

From Identification to Mass Surveillance: FRT use and Regulation in the United States of America*

Yvonne-Marie Rogez

(Associate Professor and Vice-President in charge of the 4EU+ European University Alliance at Paris-Panthéon-Assas University)

ABSTRACT FRT (facial recognition technology) in the United States of America is subjected to differing forms of regulation, from bans to lighter restrictions. They originate mostly from state and local governments and aim to control its use by private companies and law enforcement. There is however no all-encompassing regulation or oversight at the federal level. The first part of this study analyses the different types of FRT uses and regulations in the U.S., showing how the complexity and specificity of governmental regulation allows for a rather permissive use of FRTs. The second part demonstrates how protest movements, and more specifically the protests following the death of George Floyd and the January 6th attack on the Capitol, have been both a catalyst for the government and source of concern for civil rights groups. The ever-growing effectiveness of FRT, as well as its flaws, pose new legal challenges and the question of what may be the most shielding law-making process.

KEYWORDS: Civil rights - Facial recognition technology - Protest movements - Surveillance - United States of America

TABLE OF CONTENTS: 1. Introduction. – 2. Balancing privacy issues and technological progress: FRT regulation in the United States. – 2.1. Definitions. – 2.2. Federal-level regulation. – 2.3. State-level regulation. – 3. Flaws, concerns and lawsuits. – 3.1. Civil liberties and the U.S. Constitution: discrimination, false negatives, false positives and the end of anonymity. – 3.2. Protests and civil rights claims. – 3.3. Wrongful arrests.

1. Introduction

In the United States of America, the use of facial recognition technology (FRT) by law enforcement was banned from the onset in certain states and municipalities.¹ It is the only advanced technology to have been subjected to such a strong legislative reaction. The reasons for this may be found in the fact that people's faces are pervasive: omnipresent when individuals are out on the public space and difficult to obstruct or alter.² This gives the face a unique status as a biometric marker and therefore only regulation, state and federal, may limit its use by both the government and private companies, focusing on the circumstances of its use, including consent, who can use and apply FRT, and whose face may be subjected to FRT. The U.S. government first expressed interest in FRT in 1996 when the effectiveness of FRT in

identifying suspects was brought forward. The US Department of Defense then invested in the FERET (Face Recognition Technology) project which established a database of facial images, and its report, "The FERET Evaluation Methodology for Face Recognition Algorithms", was published in 1999.³ Since then, FRT has developed into an essential tool for both law enforcement and private companies, who use the biometric information they collect for business purposes.

There are three categories of regulations of FRT in the U.S.: bans, moratoriums and others that could be described as intermediate regulations. There is indeed a distinction to be made between bans and moratoriums, as the latter allow for more flexibility and adaptability to changes in circumstances, particularly when the use of certain FRTs is considered as safe and controlled. Another distinction must be established between regulations aimed at the treatment of information by public authorities and by private companies. Private companies use FRT to turn on phones, detect rare genetic diseases or even find a lost pet. In 2023,

* Article submitted to double-blind peer review.

¹ For instance: Vermont in 2020 and Virginia in 2021, 13 cities in Massachusetts from 2019, San Francisco, Berkeley and Alameda in California, Portland in Oregon, Portland in Maine in 2019 and 2020.

² M. Fidler and J.(G.) Hurwitz, *An Overview of Facial Recognition Technology Regulation in the United States*, in R. Matulionyte and M. Zalnieriute (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge Law Handbooks, Cambridge University Press, 2024, 214-227.

³ https://tsapps.nist.gov/publication/get_pdf.cfm?pubid=900863.

Yvonne-Marie Rogez

Forbes⁴ listed 14 new uses, including commercial real estate security, authentication⁵ for banking services, patient safety in healthcare, but also refusing services, such as access to large venues. Public authorities use them for law enforcement purposes. One last distinction must be made between the laws and ordinances that apply in a city, a whole state, or the federal level. There is in the US a multiplicity of uses and levels of authorities that may use FRT. However, there is not a single state in the USA today where FRT is banned without exceptions.

In the last few years, there have been two distinct and rather opposite movements in FRT uses and regulation. The use of FRT by private companies has been increasingly limited and controlled, while regulation of its use by law enforcement has followed a clear movement away from total bans and towards more exceptions and flexibility, due to increasing crime rates and shortages of staff.⁶ Both movements seem to come with the realization that FRT may lead to the mass surveillance of individuals. The terms mass surveillance cover two different phenomena which can both be described as surveillance “on a grand scale”⁷: the surveillance of masses, *i.e.* of a crowd in the context of a single event, and the constant surveillance of every single individual. While the first type is increasingly applied and raises privacy concerns for civil rights groups, the second type is often seen as the unfortunate and unintentional consequence of a technology whose benefit/risk assessment weighs in favor of its use, particularly by law enforcement. Legal scholars have indeed warned against extensive use of FRT, with Woodrow Hartzog & Evan Selinger famously calling FRT “the

most uniquely dangerous surveillance mechanism ever invented”⁸.

The first part of this study analyses the different types of FRT uses and regulations in the US, showing how the complexity and specificity of governmental regulation allows for a rather permissive use of FRTs. The second part demonstrates how protest movements have been both a catalyst for the government and source of concern for civil rights groups. The ever-growing effectiveness of FRT, as well as its flaws, poses new legal challenges and the question of what may be the most shielding law-making process.

2. Balancing privacy issues and technological progress: FRT regulation in the United States

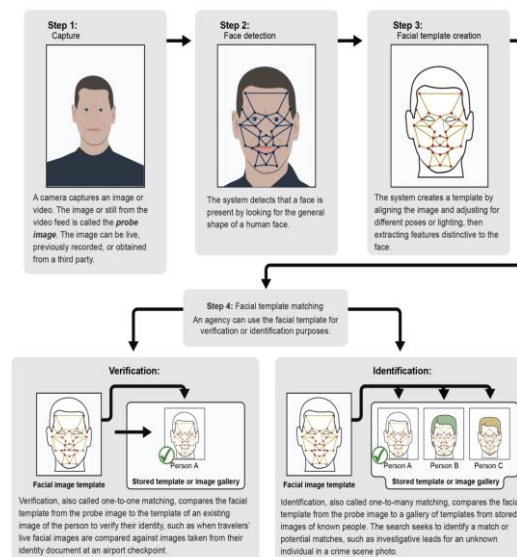


FIG. 1: United States Government Accountability Office, FACIAL RECOGNITION TECHNOLOGY Current and Planned Uses by Federal Agencies, August 2021, www.gao.gov/assets/gao-21-526.pdf

2.1. Definitions

The diagram above, presented by the U.S. Government Accountability Office in its 2021 report on FRT current and planned uses by federal agencies, distinguishes between two types of facial recognition software: those which match a picture against other pictures that are available on a database (verification or authentication / one-to-one), and those that match a picture against another type of picture

⁴ www.forbes.com/councils/forbestechcouncil/2023/08/18/14-intriguing-new-and-potential-uses-for-facial-recognition-technology/#:~:text=Now%2C%20it's%20expanding%20into%20other,security%20and%20offer%20personalized%20experiences.

⁵ Authentication differs from identification as the former verifies the claimed identity of a user while identification simply refers to the process of recognizing who the user is, without verification.

⁶ T.L. Johnson and N.N. Johnson, *Your face could be in this database. How will it be used?*, in *The Washington Post*, 24 February 2025, www.washingtonpost.com/opinions/2025/02/24/ai-crime-facial-recognition-technology.

⁷ The United States Commission on Civil Rights 2024 Statutory Enforcement Report, *The Civil Rights Implications of the Federal Use of Facial Recognition Technology*, 22, www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

⁸ W. Hartzog and E. Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, in *MEDIUM*, 2 August 2018, available at: <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

(identification, or one-to-many matching). Law enforcement use FRTs with these two objectives: verification, to confirm an individual's identity, and identification of an unknown face.⁹ In several states, ordinances and laws mention varied databases and differing picture analysis technologies. The oldest facial recognition tool is the human eye, identifying photographs of people (called "human analysis"), and it does not use artificial intelligence. The most recent technologies include "cloud computing"¹⁰ (the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer), "machine learning" and increasingly precise digital cameras, using artificial intelligence.

Additionally, facial recognition is not limited to an individual's identity and allows for the recognition of many other characteristics. For instance, in the State of Vermont, a 2020 moratorium includes, beyond identification of faces, the automated or semiautomated process by which the characteristics of a person's face are analyzed in order to determine "a person's sentiment, state of mind, or other propensities, including a person's level of dangerousness."¹¹ This distinction between technologies and their applications seems to guide municipalities when deciding exceptions within the bans. This reveals a sort of inverse proportionality rule: the more nonhuman technology the use requires, the less likely it is of being authorized, or at least the more controversial its use will be, as "new technology has always been scary".¹² This rule comes alongside another one which moves towards the

proportionality of exceptions and authorizations with the seriousness of the crime committed or thought to be committed. For instance, the same Vermont law was updated in 2021 and now allows the use of FRT while investigating cases involving the sexual exploitation of children. It permits "law enforcement to utilize facial recognition technology in the investigation of certain crimes provided the search is solely confined to locating images of an individual within electronic media legally seized by law enforcement in relation to the specific investigation."¹³

2.2. Federal-level regulation

There is no all-encompassing regulation or oversight at the federal level that controls the use of FRT. The United States Commission on Civil Rights 2024 Statutory Enforcement Report, *The Civil Rights Implications of the Federal Use of Facial Recognition Technology*, notes that, as of July 2024, there is no official, standardized policy published for federal FRT use.¹⁴ "There are also no federal laws that explicitly protect an individual's civil rights in the use of FRT or other AI technology by the government."¹⁵ However, discriminatory uses of FRT by the government may fall foul of both the *Civil Rights Act 1964* and the *Fair Housing Act 1968*.

In 2023, the U.S. government had spent \$76 million in FRT-related contracts in 20 years.¹⁶ Many U.S. agencies use FRT such as the Bureau of Alcohol, Tobacco, Firearms, and Explosives, U.S. Customs and Border Protection,¹⁷ the Transport Security

⁹ A. Babu and S. Shahin, 'Not Ready for Prime Time': *Biometrics and Biopolitics in the (Un)making of California's Facial Recognition Ban*, in *AI For Everyone?, Critical Perspectives*, University of Westminster Press, 2021, 224.

¹⁰ S. Kumar et al., *Cloud Security Using Face Recognition. Web-Based Services: Concepts, Methodologies, Tools, and Applications*, edited by Information Resources Management Association, IGI Global, 2016, 2055-2075, <https://doi.org/10.4018/978-1-4666-9466-8.ch090>.

¹¹ Vermont General Assembly, *Bill as Introduced and Passed by Senate and House S. 124 2019*, 2020, <https://legislature.vermont.gov/Documents/2020/Docs/BILLS/S-0124/S-0124%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf>.

¹² C. Keil, *New technology has always been scary*, in *Medium*, 20 September 2021, available at: <https://medium.com/pronouncedkyle/new-technology-is-always-scary-8bf977a13773>.

¹³ VT H0195, An act relating to use of facial recognition technology by law enforcement in cases involving sexual exploitation of children. www.billtrack50.com/billdetail/1301705.

¹⁴ The United States Commission on Civil Rights 2024 Statutory Enforcement Report, *The Civil Rights Implications of the Federal Use of Facial Recognition Technology*, www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

¹⁵ *Ibid.*, 16.

¹⁶ C. Rabinowicz, *Approaches to Regulating Government Use of Facial Recognition Technology*, in *Jolt Digest*, 4 May 2023, <https://jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-of-facial-recognition-technology>.

¹⁷ This represents the most extensive use of FRT at the federal level. All international airports and 53 domestic airports use Biometric Facial Comparison Technology (www.cbp.gov/travel/biometrics). This technology was extended to 40 seaports and all pedestrian entry lanes into the US from the North and South-West borders.

Administration, the Drug Enforcement Administration, the Federal Bureau of Investigation, Homeland Security Investigations, the U.S. Marshals Service and the U.S. Secret Service. They use five different services: IntelCenter, Marinus Analytics, Thorn, Idemia, and Clearview AI.¹⁸ Some of these agencies have established rules and directives, such as the Department of Homeland Security's *Use of Face Recognition and Face Capture Technologies*,¹⁹ outlining authorized uses.

Under Biden's presidency, in July 2023, Senator Ed Markey (D-MA) and other congresspersons introduced the *Facial Recognition and Biometric Technology Moratorium Act 2023*.²⁰ This bill imposes limits on the use of biometric surveillance systems by federal, state, and local government entities and provides that an individual aggrieved by a violation of these restrictions shall have the right to sue. In October 2023, President Biden issued an Executive Order "to ensure that America leads the way in seizing the promise and managing the risks of artificial intelligence".²¹ It was revoked in January 2025 by President Trump who highlighted the fact that: "It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security."²² The Biden-era timid movement towards regulation may then be fully halted, as the Republican's "emphasis on privacy, business freedom, and innovation",²³ including technological development, showcases a desire to move towards less federal regulation.

It is interesting to note that, faced with the current lack of strict regulation, two major

FRT developers, Amazon²⁴ (using Rekognition) and Microsoft²⁵ (using Azure OpenAI Service) have paradoxically implanted moratoriums,²⁶ and renewed them, on the use of their technology by law enforcement. These self-generated moratoriums are meant to stay in place until Congress passes the regulatory legislation they deem necessary. However, the future of these moratoriums could be uncertain. In January 2025, Meta decided to change its online moderation guidelines.²⁷ As their hate speech guidelines initially reached beyond the constitutional limits placed upon governments, the question of the same process of deregulation happening with FRT can then be raised.

2.3. State-level regulation

Regulation is therefore mostly established at state, county and municipal level and the diversity of the different types of regulation is noteworthy. Concerning their use by law enforcement, there are bans, such as *Bill S.1385* in Massachusetts²⁸ and Chapter 19B of the Administrative Code of the City of San Francisco,²⁹ moratoriums, such as the

¹⁸ *Ibid.*, 15.

¹⁹ www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.

²⁰ www.congress.gov/bills/118/congress/senate/bills/681.

²¹ www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

²² www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

²³ A. Kimery, *Biometrics regulation under Trump likely to minimize federal overreach*, in *BiometricUpdate.com*, 13 November 2024, www.biometricupdate.com/202411/biometrics-regulation-under-trump-likely-to-minimize-federal-overreach.

²⁴ www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition.

²⁵ <https://learn.microsoft.com/en-us/legal/cognitive-services/openai/code-of-conduct>. The Code of Conduct states that: "Customers, users, and applications built with Microsoft Generative AI Services and Azure AI Content Safety must NOT use the services:- for facial recognition purposes (including identification or verification of individual identities) by or for a state or local police department in the United States -for any real-time facial recognition technology on mobile cameras used by any law enforcement globally to attempt to identify individuals in uncontrolled, "in the wild" environments, which includes (without limitation) police officers on patrol using body-worn or dash-mounted cameras using facial recognition technology to attempt to identify individuals present in a database of suspects or prior inmates".

²⁶ Ironically, this move resulted from the bad publicity that followed the publication of J. Buolamwini and T. Gebru's research, *Gender Shades*, in February 2018, which highlighted the fact that FRT programs created by companies such as IBM and Microsoft were less efficient when processing images of women and individuals with darker skin (<https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>).

²⁷ www.nbcnews.com/tech/social-media/meta-new-hate-speech-rules-allow-users-call-lgbtq-people-mentally-ill-rcna186700.

²⁸ *Bill S.1385*, An Act establishing a moratorium on face recognition and other remote biometric surveillance systems, 2019. <https://malegislature.gov/Bills/191/SD671>.

²⁹ https://codelibrary.amlegal.com/codes/san_francisco/

California Biometric Surveillance Bill 2019 which banned police from using facial recognition and biometric scanners in body-worn cameras for 4 years and was not extended; “light regulations” such as technology specific regulations (like the use of drones in the City of Los Angeles³⁰); limitations to the warrantless use of FRT by law enforcement; the establishment of dedicated taskforces and working groups;³¹ requirements for the publication of reports and transparency requirements;³² and the validation of contracts between municipalities and tech companies.³³ Conversely, the City of New York uses FRT extensively, using databases of images obtained during criminal investigations and mugshots.³⁴ However, in several states using FRT, matches cannot be used as probable cause for arrests.³⁵ Overall, there are currently only a very small number of total bans within the 50 states. Twenty-five states or municipalities have enforced bans and even the most stringent of these bans, like the Vermont ban, have recently allowed for exceptions.

Some state laws focus on users and target the use of FRT and customers’ biometric information by private companies. The first and most famous of these laws is the *Illinois Biometric Information Privacy Act 2018*. It establishes standards which companies must follow when handling consumers’ biometric information. Under this law, in June 2024, Clearview AI agreed to a settlement in a lawsuit alleging its massive photographic

collection of faces violated the subjects’ privacy rights.³⁶ Texas and Washington have also enacted biometric privacy legislation. In July 2024, Meta agreed to pay \$1.4 billion to the State of Texas for illegally using facial-recognition technology and collect biometric data of millions of Texans without their consent.³⁷ Broader consumer data privacy laws were enacted in over 20 states. There is also a multiplicity of bills which were introduced in various states and were never passed including bans that would have provided for a blanket prohibition of the use of information collected by FRT.³⁸

State laws have recently evolved towards less restrictions and more exceptions. Where the use of FRT during the protests following the death of George Floyd had raised concern among civil rights groups and government alike and led to the implementation of around 25 bans, this trend was reversed in 2022. The State of Virginia and the Cities of New Orleans and San Francisco, where strong bans were in place, decided to allow for the use of FRT in some situations. There are a few possible reasons for these reversals, including concerning rises in crime rates and the January 6 2021 attack on the U.S. Capitol. The second part of this article deals with the legislation and lawsuits that came with the concerns and dangers linked with the expanding use of FRT.

3. Flaws, concerns and lawsuits

3.1. Civil liberties and the U.S. Constitution: discrimination, false negatives, false positives and the end of anonymity

There have always been many issues raised

atest/sf_admin/0-0-0-47320. For a more in-depth study of the San Francisco ordinances (2019 and 2022), see Y. Rogez, *Les enjeux de la reconnaissance faciale aux Etats-Unis à travers l'exemple de la ville de San Francisco*, in M. Bozzo-Rey, A. Brunon-Ernst and C. Wrobel (eds.), *Reconnaissance faciale : défis techniques, juridiques et éthiques*, Paris, Éditions Panthéon-Assas, 2024, 107-131.

³⁰ clkrep.lacity.org/online/docs/2015/15-0927_misc_09-17-2015.pdf.

³¹ For example in Ohio, Colorado, and at national level.

³² For example in Washington (<https://app.leg.wa.gov/RCW/default.aspx?cite=43.386&full=true&pdf=true>), and in the City of Detroit following the decision in *Williams v. Detroit* (see 2.3 Wrongful arrests), as well as the federal level (<https://www.fbi.gov/news/speeches-and-testimony/facial-recognition-technology-ensuring-transparency-in-government-use>).

³³ For example in San Francisco, New York City and Anchorage (Alaska).

³⁴ nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_10.26.23.pdf.

³⁵ In Alabama, Colorado, Maine, Maryland, Montana, Virginia, and Washington.

³⁶ K. Foody, *Facial recognition start-up Clearview AI settles private suit*, Associated Press, 22 June 2024, <https://apnews.com/article/clearview-ai-facial-recognition-lawsuit-settlement-5a99ded04630a4e94af01f9f3adf1e29>.

³⁷ M. Scarcella and J. Godoy, *Meta to pay \$1.4 billion to settle Texas facial recognition data lawsuit*, in *Reuters*, 31 July 2024, www.reuters.com/technology/cybersecurity/meta-platforms-pay-14-bln-settle-texas-lawsuit-over-facial-recognition-data-2024-07-30.

³⁸ For instance, in Georgia (<https://legiscan.com/GA/text/HB1245/id/2925632>), Hawaii (www.capitol.hawaii.gov/sessions/session2022/bills/HB1226_.HTM), Kentucky (<https://apps.legislature.ky.gov/record/24rs/sb180.html>), New Hampshire (<https://legiscan.com/NH/text/HB1417/id/2072324>), Minnesota (www.revisor.mn.gov/bills/text.php?number=HF2314&type=bill&version=0&session=ls93&session_year=2023&session_number=0) and West Virginia (https://www.wvlegislature.gov/Bill_Status/bills_text.cfm?billdoc=hb5571%20intr.htm&yr=2024&sesstype=RS&i=5571).

by FRT as a technology and by its uses. Indeed, issues beyond identification are a concern, such as profiling (mentioned above) and the detection of identity markers (gender, race, sexual orientation). Poor quality, and the grainy aspect of some of the collected footage or images generate false positives but also false negatives. Civil rights groups point at the threat of mass surveillance and violations of the right to remain anonymous in public spaces and freedom of association. The Commission on Civil Rights has identified three consequences in case of misuse of FRT: wrongful arrest, unwarranted surveillance (without knowledge or consent) and discrimination.³⁹ Indeed, scale needs to be considered when measuring accuracy. If an algorithm is almost 100% accurate, and the number of images it processes is extremely high, this “almost” may lead to thousands of people being misidentified and some wrongfully arrested.⁴⁰ Also, FRT has introduced a revolution in law enforcement as it reversed the entry point of its databases. In 2016, the Georgetown Law Center on Privacy & Technology reported that law enforcement facial recognition networks included over 117 million American adults and explained this evolution in surveillance: “Historically, FBI fingerprint and DNA databases have been primarily or exclusively made up of information from criminal arrests or investigations. By running face recognition searches against 16 states’ driver’s license photo databases, the FBI has built a biometric network that primarily includes law-abiding Americans.”⁴¹ As there is no federal legislation that can be invoked against the use of FRT by law enforcement, individuals have turned to constitutional privacy protections. As Justice Alito wrote in his concurring opinion in *United States v. Jones* (2012): “In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.”⁴² It is indeed modern technology that broke the barriers of modern surveillance.

There is, quite predictably, no specific reference to FRT in the U.S. Constitution.

However, the privacy protections laid out in the Constitution in the Fourth, Sixth (right to be informed of the nature and cause of the accusation) and Fourteenth (equal protection) Amendments, as well as the freedoms protected in the First Amendment (more particularly expressive association), provide the grounds for lawsuits against law enforcement authorities. Under the First Amendment, individuals may claim the fear of being surveilled deters individuals from associating with others. The Fourth Amendment protects against unreasonable searches and seizures from the government and prevents compelled disclosure of information to the government without a warrant. However, when information is communicated to a third party,⁴³ an individual has no expectation of privacy. “This includes merely being seen in public – with few exceptions, under US law an individual may have their public activities tracked, documented, and shared by other individuals and private entities.”⁴⁴ In April 2024, the House of Representatives passed the “Fourth Amendment is not for Sale Act”, which “prohibits law enforcement agencies and intelligence agencies from obtaining the records or information from a third party in exchange for anything of value (e.g., purchasing them); prohibits other government agencies from sharing the records or information with law enforcement agencies and intelligence agencies; and prohibits the use of such records or information in any trial, hearing, or proceeding.”⁴⁵ However, the future of this bill is uncertain as it is now on the hands of the Republican-controlled Senate. Therefore, the regulations described above, which are of varying strength, are what forms the basis for potential lawsuits against the government. The reality, extent and capability of the surveillance operated by the government is best exemplified by protest

³⁹ US Commission on Civil Rights, *Ibid*, 1-2.

⁴⁰ *Ibid.*, 24.

⁴¹ www.perpetuallineup.org.

⁴² *United States v. Jones* 565 U.S. 400 (2012), Justice Alito, concurring in judgment, 12.

⁴³ In the 1970s, The US Supreme Court developed the “third-party doctrine”, “which provides that that a person waives their Fourth Amendment rights in information they voluntarily disclose to a third party. For example, the Fourth Amendment does not apply to the phone numbers that a person dials, because they have disclosed those numbers to the phone company. The police can accordingly obtain a list of anyone’s dialed numbers without a warrant or probable cause.” (Matthew Tokson, “Inescapable surveillance”, *Cornell Law Review*, Vol. 106, p. 409-56, 2021).

⁴⁴ M. Fidler and J.(G.) Hurwitz, *Ibid.*, 217.

⁴⁵ www.congress.gov/bill/118th-congress/house-bill/463 9.

movements and events involving crowds.

3.2. Protests and civil rights claims

There is no better way to understand the threat of extensive FRT use than the realization that there no longer is “anonymity in crowds”. In 2021, the only two events that the U.S. Government Accountability Office reported in its “fast facts” section⁴⁶ are the “civil unrest, riots, or protests following the death of George Floyd in May 2020”, where 6 federal agencies used FRT, and the U.S. Capitol attack on Jan. 6, where 3 agencies did. It is indeed the necessity to investigate large crowds that led to extensive FRT use. Attitudes to FRT regulation however differed in these two events. While what can be defined as “First Amendment” protests led to a desire to restrict FRT use, the unlawful conduct identified on January 6 somehow justified the use of technology in order to punish the offenders. There has always been a link between evolutions and shifts in FRT uses and mass crowds. The “first major breakthrough of police-sponsored facial recognition occurred in 2002, where law enforcement successfully used the technology to identify people in the Super Bowl crowd”.⁴⁷ In 2020, the federal government and local authorities used FRT to identify individuals protesting in reaction to the death of George Floyd. At that time, debates about the biases of algorithms were also taking place against the backdrop of the rise of the “Black Lives Matter” movement and the resurgence of racial tensions. This context undoubtedly amplified the observed trend of moving away from facial recognition. Indeed, the context of those protests helped discover that in many states, police forces used FRT to watch protesters and it was not clear whether they were watching them more for political reasons than real suspicion of criminal activity.⁴⁸ In 2019, the Cities of San Francisco and Oakland

in California and Somerville in Massachusetts adopted bans on the use of FRT by law enforcement. Roughly two-dozen bans of various types were enacted. The San Francisco ban mentioned that: “The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring.”⁴⁹ In Oakland, the president of the municipal board who drafted the ban mentioned the flaws of FRT and its potential violation of protected rights, and more particularly freedom of speech and religion, the right to privacy and the equal protection of the laws. Public protests are precisely what led to the drafting of the 2022 ordinance in San Francisco and illustrated the surveillance shift which happened that year. The City needed to clarify what a legitimate use of this footage by police exactly is. In the case of *Williams v. City and County of San Francisco*, decided by the Superior Court of the County of San Francisco in March 2022, civil rights organizations and activists alleged that the San Francisco police department illegally accessed real-time surveillance footage from more than 400 surveillance private cameras to monitor demonstrators following the Memorial Day police killing of George Floyd in Minneapolis. The suit centered on the demonstrations, where thousands in San Francisco and elsewhere took to the streets to protest against police violence against black and brown people. The City won in the trial court. The Court based its reasoning on the legal application of an exception within the 2019 ban. The protestors were supported by many civil rights and civil liberties activists, including the Electronic Frontier Foundation. They appealed the decision on the 15th of August 2022. In June 2023, the appeal was dismissed as moot. The September 2022 ordinance has been used several times. In January 2023, the SFPD obtained access to live footage collected by hundreds of private cameras for 12 hours during protests in reaction to Tyre Nichols’ death in Memphis Tennessee.⁵⁰ In May 2023, the police

⁴⁶ www.gao.gov/products/gao-21-518.

⁴⁷ G.E. Marino, *Staying a Jane Doe Post Dobbs and Roe: The Risk Modern Technology Poses with Archaic Abortion Restrictions*, in *Northwestern Journal of Technology and Intellectual Property*, Vol. 21, Issue 2, 2024, 256, <https://scholarlycommons.law.northwestern.edu/njtip/vol21/iss2/4>.

⁴⁸ S. Ikeda, *Facial Recognition Bans Begin to Fall around the US as Re-funding of Law Enforcement Becomes Politically Popular*, in *CPO Magazine*, 18 August 2022, www.cpomagazine.com/data-privacy/facial-recognition-bans-begin-to-fall-around-the-us-as-re-funding-of-law-enforcement-becomes-politically-popular.

⁴⁹ <https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A>.

⁵⁰ M. Barba, *Activists Alarmed by San Francisco Police Plan To Monitor Tyre Nichols Protests With Live*

reportedly again used this type of footage in investigations involving Fentanyl dealers.⁵¹

The second event which may have led to the increasing use of FRT by law enforcement is the January 6th attack on the U.S. Capitol. In the investigations that followed, FRT was a particularly effective tool. The government used more than 15,000 hours of surveillance and body-worn camera footage from multiple law enforcement agencies, approximately 1,600 electronic devices, the results of hundreds of searches of electronic communication providers, over 210,000 tips, and over 80,000 reports and 93,000 attachments related to law enforcement interviews of suspects and witnesses and other investigative steps.⁵² This investigation was called by the Justice Department “one of the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence.”⁵³ Since then, the tide seems to have turned and some of the states, cities and counties that had decided to ban the use of images collected by surveillance cameras and facial recognition software are backtracking, relaxing their bans and authorizing their use under certain conditions, for example when the crime committed is particularly violent, or limiting such use to law enforcement. For instance, the City of New Orleans determined that officers could request permission to use FRT for violent crime investigations and the State of Virginia now allows FRT in some situations.⁵⁴

3.3. Wrongful arrests

Recent cases illustrate how the efficiency of FRT as a weapon against crime may be challenged. Numerous studies, including the

Surveillance, The San Francisco Standard, 23 May 2023, <https://sfstandard.com/criminal-justice/san-francisco-police-planned-to-watch-live-surveillance-footage-during-tyre-nichols-protest>.

⁵¹ M. Barba, *SF Police Now Watch Private Cameras in Real Time to Arrest Suspected Fentanyl Dealers*, *The San Francisco Standard*, 17 May 2023, <https://sfstandard.com/criminal-justice/sf-police-watch-private-camera-s-to-arrest-fentanyl-dealers>.

⁵² *United States v. Cudd*, United States District Court for the District of Columbia, 2021.

⁵³ www.politico.com/f/?id=00000178-26d0-da67-a3fe-2ed685160000.

⁵⁴ R. Metz, *First they banned facial recognition. Now they're not so sure*, in *CNN Business*, 5 August 2022, available at: <https://edition.cnn.com/2022/08/05/tech/facial-recognition-bans-reversed/index.html>.

CITRIS Report: the San Francisco Community Safety Camera Program, University of California, Berkeley, in December 2008⁵⁵, and *The Crime Prevention Effect of CCTV in Public Places: A Propensity Score Analysis*, New Jersey 2018⁵⁶ note that there is little evidence that access to video surveillance footage, especially live streams, is efficient when reducing or fighting crime. In its 2024 report, the U.S. Commission on Civil Rights highlights the fact that “there remains a significant risk of false positives for specific demographic groups, including Black people, individuals of East Asian descent, women, and older adults.”⁵⁷ In addition to “automation bias”,⁵⁸ which refers to people’s inclination to trust without reservation the results of computer technology tools, especially as they do not master them, this risk may lead to misidentification. Another cause for concern comes from the fact that black people are overrepresented in police databases and “accuracy is affected by frequency of contact.”⁵⁹

Six cases of wrongful arrests were filed against law enforcement and in five of them, the person who was wrongly arrested was black. In *Oliver v. Detroit* (filed in 2020), *Williams v. Detroit* (filed in 2021), and *Woodruff v. Detroit* (filed in 2023), Porcha Woodruff, Michael Oliver, and Robert Williams took legal action against Detroit police. All three were arrested as a result of a combination of errors: a false match from FRT and false identification from a witness who looked at a photo line-up where the FRT picture appeared alongside five filler photos. Robert William’s case led to a settlement reached in June 2024 and Williams received

⁵⁵ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2183381.

⁵⁶ https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1188&context=jj_pubs.

⁵⁷ US Commission on Civil Rights, *Ibid.*, 109.

⁵⁸ See S. Alon-Barkat and M. Busuioc, *Human-AI Interactions in Public Sector Decision Making: “Automation Bias” and “Selective Adherence” to Algorithmic Advice*, in *Journal of Public Administration Research and Theory*, vol. 33, Issue 1, January 2023, 153-69 or H. Ruschmeier and L.J. Hondrich, *Automation bias in public administration – an interdisciplinary perspective from law and psychology*, in *Government Information Quarterly*, vol. 41, Issue 3, 2024, www.sciencedirect.com/science/article/pii/S0740624X24000455?utm_source=chatgpt.com.

⁵⁹ S.M. Bowen, *Man vs. Machine: Facial Recognition Technology Replacing Eyewitness Identifications*, in *Lincoln Memorial University Law Review*, vol. 10, 2022, 51.

\$300,000. In the settlement, “the City of Detroit and Chief James White recognize the need to safeguard the Fourth Amendment rights of individuals involved in a criminal investigation and to ensure that policy advances to keep pace with evolving technology used to fight crime in the City of Detroit.”⁶⁰ Detroit also amended the “Eyewitness Identification and Lineups” provisions in their Manual Directive, and this was seen as a major victory by civil rights groups. Three other cases, *Parks v. McCormac* (filed in 2021), *Reid v. Bartholomew et al* (filed in 2023), and *Murphy v. Essilorluxottica USA and Macy’s* (filed in 2024) center on the misuse of FRT by the police leading to wrongful arrests. Parks alleges he was wrongfully arrested based as police used AI-driven facial recognition systems in New Jersey. Reid was arrested and held without bond for six days after being misidentified by FRT in Louisiana. In Texas, Murphy was misidentified by a facial recognition system owned by Macy’s and Sunglass Hut and as an armed robber. He is using the company and alleges he was assaulted and raped while in jail awaiting trial.

Courts have repeatedly found or commented on the fact that findings resulting from the use of FRT are not reliable enough to be used as evidence or at least that guilt should be proven solely using FRT identification.⁶¹ Even though in *Leaders of a Beautiful Struggle v. Baltimore Police Department* (2020) the District Court and the Court of Appeals for the Fourth Circuit decided to deny the plaintiffs’ request for a preliminary injunction against Baltimore’s aerial surveillance program, the Circuit court stated that they “agree with plaintiffs that there are aerial surveillance programs that would transgress basic Fourth Amendment protections”. They “further agree that investigative tools, whether aerial or electronic, should not operate without

restrictions”.⁶²

In the United States, whether through the application of State biometric laws or when deciding cases of wrongful arrests and imprisonment and interpreting laws and ordinances, courts often seem to provide the necessary safeguards against the dangers of FRT use. Adjudication also leads to legislation, while highlighting the flaws of FRT use, even though only a small proportion of the disastrous consequences of FRT misuse turns into claims. Recent cases show how dangerous the application of FRT with too much deference and not enough cross-referencing and more traditional methods of investigation can be. Many recommendations aim to alleviate some of the undesirable effects of FRT uses by law enforcement, such as self-regulation at the federal level, the development and mandatory application of FRT testing and internal audits. Specific staff training is also essential in order to avoid identification errors. Some academics would also like the debate to move beyond the traditional “technology-versus-law showdown” as they believe that regulating technology rather than conduct may quickly become irrelevant as newer technology requires new regulation.⁶³

The fears expressed by civil rights groups⁶⁴ reach beyond misidentification and point to the fact that mass surveillance is not only a reality, but privacy has become an illusion. The future of efficient regulation may therefore lie in a combination of political pressure aimed at vindicating privacy and other civil rights, traditional legislation on data use and collection, as well as creating new technological tools in order to lessen the undesirable effects of FRT.⁶⁵ Political choices will reveal the society that is envisaged as the development of AI requires constant observation and adaptation, as well as swift decision-making.

⁶⁰ *Williams v. Detroit*, US District Court Eastern District of Michigan Southern Division, Stipulated Order of Voluntary Dismissal with Prejudice, 28 June 2024, www.aclumich.org/sites/default/files/field_documents/r-obert-williams-settlement-order-and-agreement.pdf.

⁶¹ See for instance: *People v. Collins* (Sup Ct, Kings County), 2015, <https://law.justia.com/cases/new-york/other-courts/2015/2015-ny-slip-op-25227.html>. *People v. Reyes* (Sup Ct, NY County), 2020, <https://law.justia.com/cases/new-york/other-courts/2020/2020-ny-slip-op-20258.html#:~:text=Defendant%20Luis%20Reyes%20is%20charged,seen%20in%20crime%20scene%20video> s.

⁶² *Leaders of a Beautiful Struggle v. Baltimore Police Department*, US Court of Appeals for the Fourth Circuit, 2020, 20. www.aclu-md.org/sites/default/files/field_documents/46_-_4th_cir_opinion.pdf.

⁶³ A. Solow-Niederman, *Information Privacy and the Inference Economy*, in *Northwestern University Law Review*, vol. 117, 357, 2022, <https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1>.

⁶⁴ The two most prominent groups who have expressed those fears are the ACLU and the Electronic Frontier Foundation (EFF).

⁶⁵ J.L. Zittrain, *A World Without Privacy Will Revive the Masquerade*, in *The Atlantic*, 7 February 2020, www.theatlantic.com/technology/archive/2020/02/we-may-ha-ve-no-privacy-things-can-always-get-worse/606250.

