Microsoft's Windows Hello Will Make Your Face, Finger or Iris the New Sign-In*, CNET, March 17, 2015, available at - https://www.cnet.com/news/privacy/microsoft-introduces-windows-hello-for-signing-in-with-your-face-finger-or-iris/.
[15] Indla, Raghavendra Kumar, *An Overview on Amazon Rekognition Technology*, 2021, Electronic Theses, Projects, and Dissertations. 1263, 3.
[16] Obari, Dreamchild, *What Is Apple's Face ID and How Does It Work?*, MUO, June 12, 2023, available at - https://www.makeuseof.com/apple-face-id-explained/.
[17] Id.
[18] Smith, Marcus, and Seumas Miller, 28-35.

FRT is an AI-based technology, that could be defined as "automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates".[19] FRT allows to automatically identify individuals by matching digital face images through a comparison of facial features extracted from the images;[20] it also allows to compare face images obtained from CCTV cameras with images stored in the existing databases, which is referred to as 'live' FRT.[21] Every system of facial recognition works differently, however, the process usually comprises at least three steps: detection, analysis, and recognition.[22]

Detection, as the first step, implies the process of identifying a face.[23] This is achieved using artificial intelligence algorithms, machine learning, statistical analysis, and image processing to identify human faces and distinguish them from other objects and landscapes.[24] Face detection usually starts from the search for human eyes, which are considered to be the easiest feature to detect.[25] Once the algorithm finds eyes, it goes on to identify other landmark facial features such as nose, nostrils, chin, and mouth to conclude, after running several more crosschecks, that it has indeed found a face.[26] To improve the accuracy of the face detection technology, the algorithms are trained on large amounts of images depicting faces and non-

[19] Council of Europe, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, *Guidelines on Facial Recognition*, June 2021, 5.
[20] I. Berle, FACE RECOGNITION TECHNOLOGY, Law, Governance and Technology Series 41, Springer Nature Switzerland AG 2020, 2; European Union Agency for Fundamental Rights, *Facial Recognition Technology: fundamental rights considerations in the context of law enforcement*, 2019, 1-2.; For more detail on how facial recognition technology works, see e.g. Introna, L. and Nissenbaum, H. (2010), *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Lancaster University Management School Working Paper 2010/030.
[21] Smith, Marcus, and Seumas Miller, 22.
[22] Klosowski, Thorin, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, Wirecutter: Reviews for the Real World, July 15, 2020, available at - https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/; Dauvergne, 4.
[23] European Data Protection Board, *Guidelines 05/22 on the use of facial recognition technology in the area of law enforcement*, 12 May 2022, 7.
[24] Barney, Nick, and Corinne Bernstein, *Face Detection*, Enterprise AI, April 20, 2023, available at - https://www.techtarget.com/searchenterpriseai/definition/face-detection.
[25] Id.
[26] Id.

facial objects.[27] Everyday user has most probably encountered this technology while using auto-focus technology in cameras, that draw a yellow rectangle around a face.[28]

In the course of **analysis** (otherwise called face mapping), the algorithm maps detected faces by measuring the shape of the face and the distance between different facial features.[29] There are around 80 landmark facial features such as "distance between the eyes, the depth of the eye socket, and the shape of the nose", which do not change with age or varying weight.[30] Upon gathering this data, the algorithm transforms it into numerical codes, often referred to as 'faceprints'.[31] This is used, for example, by Snapchat to apply filter features to mapped faces.[32]

The third step relates to actual **recognition**. The algorithm runs a faceprint against the faceprints stored in the database of other faces in an attempt to find a matching face (verification process), identify an individual (identification process)[33] and/or apply certain classification (classification process).[34] The latter implies extracting data from the faceprint to determine various attributes "such as age, gender, or emotional state".[35]

The technology has gained significant traction in law enforcement, "with 20 out of 42 federal law enforcement agencies" employing it, as per a 2021 Government Accountability Office report.[36] Besides its widespread use in law enforcement, facial recognition technology

[27] Id. Smith, Marcus, and Seumas Miller, 23.
[28] Klosowski, Thorin. *Facial Recognition Is Everywhere. Here's What We Can Do About It*, Wirecutter: Reviews for the Real World, July 15, 2020, available at - https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.
[29] Smith, Marcus, and Seumas Miller, 22; European Data Protection Board, *Guidelines 05/22 on the use of facial recognition technology in the area of law enforcement*, 12 May 2022, 7.
[30] Ramya Mohanakrishnan, *Top 11 Facial Recognition Software in 2021*, September 2, 2021, available at - https://www.spiceworks.com/it-security/identity-access-management/articles/facial-recognition-software/.
[31] Smith, Marcus, and Seumas Miller, 22.
[32] Le, James, *Snapchat's Filters: How Computer Vision Recognizes Your Face*, Medium, July 25, 2018, available at - https://data-notes.co/snapchats-filters-how-computer-vision-recognizes-your-face-9907d6904b91#:~:text=This%20is%20done%20with%20the,the%20image%20that%20is%20provided.
[33] Smith, Marcus, and Seumas Miller, 22.
[34] European Parliamentary Research Service, *Regulating Facial Recognition in the EU*, September 2021, available at - https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf; Dauvergne, 5.
[35] European Parliamentary Research Service, *Regulating Facial Recognition in the EU*, September 2021, available at - https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf; Smith, Marcus, and Seumas Miller, 22.
[36] Government Accountability Office (GAO), *"Facial Recognition Technology: Federal Law Enforcement*

(FRT) is now being employed at airports and travel centers. The Transportation Security Administration (TSA) has broadened a pilot initiative to employ FRT for traveler identity verification at security checkpoints in 25 US airports.[37] Concurrently, Customs and Border Protection utilizes FRT to monitor travelers exiting the country at 32 US airports and for arrivals at all international airports across the nation.[38]

As face recognition software expands, so does the effectiveness and intrusiveness of these technologies, driven by the accumulation of vast databases of facial images.

Facial Recognition Technology (FRT) joins a line of identification tools like fingerprinting and DNA comparison, stirring similar privacy and fairness concerns. Surveillance cameras, cell phone tracking, and license plate readers have long been in use, each with its own set of benefits and challenges.[39] While some issues overlap with previous technologies, FRT brings its own unique complexities and intensifies existing concerns.[40]

FRT offers cost-effective, scalable, and non-contact identification solutions.[41] It facilitates rapid processing of large crowds at checkpoints, quick identification of high-risk individuals in crowded venues, and aids law enforcement in criminal investigations by generating leads from crime scene images or identifying missing persons.[42]

FRT possesses unique characteristics that set it apart from other identification methods like fingerprinting, handprint analysis, iris scanning, DNA comparison, cell phone tracking, license plate readers as well as human review of the surveillance footage that have long been

Agencies Should Have Better Awareness of Systems Used by Employees, 2021, available at - https://www.gao.gov/products/gao-21-105309.

[37] K.V. Cleave, 2023, *TSA Expands Controversial Facial Recognition Program*, CBS News, June 5, https:// www.cbsnews.com/news/tsa-facial-recognition-program-airports-expands.

[38] GAO, 2022, *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues*, available at - https://www.gao.gov/products/gao-22-106154.

[39] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance. Washington, DC: The National Academies Press (2024), 23.*

[40] Id.

[41] Id.

[42] Id.

used in both forensic and non-forensic settings.[43] It is highly personal, leveraging the distinctiveness of individual faces, which are more visible and easily identifiable than other body parts like iris patterns or fingerprints.[44] FRT can be deployed remotely and is closely linked to an individual's identity, unlike other tracking techniques such as license plate readers.[45] Moreover, FRT benefits from pervasive access to a vast array of facial images captured by government, business, and personal cameras, making it challenging to opt out of data collection.[46] It is widely available to both public and private sectors and can be applied to stored images and videos retroactively.[47] The technology operates stealthily, making it difficult to detect its usage and purpose in various settings.[48] Additionally, FRT offers cost-effective automation compared to human review of camera footage or DNA testing, making it an inexpensive identification solution.[49] These characteristics make FRT an efficient tool for recognition and surveillance, raising concerns about privacy, surveillance, and individual autonomy in areas ranging from personal device access to law enforcement and public safety.[50]

Government agencies gather facial images for identity documents like driver's licenses and passports, and through mugshots during arrests.[51] Private entities also contribute by collecting images from various sources including their premises or the Internet.[52] The distinction between public and private FRT databases is often blurred, with law enforcement frequently utilizing databases created by private entities.[53]

Given that, FRT also presents unprecedented governance challenges due to the multitude of legal and policy issues that arise throughout its development, deployment, and

[43] Id.
[44] National Academies of Sciences, Engineering, and Medicine, 2024, 26.
[45] Id.
[46] Id.
[47] Id.
[48] Id.
[49] Id.
[50] Id.
[51] National Academies of Sciences, Engineering, and Medicine, 2024, 21.
[52] Id.
[53] Id.

usage. These issues are complex and mostly unsettled, as the governance of FRT depends on the specific contexts in which it is employed, the level of regulation at play – international, national, state, and local, the existence or rather absence of specific legislation governing FRT and the substantive norms of intellectual property, privacy, law enforcement and other laws and regulations that are used to fill in the gaps.

Compounding the challenges is the societal impact of FRT, which touches on core values such as freedom from surveillance by state or private entities and control over one's personal data. The technology's use can interfere with and significantly influence values related to privacy, civil liberties, and human rights.

Thus, FRT presents a sophisticated mix of "artificial intelligence, deep learning, machine learning and image processing techniques" and algorithms, designed to detect, identify, and verify individuals through the use of digital facial images.[54] The more data and facial images are being used by the FRT, the more advanced it becomes. As FRT continues to evolve and improve its accuracy rate, we need to consider the impact it might have on a myriad of human rights.

[54] Dauvergne, 4.

3. NORMATIVE AND LEGAL FRAMEWORK

Despite the widespread adoption of FRT, its deployment has outpaced the development of comprehensive legal frameworks, leading to a patchwork of regulations that vary significantly across jurisdictions. This chapter aims to provide a broad outlook into the normative and legal frameworks governing the use of FRT by private companies and law enforcement authorities in particular. It will explore how the development and use of FRT is governed at the international, regional, and national levels to provide a general idea of the level of regulation and its comprehensiveness, as well as to potentially identify trends and different approaches used in legislating on the matter. The regional framework will be examined using the example of the European Union, which is considered to be a comprehensive and cautious legal regulator, while the national legal framework will be considered using the example of the United States, having a distinct regulatory philosophy.

International level

International law does not offer any specific convention addressing FRT. While there are numerous human rights instruments that provide a broad framework for protecting individual rights relevant to the use of FRT, none of them specifically refer to FRT and its unique challenges. This absence is understandable given the rapid pace of technological advancement, but it necessitates an evolutionary interpretation of existing legal instruments to ensure they adequately cover the implications of FRT. We begin by examining the specific instruments and mentions of FRT that have taken place at the international level in order to grasp existing international perspectives, better contextualize national and regional approaches and identify best practices and potential areas for improvement in the regulation of FRT.

United Nations

At the United Nations, a report presented by the Office of the High Commissioner for Human Rights (OHCHR) in 2021 to the Human Rights Council and submitted in accordance with Human Rights Council resolution 42/15, highlighted the need to ban AI applications that cannot "comply with international human rights law".[55] Focusing on FRT used by law enforcement and national security authorities, the report noted that remote biometric recognition significantly enhances state authorities' ability to "systematically identify and track individuals in public spaces", undermining individuals' privacy and potentially affecting their freedom of expression, peaceful assembly, association, and movement.[56] The report also called for a "moratorium on the use of remote biometric recognition in public areas" until accuracy and discrimination concerns are resolved and compliance with strong privacy and data protection standards is ensured.[57] This reflects a cautious approach towards the use of FRT, emphasizing the need to ensure compliance with human rights standards and addressing significant concerns about privacy, discrimination, and fundamental freedoms before allowing its widespread use.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his report on 'Surveillance and human rights' enumerated FRT among the types of surveillance often leading to unlawful discrimination. [58] The UN Special Rapporteur emphasized the example of China which extensively uses these technologies to monitor and track the movements of Uighurs based on their appearance,[59] highlighting the

[55] Human Rights Council, *Report of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age*, 13 September 2021, A/HRC/48/31, paras 25-28.
[56] Human Rights Council, *Report of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age*, 13 September 2021, A/HRC/48/31, paras 25-28; See also European Data Protection Board and European Data Protection Supervisor, joint opinion 5/2021, para. 30; A/HRC/44/24, para. 34, and A/HRC/41/35.
[57] Human Rights Council, *Report of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age*, 13 September 2021, A/HRC/48/31, para 45.
[58] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, (28 May 2019) A/HRC/41/35, para 50.
[59] See Paul Mozur, *One month, 500,000 face scans: how China is using A.I. to profile a minority*, *New York Times*, 14 April 2019.

extensive and intrusive nature of these surveillance practices.[60] He also noted that much of the technology is produced domestically by state-owned and private enterprises.[61]

On March 7, 2024, the UN special rapporteur on the rights to freedom of peaceful assembly and association released a "Practical toolkit for law enforcement officials to promote and protect human rights in the context of peaceful protests".[62] The model protocol, published on January 31, 2024, lays out principles for the lifecycle of artificial intelligence systems, while the subsequent components provide action-oriented checklists, principled-based guidance for using digital technologies, and a handbook for law enforcement. These resources emphasize the importance of respecting human rights, ensuring transparency and oversight, establishing accountability, promoting equality, protecting privacy, enhancing reliability, and enabling safe innovation in the context of peaceful protests.[63] While the toolkit addresses various aspects of digital technology use, it underscores the need for a careful balance between facilitating peaceful assembly and avoiding intrusive surveillance or data collection methods, including in the context of using FRT.[64]

As evidenced by the above reports, the UN's approach is characterized by a deliberate and precautionary methodology, prioritizing the protection of human rights and ethical considerations in the deployment of FRT. Despite a strong emphasis on stringent compliance with human rights standards, however, the UN does not offer any extensive guidance on the matter, demonstrating a critical gap that underscores the need for more comprehensive and

[60] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights* (28 May 2019) A/HRC/41/35, para 50.
[61] See also A/HRC/39/29, para. 14.
[62] UN Special Rapporteur on the rights to peaceful assembly and of association, Clément Nyaletsossi Voule, *Human rights compliant uses of digital technologies by law enforcement for the facilitation of peaceful protests (2024), available at* - https://www.ohchr.org/en/documents/tools-and-resources/practical-toolkit-law-enforcement-officials-promote-and-protect-human.
[63] Id.
[64] Id.

binding international regulations specifically tailored to address the unique challenges posed by FRT.

United Nations Guiding Principles on Business and Human Rights

The UN Guiding Principles on Business and Human Rights (UNGPs) are also relevant for understanding and regulating the interplay between private companies, governments, and individuals in the development and use of FRT.[65] The Guiding Principles emphasize that states have a duty to protect human rights against abuses by third parties, including business entities by implementing and enforcing laws that require businesses to respect human rights.[66] Businesses, on the other hand, have a responsibility to respect human rights by conducting due diligence to identify, prevent, and mitigate human rights impacts, ensuring their products do not contribute to human rights abuses.[67] Both states and businesses must ensure that individuals adversely affected by business activities have access to effective remedies through judicial and non-judicial mechanisms.[68]

However, the non-binding nature of the UNGPs prevents them from properly filling out the governance gap. With little to no mandatory obligations placed on corporations, businesses are essentially asked to voluntarily adopt ethical standards and practices regarding the export of such technologies and engage in corporate social responsibility. However, with the large monetary incentives from selling their technology, corporate social responsibility falls short of its promise.

The currently negotiated UN Binding Treaty on Business and Human Rights would make an invaluable contribution to ensuring corporate and state responsibility for human rights

[65] United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, United Nations (2011), available at - https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[66] Id.
[67] United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, United Nations (2011), Articles 17-21, available at - https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[68] United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, Articles 25-31..

protection in the context of FRT. For example, Article 6 of the current Third Draft outlines the obligation of states to adopt legislative, administrative as well as all other measures to oblige business entities to conduct human rights due diligence.[69] Such due diligence shall include regular conduct and publication of human rights impact assessment reports, integrate a gender and race perspective, and take particular care of vulnerable and affected groups (ex. journalists, human rights defenders, indigenous people).[70] The Draft seeks to establish universal standards, ensuring consistency and predictability for transnational corporations. This uniformity is critical in discouraging businesses from exploiting disparities in human rights protections and choosing jurisdictions with less stringent protections for their operations.

The Draft refers to adverse impact of businesses on all internationally recognized human rights[71] and requires states to establish a system of legal corporate liability providing access to remedies, having jurisdiction with regard to potential human rights violations committed by businesses and reinforce their accountability regardless of the place of their registration and operation.[72] The Draft, however, does not provide for an international tribunal or any other international enforcement mechanism. Thus, the responsibility of holding corporations accountable for human rights violations would still be vested with national or regional institutions, which shall make sure that their regulations extend to cover global operations of private companies and that the latter could be held accountable if such operations do not comply with the established legal standards.

Therefore, while the UNGPs provide essential guidelines, their voluntary nature limits their impact on regulating FRT. The proposed UN Binding Treaty on Business and Human

[69] Human Rights Council, *Updated draft legally binding instrument (clean version) to regulate, in international human rights law, the activities of transnational corporations and other business enterprises*, available at - https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/igwg-transcorp/session9/igwg-9th-updated-draft-lbi-clean.pdf ("Updated Third Draft"), Articles 1.8, 6.
[70] Updated Third Draft, Article 6.4.
[71] Updated Third Draft, Article 1.2.
[72] Updated Third Draft, Articles 7-9.

Rights, with its mandatory provisions for human rights due diligence, and corporate accountability, would signify a substantial step forward. It has the potential to create a more robust and uniform regulatory environment for the development and distribution of FRT, ensuring that both businesses and governments uphold human rights standards. However, it is not clear if and when the binding treaty will be adopted, casting doubt on its potential impact and leaving little hope for immediate improvements in corporate and state accountability for the abuses of FRT.

AI Convention

On 17 May 2024, the Council of Europe adopted a pioneering international framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, that will be open for signature (including to states beyond Europe) on 5 September 2024 and will become effective three months after at least five signatories, including three Council of Europe member States, agree to be bound by it.[73] The treaty establishes regulations spanning the entire AI lifecycle, managing associated risks, and encouraging responsible innovation.[74] Employing a risk-oriented strategy, it mandates a thorough evaluation of potential adverse effects throughout the design, implementation, operation, and dismantling phases of AI systems.[75] Even though the treaty does not explicitly address the use of FRT, the FRT falls within the scope of the definition of "artificial intelligence systems" and thus, may prove important in regulating the technology.

The preamble of the Convention expresses concern over the abuse of artificial intelligence systems in violation of international human rights law, in particular, in cases of its use for "arbitrary or unlawful surveillance and censorship practices that erode privacy and

[73] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, 17 May 2024, Article 30, available at - https://rm.coe.int/1680afae3c.
[74] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, 17 May 2024, available at - https://rm.coe.int/1680afae3c.
[75] Id.

individual autonomy".[76] Article 4 of the Convention stipulates that every Party must implement or uphold measures to guarantee that all stages of artificial intelligence systems are compliant with human rights obligations set out in international and national laws.[77] Chapter III then outlines general principles that each Party is required to abide by in dealing with artificial intelligence systems, including measures to respect human dignity and individual autonomy, ensure transparency and oversight, establish accountability for adverse impacts on human rights, promote equality and non-discrimination, protect privacy and personal data, enhance reliability, and facilitate safe innovation through controlled environments for AI system development and testing.[78] As will be outlined below, these principles bear particular importance for the development and use of FRT as well.

The Council of Europe's adoption of the AI Convention marks a pivotal moment in the regulation of artificial intelligence, signaling a concerted effort to uphold human rights, democracy, and the rule of law amid technological advancements. The Convention addresses critical concerns regarding the ethical and societal implications of AI systems and establishes basic principles to create a baseline for future regulations. While the Convention does not explicitly mention Facial Recognition Technology (FRT), its broad principles have significant implications for the development and application of this technology, particularly in safeguarding privacy, promoting transparency, and ensuring accountability. Thus, the Convention sets a precedent for international cooperation and governance in navigating the complex intersection between technology and human rights, paving the way for a more ethical and inclusive approach to AI implementation. However, its actual impact will only become

[76]Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, Preamble.
[77] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, Article 4.
[78] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, Chapter III.

evident once it enters into force, as its implementation and enforcement will determine how effectively it safeguards human rights and shapes the development and deployment of FRT.

Regional level - European Union

European regulatory framework led by the General Data Protection Regulation,[79] imposing strict rules on the processing of biometric data, and the Law Enforcement Directive,[80] regulating law enforcement's use of personal data, including FRT, provides a more unified and strict approach to the use of FRT. This section will focus on the proposed AI Act and the Law Enforcement Directive, as these instruments provide more specific regulations and guidelines relevant to the use of FRT by private companies and law enforcement authorities. The GDPR, while foundational, serves as a general framework for data protection and will not be addressed in detail here.

AI Act

The AI Act represents a landmark regulation by the European Union, being the first comprehensive legal framework on artificial intelligence introduced by a major regulator. Following the final endorsement by the Council of the EU on May 21, 2024, the AI Act will become effective 20 days after its publication, with full implementation set for 24 months thereafter, except for specific provisions outlined in Article 113.[81]

The Act categorizes AI systems based on their risk levels.[82] AI systems that pose unacceptable risks are prohibited.[83] These include "biometric categorization systems inferring

[79] 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.
[80] 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.
[81] EU Artificial Intelligence Act, 19 April 2024, Article 113, available at - https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf
[82] EU Artificial Intelligence Act, Article 2.
[83] EU Artificial Intelligence Act, Article 5.

sensitive attributes" such as "race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation" unless used for labeling or "filtering lawfully acquired biometric datasets" or for law enforcement categorization.[84] It also bans AI systems used for social scoring, which involves assessing or classifying individuals on the basis of social behavior or personal traits, leading to harmful or discriminatory treatment.[85] Additionally, the act forbids the "creation of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage" and prohibits "'real-time' remote biometric identification in publicly accessible spaces for law enforcement", except under specific conditions related to "targeted search for" missing, abducted or sexually exploited persons, prevention of "a specific, substantial and imminent threat to the life or physical safety of natural persons", and for the investigation of serious crimes, like murder, human trafficking, rape, etc.[86]

Such deployment of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement is permissible only to confirm the identity of a specific individual and must take into account the situation's nature, potential harm, and the impact on individuals' rights and freedoms.[87] The use of these systems is subject to a prior authorization from a judicial or independent administrative authority that evaluates the necessity of the proposed measure based on objective evidence and must follow the necessary safeguards and conditions stipulated by national law, including limitations on time, geography, and personal scope.[88] In urgent cases, real-time FRT may be used without prior authorization, provided the request is made within 24 hours, and must cease immediately if authorization is denied.[89] Notifications of each use must be submitted to relevant authorities, who will report annually to

[84] Id.
[85] Id.
[86] EU Artificial Intelligence Act, Article 5, Annex II.
[87] EU Artificial Intelligence Act, Article 5.
[88] Id.
[89] Id.

the Commission, which will publish aggregated data reports.[90] These provisions do not override other EU laws that prohibit certain AI practices.

FRT which is not used in real-time is considered a high-risk AI system and is strictly regulated.[91] The primary responsibilities lie with providers (developers) of high-risk AI systems, including those intending to market or deploy such systems within the EU, regardless of their geographical location.[92] This also includes third-country providers whose high-risk AI systems' outputs are utilized within the EU.[93] Providers of high-risk AI systems are obligated to establish a comprehensive risk management system and ensure that data governance practices maintain "training, validation, and testing datasets" that are "relevant, representative", and as "error-free and complete" as possible for their intended purpose.[94] Providers shall also create technical documentation that illustrates compliance and enables authorities to assess this compliance.[95] The design of high-risk AI systems must include mechanisms for record-keeping, automatically recording events that could identify risks and substantial modifications at the national level.[96] Additionally, high-risk AI systems must be designed to facilitate human oversight by deployers and to achieve appropriate levels of accuracy and cybersecurity.[97] Lastly, providers must establish a quality management system to ensure ongoing compliance.[98]

The Act and the safeguards it introduces represent a huge step towards more certainty in regulating the FRT, however is criticized for failure to prioritize basic human rights, focusing instead on the interests of industry and law enforcement.[99] It is asserted that the AI Act sets a

[90] Id.
[91] EU Artificial Intelligence Act, Chapter III.
[92] EU Artificial Intelligence Act, Article 2.
[93] Id.
[94] EU Artificial Intelligence Act, Articles 8-10.
[95] EU Artificial Intelligence Act, Articles 11,18, 19.
[96] Id.
[97] EU Artificial Intelligence Act, Article 14.
[98] EU Artificial Intelligence Act, Article 15, 17.
[99] Amnesty International, *EU: Artificial Intelligence rulebook fails to stop proliferation of abusive technologies*, 13 March 2024, available at - https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/.

troubling precedent by introducing unwarranted exemptions for AI applications used by law enforcement, migration control, and national security authorities. In particular, the European legislator failed to provide the same level of protection to migrants, refugees, and asylum seekers,[100] and postponed compliance requirements for AI used in large-scale EU migration databases until 2030.[101]

One of the most concerning elements of the EU AI Act is its creation of a separate legal framework for AI applications used by law enforcement, migration, and national security authorities, that have been provided with substantial exemptions from crucial regulations and safeguards within the Act.[102] For instance, law enforcement and migration authorities are not required to adhere to transparency and oversight protections. Specifically, while the Act mandates that public authorities register high-risk AI systems in a publicly accessible database, law enforcement and migration authorities are exempt from this requirement, thereby promoting secrecy around some of the most potentially harmful applications of AI.[103] This exemption prevents affected individuals, civil society, and the media from understanding where and how AI systems are being implemented but will also hinder accountability. Furthermore, the exemption related to national security allows member states to sidestep the Act's stipulations for any activities they classify as "national security."[104] This broad exemption could potentially be applied to any aspect of migration, policing, and security, effectively placing these areas beyond the reach of the Act's rules.[105]

[100] Amnesty International, *EU: European Parliament Adopts Ban on Facial Recognition but Leaves Migrants, Refugees and Asylum Seekers at Risk*, June 19, 2023, available at - https://www.amnesty.org/en/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/.
[101] Access Now, Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move, 13 March 2024, available at - https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/.
[102] Id.
[103] Id.
[104] Id.
[105] Id.

Unfortunately, all this criticism is perfectly applicable to the development and use of FRT. Thus, by providing these exemptions, the Act implicitly supports the expansive use of FRT by authorities without adequate safeguards, raising valid concerns about privacy, discrimination, and the potential for abuse. The Act seems to prioritize the interests of industry and law enforcement over fundamental human rights, reinforcing the symbiotic relationship between private businesses and governments in the development and deployment of FRT. This preferential treatment undermines the AI Act's effectiveness in comprehensively and equitably regulating FRT. Therefore, while the AI Act establishes important regulatory mechanisms, it falls short in addressing key conflicts of interest and governance gaps in the area of FRT use, emphasizing the need for continuous evaluation and enhancement of AI governance frameworks to ensure human rights protection.

Law Enforcement Directive

The Law Enforcement Directive establishes regulations concerning the safeguarding of individuals' personal data by competent authorities.[106] It applies to data processing activities carried out for preventing, investigating, detecting, or prosecuting criminal offenses, as well as ensuring public safety and preventing threats to public security.

To clarify the application of the Law Enforcement Directive in the context of FRT use by law enforcement authorities, the European Data Protection Board has adopted the Guidelines on the use of facial recognition technology in the area of law enforcement.[107] It is emphasized, that any use of FRT must have a clear legal basis respecting fundamental rights established in the national legislation, and shall be necessary, proportionate, and target specific objectives,

[106] Directive 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, 2016 O.J. (L 119) 89, Article 1.

[107] European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 26 April 2023, available at - https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

such as fighting serious crime, without unnecessarily infringing on rights.[108] In employing biometric processing via FRT, law enforcement authorities must comply with the data protection principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.[109] Certain uses of FRT, such as remote biometric identification in public spaces or categorization based on sensitive attributes, shall also be prohibited to protect fundamental rights.[110]

It should be noted, that faceprints processed in the course of using FRT fall within the scope of biometric data, defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[111]

The processing of such biometric data as well as other special categories of data such as political opinions or sexual orientation, is permitted only when strictly necessary and subject to safeguards, "authorized by Union or Member State law", to protect the vital interests of individuals, or when data are "manifestly made public by the data subject".[112] Processing is deemed "strictly necessary" only if it interferes with the protection of personal data to the minimum extent required, implying that special categories of data should be processed under even stricter conditions than regular necessity.[113] This crucial requirement limits the discretion of law enforcement in assessing necessity, closely tied to established CJEU case law, which emphasizes the need for objective criteria to define the circumstances and conditions of the processing.[114] Moreover, biometric data is considered manifestly made public only if the data

[108] Id.
[109] Id.
[110] Id.
[111] Law Enforcement Directive, Article 3(13).
[112] Law Enforcement Directive, Article 10.
[113] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 26 April 2023, para 73.
[114] Case C-623/17, Privacy Int'l v. Sec'y of State for Foreign & Commonwealth Aff., ECLI:EU:C:2020:790 (Ct. of Justice of the European Union Sept. 6, 2020), para 78.

subject intentionally makes the biometric template (not merely a facial image) freely accessible and public, through an open source.[115] Thus, disclosure by a third party doesn't qualify as data made public by the data subject.[116] Similarly, failure to adjust privacy settings on online platforms or social networks is not sufficient to consider data as manifestly public.[117]

Article 11 of the Directive also prohibits decisions based solely on automated processing, including profiling, if they have a significant adverse legal effect on the data subject.[118] Such decisions are allowed only if authorized by Union or Member State law, providing safeguards, such as the right to human intervention by the controller,[119] provided that such controller may "critically challenge the results of FRT during human intervention".[120] As stipulated in Article 11(3) of the Directive, profiling that leads to discrimination against individuals based on special categories of personal data, including biometric data, is also prohibited under the Directive.[121]

While the Law Enforcement Directive aims to balance public safety with individual rights, its application to FRT reveals significant deficiencies. Similarly to the AI Act, the Directive includes a number of exemptions for activities deemed relevant to public and national security, which can be broadly interpreted by member states in their national laws.[122] These exemptions may effectively place certain law enforcement activities beyond the reach of standard regulatory scrutiny, creating opportunities for unsupervised surveillance and the data processing carried out with the use of the FRT under the guise of public and national security, potentially undermining the Directive's effectiveness in protecting fundamental rights.

[115] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 26 April 2023, para 74-76.
[116] Id.
[117] Id.
[118] Law Enforcement Directive, Article 11.
[119] Id.
[120] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 26 April 2023, para 78.
[121] Law Enforcement Directive, Article 11(3).
[122] *See for example* Articles 13(3) and 15 of the EU Law Enforcement Directive.

National level - United States

Federal level

In the United States, regulation of FRT is decentralized and varies significantly across states, with no comprehensive federal law specifically addressing it. Although various bills have been proposed in Congress to address FRT regulation, none have been brought to a vote thus far. In late October 2023, the Facial Recognition Act strictly regulating the use of FRT by law enforcement was introduced to the U.S. House of Representatives. Under Title I, Section 101 of the legislation, the use of FRT by law enforcement is strictly regulated. Law enforcement officers are permitted to use FRT only under a court order, except in emergencies.[123] Investigative or law enforcement officers are prohibited from using FRT to document how individuals exercise their constitutional rights, such as free assembly, association, and speech.[124] They cannot select individuals for facial recognition based on "race, ethnicity, national origin, religion, disability, gender, gender identity, or sexual orientation" unless there is credible information linking a person with these characteristics to a specific criminal incident.[125] Officers also cannot use facial recognition for immigration enforcement or share related data with agencies for this purpose. [126] Additionally, facial recognition matches cannot be the sole basis for establishing probable cause for searches, arrests, or other actions, and officers must carefully evaluate the accuracy of such matches, ensuring that they are not using FRT with databases containing illegitimately obtained information.[127]

Any law enforcement agency using facial recognition technology must undergo audits to prevent misuse and ensure compliance with the law.[128] Federal, state, and local agencies must

[123] S.681 - 118th Congress (2023-2024): Facial Recognition and Biometric Technology Moratorium Act of 2023, S.681, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/681.
[124] Facial Recognition Technology Act of 2022, Title 1, available at - https://lieu.house.gov/sites/evo-subsites/lieu.house.gov/files/evo-media-document/facial-recognition-act-of-2023.pdf
[125] Id.
[126] Facial Recognition Technology Act of 2022, Section 102.
[127] Id.
[128]Facial Recognition Technology Act of 2022, Sections 104 and 105.

annually submit data for audit by the designated body, detailing their use of facial recognition and any violations found.[129]

Data collected should be "disaggregated by race, ethnicity, gender, and age" when feasible.[130] Accuracy and bias testing of facial recognition systems are required annually, with results reported to the Administrative Office of the United States Courts.[131] The Department of Justice must establish rules for the accuracy of facial recognition systems, consulting with relevant experts.[132]

Similarly, the Facial Recognition and Biometric Technology Moratorium Act, introduced on March 7, 2023, restricts the use of biometric surveillance systems by government entities at federal, state, and local levels.[133] It prohibits their acquisition, possession, or use unless specifically authorized by Congress, with violators facing inadmissibility of obtained information in federal proceedings.[134] Individuals affected by violations retain the right to sue, and compliance with similar restrictions is required for certain federal law enforcement grants at the state or local level.[135]

While the bill introduces notable restrictions to the use of FRT, it also provides for loopholes, entitling law enforcement agencies to deploy FRT without prior authorization. These provisions are designed to ensure rapid response in emergencies, however, the Act does not define exigent circumstances, allowing law enforcement authorities broad discretion to use FRT without oversight, which could potentially lead to abuse of FRT in in situations that may not truly require such immediate action. Although the bill requires post-authorization requests to be filed within a specific period of time, the effectiveness of this measure is questionable, as

[129] Id.
[130] Id.
[131] Id.
[132] Facial Recognition Technology Act of 2022, Section 106.
[133] S.681 - 118th Congress (2023-2024): Facial Recognition and Biometric Technology Moratorium Act of 2023, S.681, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/681.
[134] Id.
[135] Id.

post-surveillance denial of authorization will not eliminate the damage to privacy and other rights that might have already occurred.

State level

At the state level, several states have taken steps to protect biometric data privacy through broader privacy laws. Illinois pioneered such legislation in 2008 by introducing Illinois' Biometric Information Privacy Act,[136] which robustly regulates biometric data, including FRT. It was followed by Arkansas, California, Texas, and Washington, among others.[137]

On May 17, 2024, Colorado set a precedent by becoming the first US state to establish a regulatory framework for artificial intelligence.[138] The Colorado AI Act, which will come into force on February 1, 2026, targets developers and deployers of "high-risk" AI systems, requiring measures to prevent "algorithmic discrimination" and report such incidents to the attorney general's office.[139] The law defines "high-risk" AI systems as those significantly influencing "consequential decisions", which are defined as decisions having significant legal or similar implications on consumers' access to "educational enrollment or opportunity, employment, financial or lending services, essential government services, healthcare services, housing, insurance, or legal services".[140] Additionally, it mandates that deployers notify consumers when high-risk AI systems are used to make consequential decisions about them.[141] Notably, and contrary to the EU's consumer-favored presumption, Colorado's AI Act favors deployers, presuming that the deployer has exercised reasonable care when it can prove that it

[136] State of Illinois Biometric Information Privacy Act of 2008, Public Act 095-0994, 740 ILCS 14, 3 October 2008, available at - https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.
[137] National Academies of Sciences, Engineering, and Medicine, 27.
[138] Tatiana Rice, *Colorado Makes History with the Nation's First Comprehensive AI Act*, 24 May 2024, available at - https://www.techpolicy.press/colorado-makes-history-with-the-nations-first-comprehensive-ai-act/; Danny Tobey, Tony Samp, Coran Darling, Connor Scott, Todd Mobley, Ted Loud, *Colorado enacts first-in-the-nation comprehensive AI guardrails*, 28 May 2024, available at - https://www.dlapiper.com/en-gb/insights/publications/2024/05/colorado-enacts-first-in-the-nation-comprehensive-ai-guardrails.
[139] Colorado Artificial Intelligence Act 24-205, 17 May 2024, available at - https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.
[140] Colorado Artificial Intelligence Act, 6-1-1701, Definitions.
[141] Colorado Artificial Intelligence Act, 6-1-1703, Deployer duty to avoid algorithmic discrimination - risk management policy and program.

complied with certain provisions of the Act, including, for example, completion of the impact assessment and implementation of the risk management policy.[142] The Act, thus, diverges from the usual approach of blatant prohibition of discriminatory conduct and instead focuses on regulating "the outcomes of AI system usage, irrespective of intent",[143] raising concerns about adequacy of the human rights protection. At the same time, the Act, which imposes extensive compliance requirements on developers and deployers in Colorado, sparked significant opposition within the business and tech community and resulted in numerous calls to veto the bill,[144] due to its potential adverse impact on an industry critical for technological progress in the state, serving both consumers and enterprises.

Colorado's pioneering AI regulatory framework aims to prevent algorithmic discrimination but prompts concerns about inadequate levels of human rights protection and stringent compliance demands potentially stifling innovation within the business and tech sectors, essentially satisfying no one.

At the local level, San Francisco led the way in 2019 by becoming the first city in the United States to prohibit the use of FRT by its public agencies, including law enforcement, through its administrative code,[145] however, the majority of states still have no or very limited regulation on the matter.[146] Cities like Oakland,[147] California, and Somerville, Massachusetts,

[142] Colorado Artificial Intelligence Act, 6-1-1702, Developer duty to avoid algorithmic discrimination - required documentation.
[143] Danny Tobey, Tony Samp, Coran Darling, Connor Scott, Todd Mobley, Ted Loud, *Colorado enacts first-in-the-nation comprehensive AI guardrails*, 28 May 2024, available at - https://www.dlapiper.com/en-gb/insights/publications/2024/05/colorado-enacts-first-in-the-nation-comprehensive-ai-guardrails.
[144] The calls for veto were made mostly by representatives of the tec industry, as well as Chamber of Progress, the Consumer Technology Association, and the US Chamber of Commerce. See Id.
[145] City and County of San Francisco, *Board of Supervisors Approval of Surveillance Technology Policy*, 2019 Admin Code Section 19B.2(d), available at - https://sfbos.org/sites/default/files/o0286-19.pdf; Kate Conger, Richard Fausset, Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, May 14, 2019, available at - https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.
[146] Center for Democracy and Technology. *Limiting Face Recognition Surveillance: Progress and Paths Forward*, October 3, 2022, available at - https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/.
[147] Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, San Francisco Chronicle, *16 July 2019, available at - https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php*.

have also restricted FRT use by public agencies, but there are calls to review these policies due to concerns about their potential impact on efforts to prevent crime.[148]

Non-legislative governance approaches manifest themselves in the recent directive of the Department of Homeland Security (DHS), emphasizing that the use of FRT is strictly authorized for DHS missions within established legal boundaries.[149] It also stresses the importance of incorporating safeguards for privacy, civil rights, and civil liberties when using FRT, mandates independent testing and evaluation of FRT, provides opt-out options for actions or investigations not related to law enforcement, and ensures alternative processing for match outcomes. Importantly, it prohibits FRT from being the sole basis for law enforcement actions and requires manual review by human examiners before any such actions can be taken.[150] More broadly, the AI Working Group in the US Senate issued a so-called Roadmap for AI Policy, suggesting a blueprint for federal legislation, which encompasses issues related to bias prevention and consumer protection similar to those addressed in the Colorado law.[151]

The patchwork FRT regulation in the United States demonstrates a clear lack of federal legislation on the matter, which the proposed Facial Recognition Act is designed to address. While there is hope for the new Act to provide for a uniform federal regulation addressing existing legal and ethical concerns, protecting human rights, and preventing abuse, its future remains to be seen. Additionally, the recent enactment of an AI law in Colorado, though applicable only within the state, reflects a broader trend of increased federal activity aimed at establishing nationwide AI standards. With bipartisan efforts in Congress and various federal

[148] National Academies of Sciences, Engineering, and Medicine, 27.
[149] Department of Homeland Security, *Use of Facial Recognition and Face Capture Technologies, 2023*, available at - https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capturetechnologies.pdf.
[150] Id.
[151] The bipartisan Senate AI Working Group, *Driving Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate*, May 2024, available at - https://www.schumer.senate.gov/imo/media/doc/Roadmap_Electronic1.32pm.pdf.

agencies releasing guidance, there's a growing push for uniform federal standards to prevent a 'patchwork' of state laws. However, state legislatures, like Colorado's, may act more swiftly, potentially prompting federal action. As other states contemplate their own AI regulations, conflicts with federal standards may arise.

This chapter highlights the recent surge in legislation and legislative proposals governing FRT, underscoring the urgency for states to regulate this domain and address existing legal gaps. The absence of international consensus or standards that could guide the development and implementation of FRT globally results in inconsistent protections and complicates compliance for entities operating across multiple jurisdictions. While some of these legislative efforts are commendable for their attempts to protect human rights, many provide extensive discretion to law enforcement authorities. This latitude could potentially be exploited under the guise of pursuing legitimate objectives such as public safety and national security, which emphasizes the critical need for ongoing vigilance and participation in the legislative process to ensure that new laws provide an adequate level of human rights protection. As the current implementation of FRT often lacks sufficient oversight and transparency, hindering effective governance of the industry, it is essential that these regulations not only keep pace with technological advancements but also firmly uphold the principles of justice and equity, preventing any misuse of power that could infringe on individual freedoms and privacy.

4. HUMAN RIGHTS IMPLICATED BY FRT

As outlined in Chapter 3 above, the legislative landscape specifically addressing FRT is still in its nascent stages. With a considerable amount of this legislation having only recently been enacted or still pending, there is a notable absence of case law that could provide insights into its effectiveness and real-world applications. This gap significantly challenges our ability to evaluate how well these new laws safeguard human rights and manage the complex implications of FRT usage.

Despite this, it remains crucial to explore the human rights dimensions implicated by FRT. This chapter, therefore, aims to analyze the human rights concerns raised by the use of FRT,[152] through the prism of existing, albeit scarce, case law that touches on related issues. By examining these available cases, we can draw the contours of the legal debates surrounding FRT. This analysis will help illuminate the broader implications for privacy, consent, and surveillance, and will provide a foundational understanding of the potential human rights infringements that could arise from the technology's deployment in both public and private sectors.

Data protection, privacy, and other human rights

As explained above, the use of FRT implies the collection, processing, and storage of large amounts of facial images amounting to personal data. In combination with other artificial intelligence-powered technologies, the Internet of Things, as well as other vast amounts of data available on every individual using the Internet, the FRT has the potential to substantially undermine the protection of individual's data and their right to privacy guaranteed by national, regional, and international legal instruments.[153]

[152] Smith, Marcus, and Seumas Miller, 29-35.
[153] Smith, Marcus, and Seumas Miller, 31.

Data protection concerns relate mainly to difficulties in acquiring express and informed consent from individuals, whose facial image is being processed.[154] Some facial images are already available on the Internet, others could be remotely made in public spaces without individuals' knowledge and thus consent.[155]

As briefly noted above, governments are often one of the main customers of the private companies developing and deploying FRT, raising concerns about their symbiotic relationship that can negatively impact human rights. One of the most illustrative examples of this is the Clearview AI case.[156] This small US company had scraped billions of images available online (including from Google, Facebook, and YouTube) to develop a massive facial recognition database that was sold to private companies, individuals, and law enforcement authorities across the United States.[157] The technology was so advanced, that it allowed for the recognition of faces in the photos' background and empowered the police to locate individuals that hold no government-issued IDs.[158]

The American Civil Liberties Union brought a lawsuit against Clearview to the Illinois Court, arguing violations of privacy rights and requesting Clearview to delete gathered facial images and stop gathering faceprints without the consent of the Illinois residents.[159] In May 2022, Clearview settled the suit, agreeing to refrain from selling the database to private individuals and businesses nationwide, however largely retaining the right to provide it to federal authorities and state agencies outside of Illinois.[160] Other jurisdictions of Clearview's

[154] Smith, Marcus, and Seumas Miller, 22.
[155] C. Castelluccia and D. Le Métayer Inria, *Impact Analysis of Facial Recognition, Centre for Data Ethics and Innovation*, 2020, 7-8, available at - https://inria.hal.science/hal-02480647/document
[156] Smith, Marcus, and Seumas Miller, 28.
[157] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://perma.cc/F2PG-JE7H.
[158] Elizabeth Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1 (2020), 4, available at - https://law.stanford.edu/wp-content/uploads/2020/12/Rowe-FINAL-Facial-Recognition.pdf.
[159] American Civil Liberties Union, *ACLU v. Clearview AI*, American Civil Liberties Union, May 11, 2022, available at - https://www.aclu.org/cases/aclu-v-clearview-ai.
[160] Mac, Ryan, and Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limits on Facial Recognition Database*, The New York Times, May 9, 2022, available at - https://www.nytimes.com/2022/05/09/technology/clearview-ai-

operation have so far been stricter, with the company's technology found violating privacy in Canada,[161] and Australia,[162] being in breach of the GDPR in Austria,[163] and facing substantial fines in France,[164] the UK (although overturned on appeal)[165] and Italy[166] for violation of data protection norms.

Apart from developing FRT for the governments, corporations themselves use FRT for different purposes. In the case of *Patel v. Facebook*, the United States Court of Appeals for the Ninth Circuit established that Facebook's use of FRT to develop its Tag Suggestions feature violated the Illinois Biometric Information Privacy Act, as Facebook used the facial data from photos without the users' prior written consent and without a retention schedule of the biometric information, thereby violating their privacy rights.[167] In 2020, the lawsuit was settled for a substantial sum of $550 million.[168]

---

suit.html; American Civil Liberties Union, *ACLU and Clearview AI Settlement Agreement and Release*, May 4, 2022, available at - https://www.aclu.org/legal-document/exhibit-2-signed-settlement-agreement.

[161] Office of the Privacy Commissioner of Canada, *Announcement: Clearview AI Ordered to Comply with Recommendations to Stop Collecting, Sharing Images*, December 14, 2021, available at - https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/.

[162] Bogle, A. *Australian federal police officers trialled controversial facial recognition tool Clearview AI*, Australian Broadcasting Corporation News, (2020, April 14), available at - https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894.

[163] Austrian SA, *Decision against Clearview AI Infringements of Articles 5, 6, 9, 27 GDPR*, 10 May 2023, available at - https://edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en.

[164] French SA, *Facial Recognition: The French SA Imposes a Penalty Payment on CLEARVIEW AI*, European Data Protection Board," n.d., available at - https://edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en; CNIL, *Facial Recognition: 20 Million Euros Penalty against CLEARVIEW AI*, n.d., available at - https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai#:~:text=Facial%20recognition%3A%2020%20million%20euros%20penalty%20against%20CLEARVIEW%20AI,-20%20October%202022&text=Following%20a%20formal%20notice%20which,delete%20the%20data%20already%20collected.

[165] Vallance, By Chris, *Face Search Company Clearview AI Overturns UK Privacy Fine*, BBC News, October 18, 2023, available at - https://www.bbc.com/news/technology-67133157.

[166] Italian SA, *Fines Clearview AI EUR 20 million*, February 10, 2022, available at - https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en.

[167] See *Patel v. Facebook, Inc.*, No. 18-15982 (9th Cir. 2019), available at - https://law.justia.com/cases/federal/appellate-courts/ca9/18-15982/18-15982-2019-08-08.html.

[168] Rachel Pester, *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit*, 14 February 2020, available at - https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit.

The above cases reflect a growing trend among companies to settle disputes related to FRT violations outside of court. These settlements, often involving substantial financial compensation or significant alterations of operational business practices, underscore the growing public and legal scrutiny faced by the companies developing, using, or distributing FRT and highlight the evolving legal landscape of data protection and privacy regulations concerning the technology at hand. Even in the absence of respective court decisions, these precedents serve as benchmarks for future conduct of business related to FRT, indicating a potential shift towards more responsible FRT development and distribution, and pushing companies towards preventing human rights abuses. At the same time, it should be noted that in the absence of clear and stringent legal regulations, law enforcement authorities, often being primary beneficiaries of the privately developed FRT, take advantage of the current legal uncertainty. The Clearview case serves as a perfect illustration of this conflict of interest, as the ban on the use of the technology in the United States did not extend to the law enforcement authorities outside of Illinois, which could still use Clearview's database to enhance their capabilities and potentially abuse human rights.

In a recent groundbreaking decision, the European Court of Human Rights also expressed its stance on the use of FRT.[169] It found that the use of Moscow subway cameras equipped with FRT to identify, locate, and arrest a protestor commuting in the subway violated his right to privacy and freedom of expression.[170] While the use of FRT in this case is attributed to Russian law enforcement authorities, the software used has been developed by private companies.[171] Notably, the Court established that besides the rights to privacy guaranteed by

[169] Palmiotto, Francesca, and Natalia Menéndez González, *Facial Recognition Technology, Democracy and Human Rights*, Computer Law & Security Review, September 1, 2023.
[170] European Court of Human Rights, *Glukhin v. Russia*, No. 11519/20, July 4, 2023.
[171] OVD-Info, *How the Russian State uses cameras against protesters*, January 17, 2022, available at - https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters?_gl=1*1d4s3uo*_ga*MTYzMDUxMjQxMC4xNzAxNDM4NjYy*_ga_J7DH9NKJ0R*MTcwMTQzODY2MS4xLjEuMTcwMTQzODY3My40OC4wLjA.#1.

Article 8 of the European Convention on Human Rights, Russia also violated Article 10 of the Convention by hindering Mr Glukhin's freedom of expression.[172]

This case underscores the international concern over the law enforcement authorities' use of FRT in violation of human rights not limited to the right to privacy. Other known instances of governments using FRT acquired from private companies to suppress dissent occurred in China,[173] Turkey, Egypt, Saudi Arabia, Sudan, and the United Arab Emirates.[174] Thus, while as indicated above, some governments have started to increase scrutiny over corporations developing and distributing FRT, at this point, there is little oversight over the states themselves using FRT to hinder human rights, and international and regional human rights mechanisms will most likely encounter an increase in the number of such cases in the recent future.

The increasing use of FRT in different areas of life and an increasing number of public spaces pose threats of extending their use far beyond the originally intended and controlled purposes. Starting from seemingly legitimate contexts such as the use of FRT at the border control at the airports,[175] the technology has the potential to transform into mass surveillance practices substantially undermining a wide range of human rights, including not only the right to privacy and prohibition of non-discrimination, but also freedom of movement, freedom of religion, freedom of opinion and expression, freedom of religion,[176] freedom of association, and freedom of assembly.[177] United Nations Human Rights Council reported, that the use of FRT

[172] European Court of Human Rights, *Glukhin v. Russia*, No. 11519/20, July 4, 2023, paras 44-99.
[173] Peter Dizikes, *How an AI-tocracy emerges*, July13, 2023, available at - https://economics.mit.edu/news/how-ai-tocracy-emerges.
[174] Amnesty International, *New EU Dual Use Regulation Agreement 'a Missed Opportunity' to Stop Exports of Surveillance Tools to Repressive Regimes*, November 23, 2021, available at - https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/.
[175] Smith, Marcus, and Seumas Miller, 23.
[176] E. Rowe, Regulating Facial Recognition Technology in the Private Sector, Stanford Technology Law Review, Vol. 24(1), 2021, 31, available at - https://law.stanford.edu/publications/regulating-facial-recognition-technology-in-the-private-sector/.
[177] European Union Agency for Fundamental Rights, *2020 Report*, 29-30, available at - https://fra.europa.eu/en/publication/2020/fundamental-rights-report-2020.

to identify persons that took part in public assemblies has a considerable chilling effect on the rights concerned.[178] It could also disproportionately affect certain vulnerable groups of individuals, such as children, that shall be subject to a higher degree of protection especially in the law enforcement context.[179]

Some say that despite the commendable trends in the recent and emerging legal frameworks, the European Union states exhibit a noticeable trend towards normalizing remote biometric identification in public spaces,[180] allowing tracking of individuals through the use of databases and substantially interfering with privacy, personal data, and dignity of affected individuals.[181] FRT appears to be even more intrusively used in the United States[182] and is interfering with almost all spheres of individuals' lives in China.[183] Such introduction of mass surveillance threatens to undermine free will by stripping individuals of autonomy and anonymity and empowering forced conformism.[184] Being aware of all-encompassing surveillance, individuals might start self-censoring and stop attending controversial events and organizations, practicing unpopular religions, or expressing unpopular views or opinions, thereby substantially changing their social and psychological behaviors and raising ethical issues related to the use of FRT.[185]

[178] United Nations High Commissioner for Human Rights, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, 2020, available at - https://www.ohchr.org/en/press-releases/2020/06/new-technologies-must-serve-not-hinder-right-peaceful-protest-bachelet-tells?LangID=E&NewsID=25996.
[179] European Union Agency for Fundamental Rights, *2020 Report*, 28-29.
[180] AlgorithmWatch and Bertelsmann Stiftung, *Report Automating Society 2019 and 2020*, available at - https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/10/Automating-Society-Report-2020.pdf.
[181] European Commission, *Impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council*, 2021, 18, available at - https://eur-lex.europa.eu/resource.html?uri=cellar:0694be88-a373-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.
[182] Garvie, C., Bedoya, A., & Frankle, J., *The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Centre on Privacy and Technology Report*, 2019.
[183] Smith, Marcus, and Seumas Miller, 31.
[184] European Parliament, *Regulating Facial Recognition in the EU*, September 2021, 8, available at - https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf
[185] See High-Level Expert on AI, *Ethics guidelines for trustworthy AI*, 2019, 33, available at - https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Some law enforcement agencies may aim to employ FRT in an unrestricted manner, conducting ongoing scans of individuals in various public settings like parks, streets, sidewalks, and transportation hubs without specific threats or suspicions.[186] For instance, in 2020, the Metropolitan Police in the United Kingdom announced their intention to implement real-time FRT in certain public areas to continuously screen for criminal suspects.[187] This application of live FRT is designed to work alongside a watchlist of wanted offenders or individuals deemed to pose a threat to themselves or others.[188]

In September 2019, a judicial review was initiated after South Wales Police launched a surveillance project called 'AFR Locate', employing FRT at events and crime-prone areas.[189] The system scanned passersby, capturing up to 50 faces per second, matching them against a police watchlist and deleting non-matches.[190] It was estimated that around 500,000 individuals had their facial biometric data collected without their consent in 2017-2018.[191] The claimant argued this use of FRT was unlawful and in breach of Article 8 of the European Convention on Human Rights and UK data protection laws, including the Public Sector Equality Duty under the Equality Act 2010.[192]

---

[186] P. Mozur, M. Xiao, and J. Liu, *How China Polices the Future: An Unseen Cage of Surveillance*, New York Times, p. A1, 25 June 2022; I. Qian, M. Xiao, P. Mozur, and A. Cardia, China's Expanding Surveillance State, New York Times, p. A10, 27 July 2022; M. Xiao, P. Mozur, I. Qian, and A. Cardia, *China's Surveillance State Is Growing: These Documents Reveal How*, New York Times, 21 June 2022, https://www.nytimes.com/video/world/asia/100000008314175/chinagovernment-surveillance-data.html; P. Mozur, C. Fu, and A. Chien, *How China's Police Used Phones and Faces to Track Protesters*, New York Times, updated December 4, https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.Html; D. Davies, *Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State,'* NPR, available at - https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-insidechinassurveillance-Sta; K. Hao, After Feeding Explosion of Facial Recognition, China Moves to Rein It In," Wall Street Journal, available at - https://www.wsj.com/articles/china-drafts-rules-for-facial-recognition-use-4953506e.

[187] Satariano, *London Police Are Taking Surveillance to a Whole New Level*, New York Times, updated October 1, 2021, available at - https://www.nytimes.com/2020/01/24/business/london-police-facial-recognition.html.

[188] Metropolitan Police United Kingdom, *Facial Recognition Technology: Live Facial Recognition*, available at - https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology.

[189] R (Bridges) v. Chief Constable of South Wales Police, 11 August 2020, Case No. C1/2019/2670, [2020] EWCA Civ 1058, available at - https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[190] R (Bridges) v. Chief Constable of South Wales Police, para 16.

[191] Id.

[192] R (Bridges) v. Chief Constable of South Wales Police, para 35-53.

While the High Court ruled that existing legal safeguards relating to the use of FRT were sufficient, the Court of Appeal, overturned this decision, finding that the use of FRT violated Article 8 ECHR by collecting and processing biometric data without consent.[193] The Court of Appeal also established, that the Data Protection Impact Assessment (DPIA) didn't adequately assess risks to people's rights and freedoms as required by the Data Protection Act 2018, and found that the Metropolitan police breached the Public Sector Equality Duty by failing to gather sufficient evidence to assess the risk of indirect discrimination before deploying the FRT.[194] The Court also emphasized the need for periodic reassessment as FRT technology evolves and outlined that business enterprises using FRT should ensure strict compliance with privacy and data protection laws, conducting thorough DPIAs that consider human rights and equality laws.[195]

Besides Clearview AI, PimEyes is another FRT engine, claiming to have a database of nearly three billion faces, that allows users to upload face images and find matching ones across the Internet.[196]

Illinois residents have filed a class action lawsuit against **PimEyes**, its cofounders, and its current CEO, alleging unauthorized collection, scanning, and utilization of their facial images, along with those of numerous other Americans.[197] The lawsuit accuses PimEyes of 'intentional or reckless' privacy violations and violations of the Illinois Biometric Information Privacy Act (BIPA), resulting in significant and irreparable harm.[198] The plaintiffs claim that

[193] R (Bridges) v. Chief Constable of South Wales Police, para 152-153, 210.
[194] Id.
[195] Id.
[196] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, 89; Big Brother Watch, *Biometric Britain: the Expansion of Facial Recognition Surveillance*, 23 May 2023, 84.
[197] Big Brother Watch, *Biometric Britain: the Expansion of Facial Recognition Surveillance*, 23 May 2023, 84-91; AIAAIC, PimEyes sued in Illinois, USA, for privacy violations, May 2023, available at - https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/pimeyes-sued-in-illinois-usa-for-privacy-violations; Andy Nghiem, Illinois residents allege facial image search engine violates BIPA, 18 May 2023, available at - https://madisonrecord.com/stories/642174142-illinois-residents-allege-facial-image-search-engine-violates-bipa.
[198] Id.

PimEyes gathers and retains biometric data from millions of Americans without their consent, utilizing it to power their facial search engine while failing to disclose its data management policies.[199] Seeking $15,000 for each affected resident, the complaint highlights BIPA's provisions prohibiting companies from gathering or storing data, including facial data of Illinois residents, without consent.[200] It mandates written notification regarding data collection purposes and storage duration, along with obtaining written consent from visitors.[201]

The state data protection authority of Baden Württemberg (LfDI) in Germany has also initiated fine proceedings against PimEyes following media reports raising concerns about the company's practices of mass scanning and storing biometric data without individuals' consent.[202] In response to the LfDI's inquiry, PimEyes claimed that it only processes publicly available images and cannot link them to identifiable individuals. However, the state commissioner found this response inadequate and raised concerns about the lack of data protection measures.[203]

As evidenced by documents acquired through freedom of information requests, the Australian Federal Police may have tested the PimEyes FRT for operational use at least 10 times, prompting ongoing investigations.[204]

Big Brother Watch, a UK privacy advocacy group, lodged a formal complaint with the Information Commissioner's Office (ICO) regarding PimEyes, similarly alleging that PimEyes unlawfully processed the biometric data of millions of UK citizens without their consent,

[199] Id.
[200] Id.
[201] Id.
[202] Big Brother Watch, *Biometric Britain: the Expansion of Facial Recognition Surveillance*, 23 May 2023, 84-91; AIAAIC, *German privacy watchdog investigates PimEyes for privacy abuse*, December 2022, available at - https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/german-privacy-watchdog-investigates-pimeyes-for-privacy-abuse; Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg. (2022). *PimEyes: LfDI eröffnet Bußgeldverfahren*, available at - https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/#:~=Aufgrund%20der%20offenbar%20fehlenden%20Datenschutzkonformität,58.
[203] Id.
[204] Big Brother Watch, *Biometric Britain: the Expansion of Facial Recognition Surveillance*, 23 May 2023, 84-91.

allowing for unprecedented surveillance and stalking capabilities.[205] Big Brother Watch argued that PimEyes' tool could be exploited by various entities, including potential employers and domestic abusers, posing a significant threat to individuals' anonymity and privacy.[206] However, in May 2023, the ICO announced its decision not to formally investigate PimEyes, deferring to another data protection authority's ongoing investigation into the matter.[207]

Facewatch could serve as another example. Originally established in 2010 as a crime reporting and intelligence-sharing platform, Facewatch facilitated swift dissemination of CCTV images among businesses and law enforcement agencies.[208] By 2012, it evolved to empower the public to search through images of wanted individuals and provide identifications to the police.[209] In early 2018, Facewatch transitioned from primarily functioning as an intelligence-sharing platform to focusing on FRT.[210] Today, Facewatch, headquartered in London, offers live FRT to businesses worldwide with the goal of curbing store theft and fostering safer retail environments.[211] It strives to democratize FRT, making it accessible even to smaller retailers, thereby expanding the scope of mass surveillance.[212] Apart from its UK operations, Facewatch has distribution channels in Spain, Brazil, and Argentina.[213]

Facewatch operates similarly to police-operated live FRT, utilizing software to monitor live video feeds from premise entrances, detecting faces within the camera's view.[214] These

[205] AIAAIC, *UK pressure group accuses PimEyes of surveillance, privacy abuse*, May 2023, available at - https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/uk-pressure-group-accuses-pimeyes-of-surveillance-privacy-abuse; Big Brother Watch, *Submission To The Information Commissioner Request For An Investigation Into Carribex Ltd T/A Pimeyes Unlawful Processing Of Biometric Data*, available at - https://bigbrotherwatch.org.uk/wp-content/uploads/2022/11/20220912-Big-Brother-Watch-Submission-re-PimEyes-AS-SENT.pdf; Big Brother Watch, B*iometric Britain: the Expansion of Facial Recognition Surveillance*, 23 May 2023, p.84-91.
[206] Id.
[207] Id.
[208] Big Brother Watch, Biometric Britain: the Expansion of Facial Recognition Surveillance, 23 May 2023, 98-105.
[209] Id.
[210] Id.
[211] Id.
[212] Id.
[213] Id.
[214] Id.

faces are then converted into biometric templates and compared against those stored on the Facewatch watchlist.[215] If a match surpasses a predetermined similarity threshold, an alert is sent to shop staff to enforce store policies.[216] Facewatch's adaptable software can integrate with various HD CCTV cameras, facilitating its potential expansion into a widespread network of private facial recognition systems.[217] Notably, the company announced in March 2023 that it ceased using cameras from Hikvision, a Chinese state-owned company implicated in human rights abuses, marking a significant shift from its previous endorsement of Hikvision's products.[218]

Apart from a complaint filed by Big Brother Watch regarding its data processing practices, Facewatch underwent an independent investigation by the Information Commissioner's Office.[219] Following the investigation, Facewatch was mandated to implement significant changes due to concerns raised by the ICO regarding its handling of personal data.[220] However, specific details regarding these changes have not been disclosed by either the ICO or Facewatch.[221]

It has been reported that UK Home Office officials might have covertly pressured the independent privacy regulator to support Facewatch seeking to expand its FRT across the country.[222] Internal emails revealed that the UK Home Office warned the Information Commissioner's Office (ICO) of potential intervention by the policing minister if the regulator's

[215] Id.
[216] Id; Facewatch, *Facewatch System Installation Guide*, available at - https://www.facewatch.co.uk/wp-content/uploads/2020/03/Facewatch-Installer-Guide-v2f-web.pdf
[217] Id.
[218] *Facewatch To Stop Using Hikvision Amid Controversy Over Uk Retail Biometrics*, Biometric Update, 23rd March 2023, available at - https://www.biometricupdate.com/202303/facewatch-to-stop-using-hikvision-amidcontroversy-over-uk-retail-biometrics.
[219] Id; Big Brother Watch, *Big Brother Watch Files Legal Complaint Against Co-Op's "Orwellian" Facial Recognition*, 26 July 2022, available at - https://bigbrotherwatch.org.uk/2022/07/big-brother-watch-files-legal-complaintagainst-co-ops-orwellian-facial-recognition.
[220] Id.
[221] Id.
[222] Mark Townsend, *Revealed: Home Office secretly lobbied for facial recognition 'spy' company*, 2 September 2023, The Guardian, available at - https://www.theguardian.com/technology/2023/sep/02/home-office-accused-of-secret-lobbying-for-facial-recognition-spy-company.

investigation into Facewatch did not favor the company.[223] Despite this, the ICO concluded its investigation into Facewatch without further regulatory action, citing the firm's legitimate purpose for using facial recognition in crime prevention. [224] Privacy advocates criticized the apparent interference, emphasizing the need for an independent regulatory process, while the Home Office defended its support for FRT to combat retail crime. [225]

In essence, the above cases demonstrate the broader implications of deploying FRT in both commercial and law enforcement settings and serve as a reminder of the potential for such technology to infringe on privacy rights and the consequent need for robust, transparent, and independent regulatory oversight, ensuring that the deployment of FRT systems does not compromise fundamental human rights. While some of the legal frameworks addressed above or other emerging legislation might eliminate some of the concerns, a large part of the use of FRT by law enforcement authorities still falls or will likely fall outside the scope of the proposed regulations, threatening to undermine the human rights of individuals potentially even without their knowledge.

Discrimination and Bias

Another concern often raised by experts and human rights lawyers and activists is potential discrimination and bias.[226] Discrimination may occur in the course of development, design, testing, or implementation of FRT through discriminatory approaches embedded into the algorithm and deriving from the data sets used to train the model, or through the way the results of FRT application are interpreted by human beings.[227]

[223] Id.
[224] Id.
[225] Id.
[226] European Parliament, *Regulating Facial Recognition in the EU*, September 2021, 7, available at - https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf
[227] Id.

Issues related to the technical features of the FRT and its accuracy appear to be of particular importance here. Current software employing FRT uses deep learning techniques to collect sensitive information on a vast number of individuals.[228] As these data sets grow in number, it becomes increasingly difficult, if not impossible to exercise human control over its operation and conduct manual verification and labelling.[229] We also cannot overlook the fact that every system is prone to error. FRT is no exception, as confirmed by some of the existing empirical studies.[230]

FRT can make two types of errors: false negatives when the technology fails to identify and match individuals that are present on the pictures and in databases, and false positives when FRT identifies a face where there is none or wrongly considers photos of two different persons to show the same individual.[231] The probability of an error increases when photos compared have different "lightening, shadows, backgrounds, poses, or expressions, […] and […] age discrepancies".[232] Additionally, experts outline the existing risks associated with the breach or misuse of high volumes of facial recognition data stored in these databases.[233]

These errors and breaches, if occur, may have far-reaching implications on human rights. It has been noted, that FRT is significantly less accurate in identifying and recognizing

[228] European Parliamentary Research Service, *Regulating Facial Recognition in the EU*, 5.
[229] K. Haoarchive, *This is how we lost control of our faces*, MIT Technology review, 2021, available at - https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/.
[230] Human Rights Council, *Report of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age*, 13 September 2021, A/HRC/48/31, paras 25-28; See also P. Grother et al., Face Recognition Vendor Test (FRVT), 2019, available at - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; European Data Protection Board, *Guidelines 05/22 on the use of facial recognition technology in the area of law enforcement*, 12 May 2022, 11-12.
[231] Trades Union Congress, *Technology managing people - The worker experience*, 2021, 3, available at - https://www.tuc.org.uk/sites/default/files/2020-11/Technology_Managing_People_Report_2020_AW_Optimised.pdf
[232] J. Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation, 2020, 11-12, available at - https://www.eff.org/wp/law-enforcement-use-face-recognition.
[233] N. Turner Lee, P. Resnick, and G. Barton, A*lgorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, Brookings, 2019, 32-34, available at - https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

women and people of color than white men,[234] thereby exhibiting discrimination on the basis of gender and race. It has also been reported that risks of discrimination towards people of color are exacerbated in the context of law enforcement.[235] There is evidence, suggesting that false positives in FRT disproportionally affect people of color thereby placing the burden on falsely identified suspects to prove that they have been wrongfully identified by the algorithm and thus potentially violating the presumption of innocence.[236] The reports of numerous cases prove the point.[237] Such outcomes violate the prohibition of discrimination enshrined in national legislations as well as regional[238] and international instruments[239] and require heightened attention from governments and legislators in particular so that emerging legal instruments ensure the absence of discriminatory approaches and prevent abuse of human rights.

On January 29, 2024, the American Civil Liberties Union and the ACLU of New Jersey submitted an amicus brief to the U.S. District Court for the District of New Jersey in support of Plaintiff Nijeer Parks, contending that Mr. Parks's constitutional rights were violated by law

[234] J. Buolamwini and T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 2018, available at - http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; J. Cavazos et al., *Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?*, IEEE Transactions on Biometrics, Behaviour and Identity Science, 2021, available at - https://ieeexplore.ieee.org/abstract/document/9209125; Dauvergne, 6.

[235] A/HRC/44/57, paras. 39–40.

[236] A/HRC/44/57, paras. 39–40; J. Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation, 2020, 11-12; Hopkins, N., & Morris, J. (2015, February 3).

[237] Carrega, Christina, and Christina Carrega. *Facial Recognition Technology and False Arrests: Should Black People Worry?*, Capital B News, December 2, 2023, available at - https://capitalbnews.org/facial-recognition-wrongful-arrests/; Hill, Kashmir, *Wrongfully Accused by an Algorithm*, The New York Times, August 3, 2020, available at -https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[238] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, Article 14; Council of Europe, *European Social Charter (Revised)*, 3 May 1996, ETS 163, Article 21; Inter-American Commission on Human Rights (IACHR), *American Declaration of the Rights and Duties of Man*, 2 May 1948, Article 2; Organization of American States (OAS), *American Convention on Human Rights*, "Pact of San Jose", Costa Rica, 22 November 1969, Article 1; Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights*, 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), Article 2.

[239] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Article 1(3); UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, Article 2(1); UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3, Article 2(2) and 3; UN General Assembly, *International Convention on the Elimination of All Forms of Racial Discrimination*, 21 December 1965, United Nations, Treaty Series, vol. 660, p. 195, Article 2; UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, 18 December 1979, United Nations, Treaty Series, vol. 1249, p. 13, Article 2.

enforcement's wrongful arrest, that resulted from their reliance on unreliable FRT.[240] In January 2019, Woodbridge, New Jersey police responded to a hotel lobby shoplifting incident where the suspect presented a fake driver's license and fled.[241] Police sent a blurry license photo to an out-of-state investigator, who identified Nijeer Parks as a potential match using facial recognition technology.[242] Despite inadequate follow-up investigation, police sought an arrest warrant, omitting key details about the technology's unreliability.[243] Mr. Parks was arrested and held for ten days, despite evidence showing he was not in Woodbridge during the incident.[244]

This case is one of several instances where wrongful arrests have occurred due to the misuse of facial recognition technology by law enforcement authorities.[245] In its brief, the ACLU emphasizes that this technology is dangerously unreliable and disproportionately affects black and brown individuals, resulting in higher rates of misidentification.[246] They outline, that nearly all known cases of wrongful arrests due to incorrect face recognition results have involved black individuals.[247] The American Civil Liberties Union, alongside the ACLU of Michigan and the University of Michigan Law School's Civil Rights Litigation Initiative (CRLI), are also representing Robert Williams in his pending lawsuit against the Detroit Police Department as Williams was wrongfully arrested and detained in January 2020 due to flawed FRT.[248]

[240] Amicus Curiae Brief Of The American Civil Liberties Union And The American Civil Liberties Union Of New Jersey In Support Of Plaintiff's Opposition To Defendants' Motion For Summary Judgment to the Case of Parks V. Mccormac, Case 2:21-cv-04021-JKS-LDW, available at - https://www.aclu.org/cases/parks-v-mccormac?document=Amicus-Brief#legal-documents.
[241] Id.
[242] Id.
[243] Id.
[244] Id.
[245] Carrega, Christina, and Christina Carrega. *Facial Recognition Technology and False Arrests: Should Black People Worry?*; Hill, Kashmir, *Wrongfully Accused by an Algorithm*.
[246] Amicus Curiae Brief Of The American Civil Liberties Union And The American Civil Liberties Union Of New Jersey In Support Of Plaintiff's Opposition To Defendants' Motion For Summary Judgment to the Case of Parks V. Mccormac, Case 2:21-cv-04021-JKS-LDW.
[247] Id.
[248] Id.

While the pieces of legislation considered in the previous Chapter include non-discrimination provisions and related norms against profiling and stipulate the need for human oversight over FRT-related decision-making, the identified gaps have the potential to nullify the efforts. The reliance on FRT, which has shown a propensity for discrimination and errors, particularly against women and people of color, reveals a stark compromise of fundamental human rights under the guise of achieving declared legitimate aims.

5. LIMITATIONS AND RECOMMENDATIONS

As evident from the above considerations, the absence of a binding international legal framework tailored specifically to address FRT's complexities is one of the most critical challenges in its regulation. Current international instruments provide overarching guidelines for privacy and rights protection but fall short of addressing the unique challenges posed by FRT. This gap in international standards results in a patchwork of regional and national laws that vary significantly from one country to another, leading to potential conflicts among states, private entities, and the rights of individuals. Without a unified international instrument dedicated to FRT, there is no consistent standard of protection, nor is there a mandate compelling states to regulate this technology.

This lack of uniformity not only complicates compliance for multinational entities but also heightens the risk of conflicts of interest between governmental objectives, commercial interests, and the preservation of fundamental human rights. Therefore, while the AI Convention, does not specifically target FRT, it represents a promising initial step towards setting a foundational baseline for the future regulation of AI-powered technologies, including FRT. This could pave the way for more comprehensive guidelines and standards that encompass the unique challenges and implications of facial recognition technology.

In their approaches to regulating FRT, the EU and the US showcase distinct strategies. The EU has attempted to create a centralized regulatory framework with instruments like the GDPR, the Law Enforcement Directive, and the recent AI Act, striving for a certain degree of uniformity and specificity across its member states. Conversely, the regulatory landscape in the US is decentralized, characterized by a mosaic of state and local regulations due to the absence of comprehensive federal legislation. This fragmentation results in varying levels of protection: some states like Illinois use existing laws such as the Biometric Information Privacy Act to adapt to the new challenges posed by the FRT, others have minimal or non-existent regulations

specific to FRT, and yet others proceed with adopting new regulations governing broad applications of artificial intelligence, as does the Colorado AI Act. At the same time, the US seems to be one of the most fast-paced jurisdictions in terms of emerging case law, as a large portion of lawsuits involving the use of FRT have been filed in the United States.

The regulatory environments in both regions are marked by an inherent conflict of interests between private companies that develop and market FRT, law enforcement authorities that utilize these technologies, and the protection of individual human rights.

Private companies have strong financial incentives to innovate and expand the capabilities of FRT to make a profit, often putting market expansion above ethical and potentially even legal considerations. The competitive nature of the tech industry encourages rapid development and deployment of FRT, sometimes bypassing thorough ethical evaluations and adequate safeguards for privacy and human rights. Recognizing the high stakes of the potential false identifications, multiple companies have decided to (temporarily) withdraw from the FRT development game. For instance, Amazon, Microsoft, and IBM have announced a moratorium on manufacturing or distribution of FRT software for the law enforcement authorities.[249] As outlined above, some authorities have also established a ban on their use[250] or might be on the verge of doing so. This demonstrates a growing awareness of the involved actors of the FRT's potential for harm and the pressing need for the legislative authorities to consider these issues and their potential harmful impact on the society and individual rights.

Law enforcement agencies seek to leverage FRT for enhanced security and surveillance capabilities, sometimes at the expense of privacy and civil liberties. The potential of FRT to identify suspects, find missing individuals, and maintain public order is highly appealing,

[249] Reventlow, Nani Jansen, *How Amazon's Moratorium on Facial Recognition Tech Is Different From IBM's and Microsoft's*, Slate Magazine, June 11, 2020, available at - https://slate.com/technology/2020/06/ibm-microsoft-amazon-facial-recognition-technology.html.
[250] Kate Conger, Richard Fausset, Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, May 14, 2019, available at - https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

however, the intrusive nature and extensive power of FRT can lead to overreach and misuse, resulting in violations of privacy and civil liberties.

Human rights advocates, in turn, focus on the implications of FRT for privacy, data protection, discrimination, and mass surveillance, emphasizing the need for stringent regulations to protect individuals from potential abuses of FRT. However, their efforts often clash with the interests of private companies and law enforcement agencies, creating a complex regulatory environment. The interests of private companies and law enforcement authorities, on the contrary, are aligned, as they both benefit from highly efficient and smooth operation of the FRT. The close collaboration between public and private sectors in the development and deployment of FRT also extends beyond initial sales.[251] It has been reported that private companies often provide ongoing technical support, updates, and training to government clients, as evidenced by contracts such as those reported for FinFisher, raising further concerns about the accountability and oversight of these practices.[252]

This triadic conflict often results in regulatory capture, where policies and regulations are influenced more by corporate and law enforcement interests than by the need to protect human rights. The above overview of the existing and upcoming legal frameworks governing FRT as well as the existing case law on the matter support this observation, demonstrating how certain provisions favor industry growth and law enforcement capabilities rather than prioritizing human rights protections.

At the EU level, AI Act establishes important regulatory mechanisms, however, falls short in addressing key conflicts of interest and governance gaps in the area of FRT use. The exemptions for law enforcement and migration authorities, coupled with broad national security clauses, dilute the Act's potential to protect human rights robustly. Similarly, the EU's Law

[251] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, (28 May 2019) A/HRC/41/35, paras 15-20.
[252] Id.

Enforcement Directive, while aiming to balance public safety with individual rights, falls short in its application to FRT due to its lack of specific guidelines, insufficient oversight, and broad exemptions that compromise its effectiveness in regulating law enforcement's use of the technology.

The post-authorization and certain other provisions of the proposed Face Recognition Act in the US portray a similar picture, with the Clearview AI case serving as one of the most illustrative examples of this conflict. The most recent piece of regulation in the US, namely the Colorado AI Act has faced significant criticism from the industry and federal agencies, expressing concerns about stifling innovation in an area that is considered critical for business and state-related advancements, and human rights defenders, stressing an insufficient level of human rights protection. This controversy is part of a broader dynamic concerning the evolution of artificial intelligence, stressing the tension between regulating emerging technologies and fostering an environment conducive to technological and economic growth.

These deficiencies and considerations highlight the ongoing challenges and underscore the urgent need for comprehensive regulations that effectively balance innovation in FRT with ethical considerations and human rights protections.

As already mentioned above, development of the international binding treaty addressing the development and use of FRT could become a starting point. While the adoption of the Convention governing FRT specifically is not realistic, the internationally binding instrument akin to the AI Convention adopted by the Council of Europe establishing minimum standards for the development, use and deployment of FRT, would be a tremendous help in ensuring that fundamental human rights are protected globally. Any other international treaty or convention under the auspices of organizations like the United Nations could serve this purpose. In the meantime, the states shall rely on the existing international law instruments, including those

governing human rights, and shall make sure to adopt evolutionary interpretation of the existing provisions, taking into account technological and societal advancements.

Existing laws should be updated to provide greater specificity and clarity regarding FRT use. This includes defining key terms, setting clear guidelines for consent and data processing, and establishing robust oversight mechanisms. Legal provisions should address the unique challenges of FRT, such as the potential for mass surveillance and the need for real-time identification. At the same time, the legislators shall pay more attention to developing strong obligations as well as review and authorization mechanisms that would limit the wide discretion of the law enforcement authorities restricting possibilities of abusing FRT on their part. The use of FRT shall be narrowly authorized by designated independent, preferably judicial, bodies, that shall restrict such practices in their duration and scope.[253] The instances of FRT use shall be transparent and public to the maximum extent possible, the individuals subject to FRT shall be made aware thereof, so that they could properly challenge it in case of abuse.[254] At the same time, judicial review alone might not be sufficient, and the governments shall employ other control and review measures, such as public oversight and consultation before the purchase and/or use of certain FRT.[255]

This shall be achieved, inter alia, by a stronger and more pronounced collaboration between governments, private companies, civil society, and international organizations, that shall raise awareness of the existing and upcoming risks of FRT use, as well as deficiencies and disparities in the proposed and enacted legislation. Such multi-stakeholder initiatives can help develop comprehensive and balanced regulatory frameworks that take into account diverse perspectives and expertise. Advancement of a more transparent approach to the existing

[253] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, (28 May 2019) A/HRC/41/35, para 15-20.
[254] Id.
[255] Id.

regulatory issues and their potential human rights impacts shall strive to tip the balance in favor of human rights.

6. CONCLUSION

FRT has revolutionized many aspects of modern life, undoubtedly providing considerable benefits not only in our everyday lives but also in the areas of public safety and national security. However, the rapid development and widespread deployment of FRT have outpaced the development of sufficiently adequate legal frameworks, leading to significant governance gaps.

The analysis of FRT regulations and case law across chosen jurisdictions presented in this thesis exposes substantial gaps within current legal frameworks that are yet to be adequately addressed to mitigate the risks associated with the use of FRT, which has a tremendous potential to erode privacy, exacerbate discrimination, and interfere with other human rights, such as freedom of expression, freedom of assembly, and freedom of movement.

The exploration in this thesis has also highlighted an inherent conflict of interest that makes the governance of FRT even more complicated. The interests of law enforcement, private sector developers, and human rights advocates often clash, as each stakeholder has different goals and priorities that influence the pace and substance of the emerging regulations. As outlined in this thesis, law enforcement authorities are frequently granted considerable discretion in the application of FRT. This discretion allows them to evade certain responsibilities, including the crucial ones related to the authorization of FRT surveillance and transparency of its application, and operate with minimal oversight, not only undermining the effectiveness of existing legal frameworks but also increasing the risk of human rights abuses.

This underscores the urgent need for an integrated approach to governance that can balance rapid technological advancements with robust human rights protections. The absence of an international standard specifically tailored for FRT complicates the landscape, leading to a patchwork of national laws that struggle to uniformly protect the rights of individuals. As individual countries like the US, and individual states in the U.S. navigate their regulatory paths,

regions like the EU attempt to formulate comprehensive regulations such as the AI Act. The discrepancies in their approaches underscore the global challenge of fostering innovation while ensuring ethical usage.

The thesis advocates for the development of legal frameworks that not only keep pace with technological advancements but also provide a sufficient level of protection from human rights abuses by corporations and law enforcement agencies. These frameworks should promote transparency, uphold principles of justice and fairness, and foster an environment where technological innovations serve the public good without compromising fundamental human rights. In particular, the thesis urges governments to pay particular attention to limiting the discretion of law enforcement authorities in a way that does not erode human rights to the point of no return, which is the threat identified in multiple UN reports analyzed.

To achieve this, it is essential for international organizations, governments, private corporations, and civil society organizations to collaborate in shaping policies that address the complexities of FRT and for civil society in particular to monitor relevant legal and policy development and oppose those initiatives that further undermine human rights protection. This cooperation is essential to develop standards that not only respect privacy and civil liberties but also provide clear guidelines for the ethical application of this transformative technology. The continuous evolution of FRT demands a dynamic legal response—one that is adaptable and resilient enough to protect human rights in a rapidly changing digital world.

7. BIBLIOGRAPHY

1. Access Now, Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move, 13 March 2024, available at - https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/.

2. *Agencies Should Have Better Awareness of Systems Used by Employees*, 2021, available at - https://www.gao.gov/products/gao-21-105309.
3. AlgorithmWatch and Bertelsmann Stiftung, *Report Automating Society 2019 and 2020*, available at - https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/10/Automating-Society-Report-2020.pdf.
4. AIAAIC, *German privacy watchdog investigates PimEyes for privacy abuse*, December 2022, available at - https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/german-privacy-watchdog-investigates-pimeyes-for-privacy-abuse.

5. AIAAIC, PimEyes sued in Illinois, USA, for privacy violations, May 2023, available at - https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/pimeyes-sued-in-illinois-usa-for-privacy-violations.

6. AIAAIC, *UK pressure group accuses PimEyes of surveillance, privacy abuse*, May 2023, available at - https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/uk-pressure-group-accuses-pimeyes-of-surveillance-privacy-abuse.

7. American Civil Liberties Union, *ACLU, and Clearview AI Settlement Agreement and Release*, May 4, 2022, available at - https://www.aclu.org/legal-document/exhibit-2-signed-settlement-agreement.

8. American Civil Liberties Union, *ACLU v. Clearview AI*, American Civil Liberties Union, May 11, 2022, available at - https://www.aclu.org/cases/aclu-v-clearview-ai.

9. Amicus Curiae Brief Of The American Civil Liberties Union And The American Civil Liberties Union Of New Jersey In Support Of Plaintiff's Opposition To Defendants' Motion For Summary Judgment to the Case of Parks V. Mccormac, Case 2:21-cv-04021-JKS-LDW, available at - https://www.aclu.org/cases/parks-v-mccormac?document=Amicus-Brief#legal-documents.

10. Amnesty International, *EU: Artificial Intelligence rulebook fails to stop the proliferation of abusive technologies*, 13 March 2024, available at - https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/.

11. Amnesty International, EU: European Parliament Adopts Ban on Facial Recognition but Leaves Migrants, Refugees and Asylum Seekers at Risk, June 19, 2023, available at -https://www.amnesty.org/en/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/.

12. Amnesty International, *New EU Dual Use Regulation Agreement 'a Missed Opportunity' to Stop Exports of Surveillance Tools to Repressive Regimes*, November 23, 2021, available at - https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/.

13. Andy Nghiem, Illinois residents allege facial image search engine violates BIPA, 18 May 2023, available at - https://madisonrecord.com/stories/642174142-illinois-residents-allege-facial-image-search-engine-violates-bipa.

14. Austrian SA**,** *Decision against Clearview AI Infringements of Articles 5, 6, 9, 27 GDPR*, 10 May 2023, available at - https://edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en.

15. Barney, Nick, and Corinne Bernstein, *Face Detection*, Enterprise AI, April 20, 2023, available at - https://www.techtarget.com/searchenterpriseai/definition/face-detection.

16. Berle, FACE RECOGNITION TECHNOLOGY, Law, Governance and Technology Series 41, Springer Nature Switzerland AG 2020.

17. Big Brother Watch, *Biometric Britain: the Expansion of Facial Recognition Surveillance*, 23 May 2023.

18. Big Brother Watch, *Submission To The Information Commissioner Request For An Investigation Into Carribex Ltd T/A Pimeyes Unlawful Processing Of Biometric Data*, available at - https://bigbrotherwatch.org.uk/wp-content/uploads/2022/11/20220912-Big-Brother-Watch-Submission-re-PimEyes-AS-SENT.pdf.

19. Big Brother Watch, *Big Brother Watch Files Legal Complaint Against Co-Op's "Orwellian" Facial Recognition*, 26 July 2022, available at - https://bigbrotherwatch.org.uk/2022/07/big-brother-watch-files-legal-complaintagainst-co-ops-orwellian-facial-recognition.

20. Bogle, A. *Australian federal police officers trialled controversial facial recognition tool Clearview AI,* Australian Broadcasting Corporation News, (2020, April 14), available at - https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894.

21. C. Castelluccia and D. Le Métayer Inria, *Impact Analysis of Facial Recognition, Centre for Data Ethics and Innovation*, 2020, available at - https://inria.hal.science/hal-02480647/document

22. Candriam, *Facial Recognition and Human Rights:Investor Guidance*, March 2021.

23. Case C-623/17, Privacy Int'l v. Sec'y of State for Foreign & Commonwealth Aff., ECLI:EU:C:2020:790 (Ct. of Justice of the European Union Sept. 6, 2020).

24. Carrega, Christina, and Christina Carrega. *Facial Recognition Technology and False Arrests: Should Black People Worry?*, Capital B News, December 2, 2023, available at - https://capitalbnews.org/facial-recognition-wrongful-arrests/.

25. Center for Democracy and Technology. *Limiting Face Recognition Surveillance: Progress and Paths Forward*, October 3, 2022, available at - https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/.

26. City and County of San Francisco, *Board of Supervisors Approval of Surveillance Technology Policy*, 2019 Admin Code Section 19B.2(d), available at - https://sfbos.org/sites/default/files/o0286-19.pdf;

27. CNIL, *Facial Recognition: 20 Million Euros Penalty against CLEARVIEW AI*, n.d., available at - https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai#:~:text=Facial%20recognition%3A%2020%20million%20euros%20penalty%20against%20CLEARVIEW%20AI,-20%20October%202022&text=Following%20a%20formal%20notice%20which,delete%20the%20data%20already%20collected.

28. Colorado Artificial Intelligence Act 24-205, 17 May 2024, available at - https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.

29. Council of Europe, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, *Guidelines on Facial Recognition*, June 2021.

30. Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, 17 May 2024, available at - https://rm.coe.int/1680afae3c.

31. Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.

32. Council of Europe, *European Social Charter (Revised)*, 3 May 1996, ETS 163.

33. D. Davies, *Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State,'* NPR, available at - https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-insidechinassurveillance-Sta.

34. Danny Tobey, Tony Samp, Coran Darling, Connor Scott, Todd Mobley, Ted Loud, *Colorado enacts first-in-the-nation comprehensive AI guardrails*, 28 May 2024, available at - https://www.dlapiper.com/en-gb/insights/publications/2024/05/colorado-enacts-first-in-the-nation-comprehensive-ai-guardrails.

35. Dauvergne, Peter. 2022. *Identified, Tracked, and Profiled: The Politics of Resisting Facial Recognition Technology*. Cheltenham, England: Edward Elgar Publishing.

36. Department of Homeland Security, *Use of Facial Recognition and Face Capture Technologies, 2023*, available at - https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capturetechnologies.pdf.

37. 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.

38. Directive 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, 2016 O.J. (L 119) 89.

39. Elizabeth Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1 (2020), available at - https://law.stanford.edu/wp-content/uploads/2020/12/Rowe-FINAL-Facial-Recognition.pdf.

40. EU Artificial Intelligence Act, 19 April 2024, available at - https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf

41. European Commission, *Impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council*, 2021, 18, available at - https://eur-lex.europa.eu/resource.html?uri=cellar:0694be88-a373-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

42. European Court of Human Rights, *Glukhin v. Russia*, No. 11519/20, July 4, 2023.

43. European Data Protection Board and European Data Protection Supervisor, joint opinion 5/202.

44. European Data Protection Board, *Guidelines 05/22 on the use of facial recognition technology in the area of law enforcement*, 12 May 2022.

45. European Parliament, *Regulating Facial Recognition in the EU*, September 2021, 8, available at - https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

46. European Parliamentary Research Service, *Regulating Facial Recognition in the EU*, September 2021, available at - https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

47. European Union Agency for Fundamental Rights, *Facial Recognition Technology: fundamental rights considerations in the context of law enforcement*, 2019, 1-2.

48. E. Rowe, Regulating Facial Recognition Technology in the Private Sector, Stanford Technology Law Review, Vol. 24(1), 2021, 31, available at - https://law.stanford.edu/publications/regulating-facial-recognition-technology-in-the-private-sector/.

49. Facewatch, *Facewatch System Installation Guide*, available at - https://www.facewatch.co.uk/wp-content/uploads/2020/03/Facewatch-Installer-Guide-v2f-web.pdf.

50. *Facewatch To Stop Using Hikvision Amid Controversy Over UK Retail Biometrics*, Biometric Update, 23rd March 2023, available at - https://www.biometricupdate.com/202303/facewatch-to-stop-using-hikvision-amidcontroversy-over-uk-retail-biometrics.

51. Facial Recognition Technology Act of 2022, Title 1, available at - https://lieu.house.gov/sites/evo-subsites/lieu.house.gov/files/evo-media-document/facial-recognition-act-of-2023.pdf

52. French SA, *Facial Recognition: The French SA Imposes a Penalty Payment on CLEARVIEW AI*, European Data Protection Board," n.d., available at - https://edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en.

53. Garvie, C., Bedoya, A., & Frankle, J., *The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Centre on Privacy and Technology Report,* 2019.

54. Government Accountability Office (GAO), *"Facial Recognition Technology: Federal Law Enforcement*

55. Government Accountability Office, 2022, *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues,* available at - https://www.gao.gov/products/gao-22-106154.

56. High-Level Expert on AI, *Ethics guidelines for trustworthy AI,* 2019, 33, available at - https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

57. Human Rights Council, *Report of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age,* 13 September 2021, A/HRC/48/31.

58. Human Rights Council, *Updated draft legally binding instrument (clean version) to regulate, in international human rights law, the activities of transnational corporations and other business enterprises*, available at - https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/igwg-transcorp/session9/igwg-9th-updated-draft-lbi-clean.pdf ("Updated Third Draft"), Articles 1.8, 6.

59. India, Raghavendra Kumar, *An Overview on Amazon Rekognition Technology*, 2021, Electronic Theses, Projects, and Dissertations. 1263.

60. Introna, L. and Nissenbaum, H. (2010), *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Lancaster University Management School Working Paper 2010/030.

61. Italian SA, Fines Clearview AI EUR 20 million, February 10, 2022, available at - https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en.

62. Inter-American Commission on Human Rights (IACHR), American Declaration of the Rights and Duties of Man, 2 May 1948.

63. J. Cavazos et al., *Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?*, IEEE Transactions on Biometrics, Behaviour and Identity Science, 2021, available at - https://ieeexplore.ieee.org/abstract/document/9209125.

64. J. Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation, 2020, 11-12, available at - https://www.eff.org/wp/law-enforcement-use-face-recognition.

65. Kate Conger, Richard Fausset, Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, May 14, 2019, available at - https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

66. K. Hao, After Feeding Explosion of Facial Recognition, China Moves to Rein It In," Wall Street Journal, available at - https://www.wsj.com/articles/china-drafts-rules-for-facial-recognition-use-4953506e.

67. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://perma.cc/F2PG-JE7H.

68. Khoury, Rita El. *Trusted Face Smart Unlock Method Has Been Removed from Android Devices*, Android Police, September 4, 2019, available at - https://www.androidpolice.com/2019/09/04/trusted-face-smart-unlock-method-has-been-removed-from-android-devices/.

69. Klosowski, Thorin. "Facial Recognition Is Everywhere. Here's What We Can Do About It." Wirecutter: Reviews for the Real World, July 15, 2020, available at - https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

70. Le, James, *Snapchat's Filters: How Computer Vision Recognizes Your Face*, Medium, July 25, 2018, available at - https://data-notes.co/snapchats-filters-how-computer-vision-recognizes-your-face-9907d6904b91#:~:text=This%20is%20done%20with%20the,the%20image%20that%20is%20provided.

71. Mac, Ryan, and Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limits on Facial Recognition Database*, The New York Times, May 9, 2022, available at - https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.

72. Mark Townsend, *Revealed: Home Office secretly lobbied for facial recognition 'spy' company*, 2 September 2023, The Guardian, available at - https://www.theguardian.com/technology/2023/sep/02/home-office-accused-of-secret-lobbying-for-facial-recognition-spy-company.

73. Metropolitan Police United Kingdom, *Facial Recognition Technology: Live Facial Recognition*, available at - https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology.

74. M. Xiao, P. Mozur, I. Qian, and A. Cardia, *China's Surveillance State Is Growing: These Documents Reveal How*, New York Times, 21 June 2022, https://www.nytimes.com/video/world/asia/100000008314175/chinagovernment-surveillance-data.html.

75. National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance. Washington, DC: The National Academies Press (2024).*

76. N. Turner Lee, P. Resnick, and G. Barton, A*lgorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, Brookings, 2019, 32-34, available at - https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

77. Obari, Dreamchild, *What Is Apple's Face ID and How Does It Work?*, MUO, June 12, 2023, available at - https://www.makeuseof.com/apple-face-id-explained/.

78. Office of the Privacy Commissioner of Canada, *Announcement: Clearview AI Ordered to Comply with Recommendations to Stop Collecting, Sharing Images*, December 14, 2021, available at - https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/.

79. OVD-Info, *How the Russian State uses cameras against protesters*, January 17, 2022, available at - https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters?_gl=1*1d4s3uo*_ga*MTYzMDUxMjQxMC4xNzAxNDM4NjYy*_ga_J7DH9NKJ0R*MTcwMTQzODY2MS4xLjEuMTcwMTQzODY3My40OC4wLjA.#1.

80. Organization of American States (OAS), *American Convention on Human Rights*, "Pact of San Jose", Costa Rica, 22 November 1969.

81. Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights*, 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

82. P. Grother et al., Face Recognition Vendor Test (FRVT), 2019, available at - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

83. P. Mozur, M. Xiao, and J. Liu, *How China Polices the Future: An Unseen Cage of Surveillance*, New York Times, p. A1, 25 June 2022.

84. Palmiotto, Francesca, and Natalia Menéndez González, *Facial Recognition Technology, Democracy and Human Rights*, Computer Law & Security Review, September 1, 2023.

85. *Patel v. Facebook, Inc.*, No. 18-15982 (9th Cir. 2019), available at - https://law.justia.com/cases/federal/appellate-courts/ca9/18-15982/18-15982-2019-08-08.html.

86. Paul Mozur, *One month, 500,000 face scans: how China is using A.I. to profile a minority*, *New York Times*, 14 April 2019.

87. Peter Dizikes, *How an AI-tocracy emerges*, July13, 2023, available at - https://economics.mit.edu/news/how-ai-tocracy-emerges.

88. Rachel Pester, *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit*, 14 February 2020, available at

- https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit.

89. Ramya Mohanakrishnan, *Top 11 Facial Recognition Software in 2021*, September 2, 2021, available at - https://www.spiceworks.com/it-security/identity-access-management/articles/facial-recognition-software/.

90. R (Bridges) v. Chief Constable of South Wales Police, 11 August 2020, Case No. C1/2019/2670, [2020] EWCA Civ 1058, available at - https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

91. 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.

92. Reventlow, Nani Jansen, *How Amazon's Moratorium on Facial Recognition Tech Is Different From IBM's and Microsoft's*, Slate Magazine, June 11, 2020, available at - https://slate.com/technology/2020/06/ibm-microsoft-amazon-facial-recognition-technology.html.

93. Satariano, *London Police Are Taking Surveillance to a Whole New Level*, New York Times, updated October 1, 2021, available at - https://www.nytimes.com/2020/01/24/business/london-police-facial-recognition.html.

94. S.681 - 118th Congress (2023-2024): Facial Recognition and Biometric Technology Moratorium Act of 2023, S.681, 118th Cong. (2023).

95. Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, San Francisco Chronicle, *16 July 2019, available at - https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.*

96. Schroff, Florian, Dmitry Kalenichenko, and James Philbin. *FaceNet: A Unified Embedding for Face Recognition and Clustering*, June 1, 2015, available at - https://doi.org/10.1109/cvpr.2015.7298682.

97. Smith, Marcus, and Seumas Miller. 2021. *Biometric Identification, Law and Ethics*. 1st ed. Cham, Switzerland: Springer Nature.

98. State of Illinois Biometric Information Privacy Act of 2008, Public Act 095-0994, 740 ILCS 14, 3 October 2008, available at - https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

99. Statt, Nick, *Microsoft's Windows Hello Will Make Your Face, Finger or Iris the New Sign-In*, CNET, March 17, 2015, available at - https://www.cnet.com/news/privacy/microsoft-introduces-windows-hello-for-signing-in-with-your-face-finger-or-iris/.

100. Tatiana Rice, *Colorado Makes History with the Nation's First Comprehensive AI Act*, 24 May 2024, available at - https://www.techpolicy.press/colorado-makes-history-with-the-nations-first-comprehensive-ai-act/

101. The bipartisan Senate AI Working Group, *Driving Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate*, May 2024, available at - https://www.schumer.senate.gov/imo/media/doc/Roadmap_Electronic1.32pm.pdf.

102. Trades Union Congress, *Technology managing people - The worker experience*, 2021, 3, available at - https://www.tuc.org.uk/sites/default/files/2020-11/Technology_Managing_People_Report_2020_AW_Optimised.pdf.

103. Qian, M. Xiao, P. Mozur, and A. Cardia, China's Expanding Surveillance State, New York Times, p. A10, 27 July 2022.
104. United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI.
105. UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.
106. UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3.
107. UN General Assembly, *International Convention on the Elimination of All Forms of Racial Discrimination*, 21 December 1965, United Nations, Treaty Series, vol. 660, p. 195.
108. UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, 18 December 1979, United Nations, Treaty Series, vol. 1249, p. 13.
109. United Nations High Commissioner for Human Rights, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, 2020, available at - https://www.ohchr.org/en/press-releases/2020/06/new-technologies-must-serve-not-hinder-right-peaceful-protest-bachelet-tells?LangID=E&NewsID=25996.

110. UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, (28 May 2019) A/HRC/41/35.

111. UN Special Rapporteur on the rights to peaceful assembly and of association, Clément Nyaletsossi Voule, *Human rights compliant uses of digital technologies by law enforcement for the facilitation of peaceful protests* (2024).

112. United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, United Nations (2011), available at - https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

113. Vallance, By Chris, *Face Search Company Clearview AI Overturns UK Privacy Fine*, BBC News, October 18, 2023, available at - https://www.bbc.com/news/technology-67133157.