POLICY BRIEF

Rose Barragan Barranco
MSSP 6310 - Law and Social Policy
Professor: Daniel Baker, JD, MPP, PhD
Spring 2024

EXECUTIVE SUMMARY

Have you ever considered the shocking scope of artificial intelligence in using your facial features to make your life easier? From the simple task of unlocking one's phone with a glance to receiving notifications identifying who is at your front door. Even in the public sector, have you ever wondered how it feels when facial technology decides who can cross borders or board a plane? But here's the intriguing question: what if, instead of being a convenience, would your own face become a factor that could complicate your life?

The expansion in the development and deployment of Facial Recognition Technologies (FRT) by public administrations and private organizations is resulting in significant ethical and legal challenges, including invasion of privacy, lack of consent in the collection of biometric data, lack of safeguards, lack of democratic oversight, and indiscriminate application of the technology, particularly affecting vulnerable groups, ethnic minorities, women and specific age groups, who continue to be stigmatized by the US Criminal Justice system.

Moreover, the lack of federal legislation that establishes the foundations for the development and use of FRT and establishes proper measures for overseeing the government's practices is resulting in legal loopholes and opening the door to the vulnerability of citizens' fundamental rights, especially considering the First, Fourth, Fifth, and Fourteenth Amendments of the US Constitution.

That is why this Policy Brief exposes the risks and challenges present in FRT technologies, not to instill fear but to raise awareness and advocate to ensure the proper protection of fundamental rights and freedoms by proposing a set of alternatives that check and balance the state-of-the-art FRT while promoting a more ethical, responsible and legal approach, focusing on protecting individual Constitutional rights and fostering a more inclusive and just society.

1. PROBLEM DEFINITION

In the digital age, Americans are witnessing a rapid expansion of technological advancements, particularly in the field of Facial Recognition Technologies (FRT) (Cision PR Newswire, 2022). However, **FRT growth comes with heightened risks due to insufficient safeguards and a lack of democratic oversight when identifying and tracking individuals' facial information, violating their liberties, undermining their civil rights, and impacting other facets of life.**

This is highlighted by a recent study conducted in 2021 by the US Government Accountability Office (GAO), entitled "Facial Recognition Technology: Current and Planned Uses by Federal Agencies," which has focused on examining its use by federal law enforcement at points of entry and in commercial environments, as well as in digital access and cybersecurity, domestic law enforcement, and physical security.

In the following sections, the policy brief addresses unsettling scenarios of how federal organizations, such as FBI & DMV, CBP & TSA, and NJPD, have indiscriminately and without oversight employed these technologies, in which human beings' civil rights and liberties are severely undermined and even violated due to:

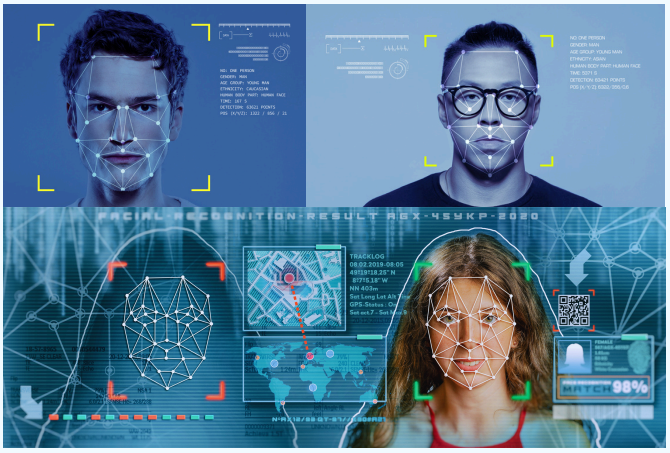
- **The inadequate safeguards in place that lead to technical vulnerabilities and breaches may result in identity theft, stalking, or harassment.**
- **Lack of awareness**
- **Lack of consent for facial data collection**
- **Indiscriminate application**
- **Insufficient democratic oversight**
- **Issues of fairness and reliability (including significant inaccuracies and racial bias)**
- **Lack of accountability and transparency measures**
- **Erosion of anonymity and privacy rights (which are crucial for safety and security)**
- **Unwarranted intrusion into individuals' lives**
- **Legal loopholes within regulations.**

Moreover, the findings of the National Institute of Standards and Technology (NIST) - which is the federal laboratory responsible for developing technology standards – discovered that the majority of facial recognition algorithms display "demographic differential" that can negatively impact their accuracy based on factors such as a person's age, gender, or race (Harwell, D, 2019). Therefore, many facial recognition applications suffer from racial bias and inaccuracies, leading to numerous damaging lawsuits and regulatory issues affecting personal data and privacy.

In other words, a part of what makes face recognition so perilous is that law enforcement agencies and private organizations continually use the technology in secret and without any democratic oversight, where there is a lack of accountability and transparency. The disproportionate use of FRT, unwarranted intrusion into individuals' lives, and legal loopholes within the regulations lead to scenarios in which rights and freedoms are severely under attack. An urgent and immediate call to action is essential to uphold privacy, security, and individual rights and ensure transparent data collection, usage, and storage.

As Jay Stanley, a senior policy analyst at the American Civil Liberties Union (ACLU), says:

"One false match can lead to missed flights, lengthy interrogations, tense police encounters, false arrests, or worse, but the technology's flaws are only one concern. FRT can enable undetectable, persistent, and suspicionless surveillance on an unprecedented scale" (Fox, A., 2019).



2.POLICY CONTEXT

2.1. RELEVANT LAW CASES

It is paramount to highlight that **no federal legislation regulates FRT in the US [*]** (Congressional Research Service, 2020) (Lively, 2021) (Sakin, 2021). As a result, cities, towns, and counties are facing the need to regulate this technology independently. Although the widespread use of FRT has increased nationwide, it has also been criticized by privacy and digital rights advocates due to privacy concerns and other tangible and potential dangers. Here are some observable scenarios in which the use of TRF is already posing significant risks to the rights and freedoms of individuals:

2.1.1. 2019 - 2020: ACLU v. DHS, CBP, TSA, & ICE

Relevant federal organizations such as the Department of Homeland Security (AKA DHS), the US Customs And Border Protection (AKA CBP), the US Immigration And Customs Enforcement (AKA ICE), and the US Transportation Security Administration (AKA TSA) have increasingly employed FRT at airports and other entry points. The first one alone has scanned more than 20 million travelers' faces by mid-2019, in collaboration with international airlines like Delta, JetBlue, and United Airlines, which are collaborating to set up surveillance infrastructure (US Department of Homeland Security, 2019).

However, there are concerns about the extensive and persistent government surveillance that FRT enables, especially given DHS, CBP, TSA, and ICE's past records of tracking journalists, subjecting travelers to invasive searches, and targeting individuals based on factors like their national origin, religious beliefs, or political views.

To shed more light on how federal agencies use facial recognition programs, a lawsuit has been filed [Case 1:20-cv-02213], where the American Civil Liberties Union (AKA ACLU) (plaintiff) sued DHS, CBP, TSA, and ICE's (defendants) in the United States District Court Southern District Of New York (SDNY) on March 2020.

The lawsuit sought information from the DHA, CBP, TSA, and ICE to disclose government contracts with airlines, airports, borders, and other entities related to facial recognition use, biometric information acquisition, processing, retention policies, and evaluation of the technology's effectiveness [Case 1:20-cv-02213] (New York Civil Liberties Union Foundation, 2020).

> ***The FOIA Request*** *(page 6): "The Request seeks several categories of documents pertaining to the use of facial recognition at airports and the border, including government contracts with airlines, airports, and other entities concerning TVS; policies and procedures concerning the acquisition, processing, retention, and dissemination of data acquired through TVS; analyses of the effectiveness of facial recognition technology; records concerning TSA's plans to apply facial recognition technology to domestic travelers […].*
>
> ***Defendants' Responses to the Request*** *(page 6): "Despite the urgent public interest surrounding the requested documents, none of the Defendants have released any record in response to the Request."*

This will help enhance public and policymaker understanding of the federal agencies' facial surveillance systems, assess privacy safeguards, and evaluate potential discrimination based on race or other characteristics in DHS, CBP, ICE, and TSA's use of this technology (ACLU, 2020).

[*]
"There is no overarching federal framework regulating the use of FRT" – (Congressional Research Service, 2020).
"Federal Legislation Lacking: Although Congress has yet to pass federal facial recognition regulation, […]" - (Lively, 2021).
"While there is no federal law in the U.S. to specifically regulate the burgeoning technology, numerous bills have been proposed"- (Sakin, 2021)

2.1.2. 2020 – 2022: ACLU OF ILLINOIS V. CLEARVIEW AI

Clearview AI, a NYC-based start-up, has secretly collected billions of faceprints from personal photos on social media and other online sources. To scale the matter, the company has also been providing access to this database to private companies, law enforcement agencies, federal entities, and wealthy individuals, allowing them to use FRT to track and target individuals without their consent or knowledge (Wessler, 2020).

This has raised significant privacy, security, and legal concerns, and the American Civil Liberties Union of Illinois (Plaintiff) has taken Clearview A.I. (Defendant) to the Circuit Court Of Cook County (Illinois) on behalf of various organizations representing vulnerable communities, including survivors of sexual assault and domestic violence, undocumented immigrants, and people of color (ACLU v. Clearview AI, 2020) [Case number 2020 CH 04353].

These organizations argue that Clearview AI's actions violate the **Biometric Information Privacy Act (BIPA)** *(740 ILCS 14/1)* by collecting and using biometric identifiers without individuals' consent, which requires notification and written consent when obtaining such information from Illinois residents.

To be more specific, BIPA is an Illinois state law enacted in 2008 to regulate the collection, storage, and usage of biometric information, including facial recognition data, by private entities. BIPA applies not only to entities within Illinois but also to companies operating beyond the state's borders. In other words, BIPA applies to any organization (such as Clearview) that collects or uses biometric information of individuals in Illinois (Sheppard Mullin Attorneys, n.d).

740 ILCS 14/15 - SEC. 15. RETENTION; COLLECTION; DISCLOSURE; DESTRUCTION.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity […].

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric information unless it first: 1) informs the subject or the subject's legally authorized represent.ative in writing that a biometric identifier or biometric information is being collected or stored […]; 2) the specific purpose and length of the term […]

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: 1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure[…].

Additionally, Clearview's practices may **violate individuals' due process rights, because:**

- The secretive collection and use of personal data may result in surveillance and potential targeting without the individual's knowledge or consent, essential components of due process.
- This lack of oversight may cause vulnerable communities to be disproportionately affected, facing heightened risks of discrimination, harassment, unjust treatment, and erosion of anonymity and privacy rights, especially if third-party organizations are using the data for monitoring purposes.
- Consequently, the lack of oversight undermines individuals' right to a fair hearing, as they may be subject to surveillance and targeting without any opportunity to challenge or contest the use of their biometric information.

2.1.3.2023 - STATE OF NEW JERSEY v. FRANCISCO ARTEAGA

The case of the State of New Jersey v. Francisco Arteaga [No. A-3078-21] - solved by the Superior Court of New Jersey in 2023 (New Jersey v. Francisco Arteaga, 2023) - is one of the most relevant cases on this topic. The New Jersey Police Department pulled out facial recognition to identify Mr. Francisco Arteaga as a potential criminal suspect in an armed robbery in the city of New Jersey. However, Arteaga's defense was not given any information regarding the algorithm or software used in the process, which raised concerns about the transparency and fairness of the identification.

The Superior Court of New Jersey held that the **defendant's due process rights** would be violated unless he was given access to the raw materials used by police to identify him, as well as information about how the facial recognition software worked, its source code, and its error rate. Such access was necessary to challenge witness identifications, examine the state's investigation, and establish reasonable doubt.

The court's decision highlighted the flaws inherent in facial recognition technology and recognized that it is often unreliable, mainly when dealing with people of color, transgender and nonbinary individuals, and Black women (Gullo, K., 2025). The court also emphasized that law enforcement should not be allowed to use "black box" technology in criminal cases without transparency and scrutiny. Despite these inaccuracies, law enforcement has widely adopted this technology for identifying suspects in criminal cases.

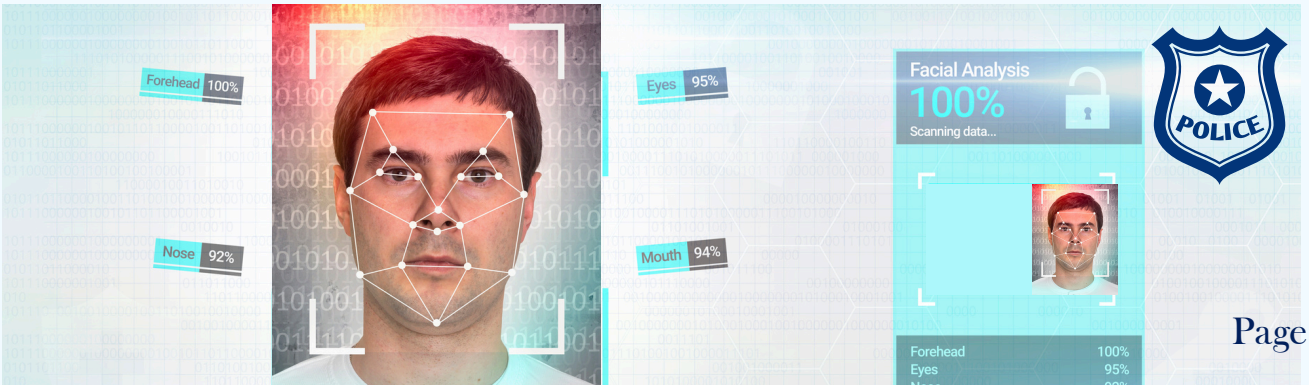
Therefore, the court reaffirmed the principle that due process is essential for safeguarding justice and protecting individuals' rights in the face of technological advancements by:

- Affirming Arteaga's right to access crucial information related to his case.
- Requesting transparency and accountability in the use of FRT by law enforcement.
- Ensuring fair treatment in the legal proceeding by understanding how the technology was employed.
- Emphasizing the importance of procedural protections inherent in due process.

This ruling sets an important precedent for cases involving facial recognition technology and emphasizes the need for defendants to examine and question the reliability of this technology in order to protect their constitutional rights.

2.2. HOW IS THE LAW INVOLVED IN THIS POLICY AREA, AND WHY IS THAT INTERACTION IMPORTANT?

As mentioned in section 2 - Policy Context, the United States still has no current federal regulation to address the problems related to the use of FRT adequately, affecting privacy and civil liberties, and potentially violating the rights and obligations contained in the US Constitution. Therefore, the Constitution's Amendment may provide some restrictions on governmental and law enforcement use of FTRs (Members and Committees of Congress, 2020):



First Amendment

"Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof, abridging the freedom of speech or of the press, or the right of the people peaceably to assemble and to petition the Government for a redress of grievances."

Although free speech is essential for a successful democracy, FRT raises First Amendment questions insofar as it is alleged to have a "deterrent effect" on the exercise of free speech and association. In other words, using FRT could unfairly restrict free speech, the right to assemble, and other rights protected by the First Amendment. For example, if FRT surveillance allows the government to identify participants in public protests easily, it could discourage individuals from exercising their right to free speech, assemble, attend protests, or peaceful demonstrations.

The Supreme Court has indicated that government surveillance of speech and association alone may not be sufficient to state a claim for a First Amendment violation. To do so, the plaintiff must show that the surveillance was linked to some government action that caused harm, such as diminishing the individual's liberties, limiting the spread of truth, enforcing silence, impeding Individual self-fulfillment, etc.

Fourth Amendment

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

Although Fourth Amendment protections against unreasonable searches and seizures generally do not prohibit surveillance by law enforcement, the Supreme Court has expressed concerns about extended technologically enhanced surveillance, and more so when such surveillance becomes so pervasive as to provide "*an intimate window into a person's life*."

For example, in the case **United States v. Jones** [United States v. Jones: 565 US 400, 2012], the Court's ruling was unanimous, holding that the Government's placement and use of a GPS device in a private vehicle to track an individual's movements constitutes a "search" under the Fourth Amendment of the U.S. Constitution. The Court emphasized that the Fourth Amendment provides protection against the Government's invasion of personal property and also rejected the Government's argument that there is no reasonable expectation of privacy in a person's movement on public streets.

In the holding, it is interesting to underscore **Justice Alito's** position, who agreed with the majority, reasoning that the Government violated Jones's reasonable expectation of privacy. However, he added, that today's technologies can change those expectations, shifting the balance between providing greater convenience or security at the expense of privacy. So, under circumstances that involve rapid technological change, the best solution to privacy concerns is legislative.

U.S. v. Jones (2012) is a landmark case because, for the first time, the U.S. Supreme Court ruled on a case that involved data security and electronic privacy. So, the real significance of the case for future scenarios in which the use of electronic data is generalized lies in how technological advances are "shaping the evolution of society's expectations of privacy" (Bosse & Mitchell, 2012).

In an era characterized by the massive use of technologies, the disclosure of personal data to third parties throughout everyday tasks, and tracking individuals' movements, safeguarding the right to "privacy" becomes a challenge.

Fifth and Fourteenth Amendments

"No State shall deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

The Fifth and Fourteenth Amendments cover the **Due Process Clause**, which declares that states may not deny any person life, liberty, or property without due process of law; and the **Equal Protection Clause**, which declares that a state may not deny any person within its jurisdiction equal protection of the laws.

The results of a US federal study conducted in 2019 showed that most FRT exhibited significant **racial bias, with minorities being consistently misidentified** (Harwell, D., 2019). This bias hurdle raised severe questions about the fairness of these Deep Learning algorithms implemented by law enforcement across the nation. The study revealed that some of the algorithms were up to 100 times more likely to misidentify Asian and African American individuals than white males. In comparison, Native Americans had the highest false positive rate among all ethnicities evaluated.

Moreover, the study also found age and gender-related disparities. For example, it showed that women were more prone to false identifications than men, while misidentifications were more present among older people and children (Konfirmi, n.d.). The National Institute of Standards and Technology (NIST) backed up this study with more evidence, which pointed out that most FRT algorithms have differences in demographics, compromising the accuracy levels based on age, gender, or race (Romine, C. H., 2020).

As covered in this Policy brief, one example of how biased FRT algorithms were misused by the police department is the case State of New Jersey v. Francisco Arteaga, where the FRT system resulted in the disproportionate misidentification of Mr. Arteaga, **violating the equal protection clause**.

A second example of misuse of the FRT algorithm by law enforcement bodies is the **Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)**. This algorithm is employed by U.S. courts as part of the pre-sentence investigation (PSI) report to assess a defendant's likelihood of recidivism, violence, or failure to appear (Lee Park, 2019).

Research conducted by the ProPublica firm, called Recidivism Risk Score Data and Analysis, concluded that African American defendants had a higher percentage chance of being incorrectly labeled as a "high-risk group for recidivism." Whereas, even with the same type of criminal profile, White defendants had a higher percentage of being incorrectly labeled as a "low recidivism risk group" (ProPublica, 2020).

Through careful analysis of Broward County (Florida) justice courts, ProPublica was able to demonstrate how COMPAS algorithms incorrectly labeled defendants of color in nearly twice as many cases, resulting in longer sentence lengths or setting higher bail amounts imposed on people of color (McKinsey & Company, 2019) – leading to a **violation of the equal protection clause and due process under the Fourteenth Amendment.**

2.3. DOES IT FIT WITH OTHER INITIATIVES PURSUED AT THE NATIONAL, SUBNATIONAL, OR INTERNATIONAL LEVELS?

- **The Facial Recognition Act of 2022 and Facial Recognition and Biometric Technology Moratorium Act of 2023** (Congress Gov, 2023). These bills aimed at restricting the use of facial recognition and biometric surveillance systems by government entities unless allowed explicitly by Congress. However, neither bill made significant progress.
- **Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through The Federal Government.** In February 2023, the White House issued the Executive Order focusing on advancing racial equity and preventing algorithmic discrimination using technologies like facial recognition (The United States Government, 2023).
- **The Traveler Privacy Protection Act of 2023** (S.3361 - Traveler Privacy Protection Act of 2023), particularly section 3 (a) (b) looks to prohibit the use of facial recognition technology or facial matching software in airports unless specifically authorized by Congress. Additionally, it requires the disposal of any facial biometric information collected through such technology within a certain timeframe.

3.ALTERNATIVES CONSIDERED TO ADDRESS THE POLICY

3.1.HUMAN-CENTRIC MODELS THAT PROMOTE PRIVACY BY DESIGN

On numerous occasions, technology is first developed in response to a problem that needs to be addressed, altogether leaving aside two fundamental considerations of ethical technologies: 1) the importance of people interacting (directly or indirectly) with these technologies and 2) ensuring privacy in the design and development of FRT systems from their very beginning.

Although at first glance they may seem to be two separate considerations, they appeal to the same paradigm since the privacy of the models places people and their data at the center of the FRT design, seeking to 1) understand who will be the end user for whom the FRT is to be intended; 2) what privacy measures will be applied to the data; and 3) guarantee privacy principles and the protection of human rights in an ever-evolving technological environment.

Anonymization and de-identification of facial data involve the application of robust techniques to process and store information in a way that makes it extremely difficult to trace it back to specific individuals. In addition, biometric encryption plays a crucial role in exploring technologies that allow biometric data to be encrypted, ensuring that it can only be decrypted by authorized parties and designated bodies for specific purposes.

Typical methods (Targeted anonymization, 2022) used for facial image anonymization include image processing with face blurring and noise adding (Rosebrock, 2021), data masking techniques (Bales & Fritsch, 2023), K-Same anonymization algorithms (Model-Based Face De-Identification, 2006), and adversarial generative networks (PrivacyNet, 2020) (Ren, Lee, & Ryoo, 2018).

These measures become cornerstones for the ethical development of facial recognition technologies, where each facial image identified by the FR model is anonymized while ensuring high action detection performance. In other words, facial image anonymization methods will ensure both privacy by design and the protection of human rights in an ever-evolving technological environment.

3.2. INDIVIDUAL CONSENT FORMS

This alternative focuses on the principle that individuals have the power and right to give explicit consent to disclose their biometric data before the FRTs can use it. Consent can be either paper or digital, but most importantly, it must address considerations such as:

- **Indicate** how the collection, storage, and specific purpose of the data will be carried out, as well as the identification of the agents who will have access to the data.
- **Establish** mechanisms to facilitate the user's access to their biometric data collected (even if he has given his consent to third parties). In the same way that access is granted, the individual should be able to limit access to third parties or even revoke access at any time and under any circumstances.
- **Set** fines for non-compliance and violation of the consent form when there is a breach or infringement of the agents in the non-consensual use of biometric data.
- **Design** a user-friendly consent form that is easy to access and simple to complete, allowing all stakeholders (regardless of their technological literacy and maturity) to understand what the consent form consists of and their role in the technological society.

As in the previous alternative, this one also promotes a human-centric approach to technologies (from a different perspective), placing individuals at the center of the decision-making process regarding their facial information, which promotes the protection of privacy and individual autonomy.

4. CRITERIA

EFFECTIVENESS

According to the paper "A Framework to Model and Measure System Effectiveness", a baseline definition for effectiveness is: "Measure of Effectiveness is a measure of the ability of a system to meet its specified needs from a particular viewpoint. This measure may be quantitative or qualitative, allowing comparable systems to be ranked". - Neill Smith and Thea Clark (Smith & Clark, n.d.).

Thus, effectiveness evaluates the **degree of success in the implementation and the accuracy rate** of FRT models for anonymizing biometric characteristics of individuals. Effectiveness can be measured in several ways:

- Degree of success in the implementation of the identified measures through the percentage of regions that have successfully implemented the regulatory frameworks, number of legal and prohibited use cases collected in a registry, and number of certifications of technical professionals trained for the ethical development, deployment, and use of FRT.
- Accuracy rate of FRT models for anonymizing biometric characteristics of individuals. The higher the accuracy rate of anonymization, the more effective the system is considered to be.

EFFICIENCY

The most prominent AI Research Laboratory in the United States, called OpenAI, defined efficiency as "the capacity to reduce the compute needed to train a specific capability" (AI and efficiency, n.d.). Therefore, efficiency must take into account **five Key Performance Indicators** (KPIs): 1) training efficiency improvement, 2) performance level, 3) runtime (processing time of the machines), 4) economic cost of development and implementation of the solution, and 5) the scalability of the solution.

For this purpose, a matrix will be created that collects each of the five KIPs to measure efficiency and will be visualized in the form of a spider graph, allowing the analysis and comparison of both the FRT models and the processes and choose those that reflect the highest total efficiency index expressed as a percentage (%). Thus, efficiency looks to handle a high volume of processes without significant performance degradation or detriment to results.

RIGHTS PROTECTION

The Rights Protection criterion seeks to evaluate the level of safeguarding and respect for the fundamental constitutional rights of individuals during the development, deployment, and use of FRT systems, complying with:

- **First Amendment:** it evaluates whether the system respects. It allows the full exercise of constitutional rights protected by the First Amendment, not intending to limit or respect the freedom of speech or association when used by law enforcement bodies.
- **Fourth Amendment:** Evaluates the data security and electronic privacy provided by the FRT system, ensuring that the collection, storage, and processing of biometric data is done securely and that the individual's right to privacy (including expectations of privacy) is respected.
- **Fifth and Fourteenth Amendments:** The extent to which the Due Process Clause and equal protection under the law are protected in the use of FRT is assessed. That is, it verifies whether the FRT algorithms ensure due process and treat all persons fairly and equitably, without discrimination or biases.

EQUITY

It is essential that FRT is developed, deployed, and used in an impartial, fair, and non-discriminatory manner, as well as the bureaucratic and regulatory processes to implement and democratize it throughout society. Misuse or bias can have negative impacts on marginalized or vulnerable groups. The evaluation of equity should consider both the technical and the ethical perspectives of the technological processes, such as:

- The inequality in the **accuracy rate and percentage of bias** is measured by quantifying false positives and false negatives and evaluating profiles of all ages, genders, and races.
- The **percentage of transparency and explainability** of models and processes, evaluating whether the FRT system is transparent and whether decision-making processes are explainable. Equitable technology should enable people to understand how decisions are made, how processes are implemented, and how their data are used.
- **Societal awareness index** to properly assess equity, it is necessary to involve all societal stakeholders, but it is indispensable to involve the most affected communities, such as marginalized and vulnerable groups and people of color.

5. ANALYSIS: OUTCOME MATRIX

	HUMAN-CENTRIC MODELS THAT PROMOTE PRIVACY BY DESIGN	*INDIVIDUAL CONSENT FORMS*
EFFECTIVENESS	**HIGH** 70 % of the developed FRT systems are founded on placing people at the center, which makes this approach more democratized in how models are trained, tested, and implemented in society.	**MEDIUM** 6/10 US cities have mechanisms in place for the provision of consent forms for collecting biometric data from users, resulting in an increase of 30% in the transparency of the models.
EFFICIENCY	**HIGH** the learning curve will be slower in the short term but will accelerate as more FRT models with privacy by design are developed, as experts will know how to train the new models, which are the best techniques, and how to embed them in the best way, increasing efficiency levels by 40% in the long-term.	**LOW** All five efficiency KPIs are experiencing a considerable improvement in the percentages. it should be noted that obtaining the consent of individuals can be a rather tiresome process, which can be lengthy and can lead to delays in the implementation of the technology.
EQUITY	**MEDIUM** This approach guarantees the principle of privacy, increasing fairness and non-discrimination by 35%. Ensuring privacy and personal data protection principles are paramount to establishing user trust, which can drive long-term growth and sustainability. However, there is still a long way to go before it becomes standard practice.	**MEDIUM** The forms promote individual autonomy and decision-making by authorizing or rejecting the use of individual data, resulting in a 25% increase in fairness, a 40% reduction in the possibility of bias, and a 35% increase in the protection of vulnerable groups.
RIGHTS PROTECTION	**HIGH** Building privacy protections directly into the design and operation of FRTs ensures the Fourth Amendment right to privacy. In addition, focusing on human-centered principles helps law enforcement continue to uphold the principles of the Fifth and Fourteenth Amendments, safeguarding due process and equal protection under the law.	**HIGH** By obtaining explicit consent from individuals before their biometric data is collected and processed, this practice aligns with the principles of the First and Fourth Amendments. It ensures that individuals maintain control over their personal information and prevents unauthorized intrusions into their privacy.

Leyend: Green = high; Yellow = medium; Red= low.

HUMAN-CENTRIC MODELS THAT PROMOTE PRIVACY BY DESIGN

The models prioritize fairness and privacy protection. Although they decrease discrimination by 35%, this approach may result in a 15% decrease in accuracy due to the reduction of available personal data. In addition, the proper development and implementation of these models requires additional investment in human training and acquisition of advanced software and hardware, which entails additional costs reaching $750,000.

Despite this initial challenge, in the long term, a 40% increase in efficiency is expected due to the growth in understanding and development of these models. In addition, it promotes equity by giving individuals greater control over their biometric data and protecting their rights – **Constitutional rights that are better protected by law enforcement bodies as they truly uphold the principles of the Fifth and Fourteenth Amendments, safeguarding due process and equal protection under the law when using FRT.**

INDIVIDUAL CONSENT FORMS

The forms empower Individuals by giving them the power and right to give explicit consent (by signing on paper or digitally) to disclose their data before the FRTs can use it. This alternative places humans at the center of the decision-making process, allowing greater control over their biometric data and promoting the protection of privacy, individual autonomy, and agency **protected by the First and Fourth Amendments.**

Implementing individual consent forms increases transparency and awareness about the use of FRTs, leading to a 25% increase in the democratization of the technology as it becomes better known and understood by a wider public. In addition, by collecting only the data allowed by consent, the investment in storage and processing is reduced by 7%, which also promotes greater efficiency in using existing resources.

However, the creation and collection processes can be tedious and lengthy, delaying the ethical adoption of technologies 18-24 months to ensure accessibility to all individuals, regardless of their level of education or technical knowledge, and inclusion by incorporating multiple languages and designing clear and concise forms.

6. RECOMMENDATIONS: ALTERNATIVE SELECTED

Considering that an effective and successful solution requires a long-term approach, opting for an alternative that establishes the solid foundations necessary for sustainable progress and lasting benefits from a technical, social, ethical, and legal is essential.

Therefore, the alternative that should be prioritized and supported is **THE HUMAN-CENTRIC MODELS THAT PROMOTE PRIVACY BY DESIGN,** as it looks to achieve an adequate balance between:

A.Technological innovation by increasing efficiency by 40% due to the growth in understanding and development of these models. In addition, it promotes equity by giving individuals greater control over their data, reducing misidentification and biases, and overseeing the protection of their rights.

B.Protecting the Due Process Clause, Equal Protection of the law, and civil rights and liberties by ensuring that the First, Fourth, Fifth, and Fourteenth Amendments are upheld throughout the FRT development and implementation process by:

- Safeguarding the fundamental rights of individuals by designing facial recognition systems that respect privacy and fairness from conception, integrating ethical and bias considerations from the outset of technology development, thereby ensuring that all individuals are treated fairly and without discrimination, regardless of their ethnicity, gender or other demographic characteristics, resulting in a fairer and more equitable process for individuals.

- Protecting people's identity and personal data strengthens due process by ensuring that any use of facial recognition technology is transparent and legally compliant. In addition, anonymizing and de-identifying facial data protects individuals' privacy and prevents unfair discrimination.

In summary, human-centric models that promote privacy by design are fundamental to:

- Maintaining the balance between technological and legal advances.
- Providing a framework with checks and balances.
- Setting a threshold with KPIs for developing and using FRT more ethically.
- Covering a gap that supports the advancements of future regulations.
- Offering the users an instrument that empowers them by making the algorithmic process more transparent and accessible.
- Guaranteeing the protection of Constitutional rights.
- Overseeing law enforcement administration practices when leveraging FRT.

7. REFERENCE LIST

[1] (2008). 740 ILCS 14/1 - Biometric Information Privacy Act. Illinois General Assembly. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[2] ACLU (2020). ACLU v. DHS: FOIA Lawsuit Seeking Information on Implementation of Face Surveillance at Airports. ACLU. https://www.aclu.org/cases/aclu-v-dhs-foia-lawsuit-seeking-information-implementation-face-surveillance-airports#:~:text=In%20March%202020%2C%20the%20ACLU,this%20technology%20in%20the%20future

[3] ACLU (2020). ACLU v. DHS: FOIA Lawsuit Seeking Information on Implementation of Face Surveillance at Airports. ACLU. https://www.aclu.org/cases/aclu-v-dhs-foia-lawsuit-seeking-information-implementation-face-surveillance-airports#:~:text=In%20March%202020%2C%20the%20ACLU,this%20technology%20in%20the%20future

[4] ACLU (2022, May 11). ACLU v. Clearview AIhttps://www.aclu.org/cases/aclu-v-clearview-ai

[5] ACLU v. Clearview AI, (2020, September 25). 2020CH04353 9337839. In The Circuit Court Of Cook County, Illinois County Department, Chancery Division. https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint

[6] AI and efficiency. (n.d.). https://openai.com/research/ai-and-efficiency

[7] Bales, A., & Fritsch, J. (2023). Market Guide for Data Masking. https://www.gartner.com/doc/reprints?id=1-2CKW1WNW&ct=230215&st=sb&utm_campaign=TY%20Mailers&utm_medium=email&_hsmi=231288347&_hsenc=p2ANqtz--7g0FRvcp1is5IIAGoStFUZdcQfqEOfp9ikAh_i1QYaCCgsc5GI8-vGFjENiz7T8GTxvhH2d561avKt43821tXvjIpug&utm_content=231288347&utm_source=hs_automation

[8] Bosse , M., & Mitchell, D. J. (2012, January 26). Digital Privacy: Supreme Court's landmark decision affects businesses large & small. Bernstein Shur Law Firm. 1]___

[9] Cision PR Newswire (2022, February 25). Facial Recognition Market Size Worth $12.67Bn, Globally, by 2028 at 14.2% CAGR - Exclusive Report by The Insight Partners. https://www.prnewswire.com/news-releases/facial-recognition-market-size-worth-12-67bn-globally-by-2028-at-14-2-cagr--exclusive-report-by-the-insight-partners-301489784.html

[10] Congress Gov. (2023). S.681 - 118th Congress (2023-2024): Facial recognition ... Congress Gov. https://www.congress.gov/bill/118th-congress/senate-bill/681

7. REFERENCE LIST

[11] Congress Gov. (2023, July 3). S.681 - Facial Recognition and Biometric Technology Moratorium Act of 2023 - S.681 — 118th Congress (2023-2024). Congress Gov. https://www.congress.gov/bill/118th-congress/senate-bill/681#:~:text=Introduced%20in%20Senate%20(03%2F07%2F2023)&text=This%20bill%20imposes%20limits%20on,state%2C%20and%20local%20government%20entities.

[12] Congress Gov. (2023, November 29). S.3361 - Traveler Privacy Protection Act of 2023 - 118th Congress (2023-2024). Congress Gov. https://www.congress.gov/bill/118th-congress/senate-bill/3361/text

[13] Congress. (n.d.). US Constitution - Fifth Amendment - Library of Congress. Congress. https://constitution.congress.gov/constitution/amendment-5/

[14] Congress. (n.d.). US Constitution - First Amendment - Library of Congress. Congress. https://constitution.congress.gov/constitution/amendment-1/

[15] Congress. (n.d.). US Constitution - Fourteenth Amendment - Library of Congress. Congress. https://constitution.congress.gov/constitution/amendment-14/

[16] Congress. (n.d.). US Constitution - Fourth Amendment - Library of Congress. Congress. https://constitution.congress.gov/constitution/amendment-4/

[17] Congressional Research Service. (2020, September 24). Congress. Congressional Research Service . https://crsreports.congress.gov/product/pdf/R/R46541 - "there is no overarching federal framework regulating the use of FRT"

[18] Fox, A. (2019). How can facial recognition be racially biased? The Hill. https://thehill.com/changing-america/respect/equality/475533-racial-bias-of-facial-recognition-systems-confirmed-in/

[19] Gullo, K. (2025). Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition.

[20] Harwell, D. (2019). Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. The Washington Post. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[21] Harwell, D. (2019, July 7). FBI and ICE find state driver's license photos are a gold mine for facial-recognition searches. The Washington Post. https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/

7. REFERENCE LIST

[22] Konfirmi (n.d.). Failures in Facial Recognition. https://konfirmi.com/blog/facial-recognition-ethical-issues/#:~:text=Racial%20Bias%20in%20Facial%20Recognition&text=One%20of%20the%20study's%20researchers,as%20compared%20to%20white%20Americans

[23] Lee Park, A. (2019) Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing. UCLA Law Review, [en línea] Disponible en: <https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/> [Consulta: 17 Oct 2020].

[24] Lively, T. K. (2021, December 1). Facial recognition in the US: Privacy concerns and legal developments. ASIS Homepage. https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/ - "Federal Legislation Lacking: Although Congress has yet to pass federal facial recognition regulation, […]"

[25] McKinsey & Company (2019) McKinsey & Co – Tackling bias in artificial intelligence (and in humans). [en línea] Disponible en: https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans. [Consulta: 21 Nov 2020].

[26] Members and Committees of Congress. (2020, September 24). Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations . Congressional Research Service . https://crsreports.congress.gov/product/pdf/R/R46541

[27] Model-Based Face De-Identification. (2006). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/1640608

[28] New Jersey v. Francisco Arteaga (June 7, 2023). A-3078-21. Superior Court Of New Jersey Appellate Division. https://www.njcourts.gov/system/files/court-opinions/2023/a3078-21.pdf

[29] New York Civil Liberties Union Foundation (2020). ACLU V. DHS — Face Recognition Surveillance Complain. United States District Court Southern District Of New York [Complaint For Injuctive Relief]. Aclu V. Dhs — Face Recognition Surveillance Complaint.

[30] PrivacyNet: Semi-Adversarial Networks for Multi-Attribute Face Privacy. (2020). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/9201364

[31] ProPublica Data Store (2020) COMPAS Recidivism Risk Score Data and Analysis. [en línea] Disponible en: https://www.propublica.org/datastore/dataset/compas-recidivism-risk-score-data-and-analysis. [Consulta: 18 Nov 2020].

[32] Ren, Z., Lee, Y. J., & Ryoo, M. S. (2018). Learning to Anonymize Faces for Privacy Preserving Action Detection. https://par.nsf.gov/servlets/purl/10100521

7. REFERENCE LIST

[33] Romine, C. H. (2020). Facial Recognition Technology (FRT). https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0#:~:text=NIST%20Interagency%20Report%208280%2C5,recognition%20algorithms%20that%20NIST%20evaluated.

[34] Rosebrock, A. (2021, 17 abril). Blur and anonymize faces with OpenCV and Python - PyImageSearch. PyImageSearch. https://pyimagesearch.com/2020/04/06/blur-and-anonymize-faces-with-opencv-and-python/

[35] Sakin, N. (2021, February 11). Will there be federal facial recognition regulation in the US? https://iapp.org/news/a/u-s-facial-recognition-roundup/ - "While there is no federal law in the U.S. to specifically regulate the burgeoning technology, numerous bills have been proposed."

[36] Sheppard Mullin Attorneys. (n.d.). Biometric Information Privacy Act (BIPA). Attorneys | Sheppard Mullin. https://www.sheppardmullin.com/biometric-information-privacy-act-bipa#:~:text=The%20Biometric%20Information%20Privacy%20Act,iris%20scans%2C%20and%20face%20prints.

[37] Smith, N., & Clark, T. (n.d.). A Framework to Model and Measure System Effectiveness. http://www.dodccrp.org/events/11th_ICCRTS/html/papers/054.pdf

[38] Targeted anonymization: a face image anonymization method for unauthorized models. (2022, 18 julio). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9859898

[39] The United States Government. (2023, February 16). Executive order on further advancing racial equity and support for underserved communities through the Federal Government. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/

[40] United States v. Jones: 565 US 400 (2012)

[41] US Department of Homeland Security (2019). Transportation Security Administration and US Customs and Border Protection: Deployment of Biometric Technologies [Report to Congress]. https://www.tsa.gov/sites/default/files/biometricsreport.pdf#page=11

[42] Wessler, N. F. (2020, February 5). We're Taking Clearview AI to Court to End its Privacy-Destroying Face Surveillance Activities. https://www.aclu.org/news/privacy-technology/were-taking-clearview-ai-to-court-to-end-its-privacy-destroying-face-surveillance-activities

[43] Witley, S., & Vittorio, A. (2023). Facial Recognition Software Is Everywhere, With Few Legal Limits. Bloomberg Law. https://news.bloomberglaw.com/privacy-and-data-security/facial-recognition-software-is-everywhere-with-few-legal-limits