p-ISSN: 2521-2982
e-ISSN: 2707-4587

GLOBAL Political REVIEW
www.gprjournal.com
empowering humanity

GPR

GLOBAL POLITICAL REVIEW

HEC-RECOGNIZED CATEGORY-Y

VOL. X, ISSUE III, SUMMER (SEPTEMBER-2025

DOI (Journal): 10.31703/gpr
DOI (Volume): 10.31703/gpr/.2025(X)
DOI (Issue): 10.31703/gpr.2025(X.III)

Double-blind Peer-review Research Journal
www.gprjournal.com

HumanityPublications
sharing research

Humanity Publications (HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Article Title

Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing

Abstract

Facial recognition technology (FRET) has completely transformed the manner of surveillance by introducing continuous and automatic identification of individuals in both digital and physical environments. This technological growth poses a challenge to the sufficiency of the Fourth Amendment, as its definition of reasonable expectation of privacy was designed in an analogue world of physical searches and physical evidence. This study proposes a technological proportionality and accountability framework (TPAF) that aims at balancing constitutional privacy rights with contemporary algorithm-based surveillance. Based on the principles of scale, persistence, and inference, TPAF provides a comprehensive mechanism that enables the courts and lawmakers to determine the proportionality, intent, and responsibility of digital surveillance operations. Recommending statutory and administrative changes in addition to transparency, fairness, and independent control, this article proposes that the Fourth Amendment should be interpreted dynamically in a way that conserves democratic values along with technological advancement in modern policing.

Keywords: Facial Recognition Technology, Fourth Amendment, Algorithmic Policing, Constitutional Privacy, Artificial Intelligence and Law, Surveillance and Civil Liberties, Technological Proportionality

Authors:

Bakht Munir: (Corresponding Author)
Postdoctoral Fellow, The University of Kansas School of Law, USA.
(Email: bakht.munir@ku.edu)

Ahmed Raza: LLM Scholar, Pennsylvania State University, USA.

Ali Nawaz Khan: Assistant Professor, University Law College, University of the Punjab, Lahore, Punjab, Pakistan.

Pages: 199-210
DOI:10.31703/gpr.2025(X-III).19
DOI link: https://dx.doi.org/10.31703/gpr.2025(X-III).19
Article link: https://gprjournal.com/article/facial-recognition-and-the-us-fourth-amendment-defining-reasonable-expectations-of-privacy-in-algorithmic-policing
Full-text Link: https://gprjournal.com/article/facial-recognition-and-the-us-fourth-amendment-defining-reasonable-expectations-of-privacy-in-algorithmic-policing
Pdf link: https://www.gprjournal.com/jadmin/Auther/31rvIolA2.pdf

Global Political Review
p-ISSN: 2521-2982 **e-ISSN:** 2707-4587
DOI (journal): 10.31703/gpr
Volume: X (2025)
DOI (volume): 10.31703/gpr.2025(X)
Issue: III Summer (September-2025)
DOI(Issue): 10.31703/gpr.2025(X-III)

Home Page
www.gprjournal.com

Volume: X (2025)
https://www.gprjournal.com/Current-issue

Issue: III-Summer (September-2025)
https://www.gprjournal.com/issue/10/3/2025

Scope
https://www.gprjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gpr/submissions

Google scholar

Visit Us

Humanity Publications (HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Citing this Article

19	Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing		
Authors	Bakht Munir Ahmed Raza Ali Nawaz Khan	DOI	10.31703/gpr.2025(X-III).19
		Pages	199-210
		Year	2025
		Volume	X
		Issue	III

Referencing & Citing Styles	
APA	Munir, B., Raza, A., & Khan, A. N. (2025). Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing. *Global Political Review*, *X*(III), 199-210. https://doi.org/10.31703/gpr.2025(X-III).19
CHICAGO	Munir, Bakht, Ahmed Raza, and Ali Nawaz Khan. 2025. "Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing." *Global Political Review* X (III):199-210. doi: 10.31703/gpr.2025(X-III).19.
HARVARD	MUNIR, B., RAZA, A. & KHAN, A. N. 2025. Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing. *Global Political Review,* X, 199-210.
MHRA	Munir, Bakht, Ahmed Raza, and Ali Nawaz Khan. 2025. 'Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing', *Global Political Review*, X: 199-210.
MLA	Munir, Bakht, Ahmed Raza, and Ali Nawaz Khan. "Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing." *Global Political Review* X.III (2025): 199-210. Print.
OXFORD	Munir, Bakht, Raza, Ahmed, and Khan, Ali Nawaz (2025), 'Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing', *Global Political Review,* X (III), 199-210.
TURABIAN	Munir, Bakht, Ahmed Raza, and Ali Nawaz Khan. "Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing." *Global Political Review* X, no. III (2025): 199-210. https://dx.doi.org/10.31703/gpr.2025(X-III).19.

Pages: 199-210 **e-ISSN:** 2707-4587 **p-ISSN:** 2521-2982 **Doi:** 10.31703/gpr.2025(X-III).19

Global Political Review
www.gprjournal.com
DOI: http://dx.doi.org/10.31703/gpr

Volume: X (2025) **URL:** https://doi.org/10.31703/gpr.2025(X-III).19 **Issue:** III-Summer (September-2025)

Title

Facial Recognition and the U.S. Fourth Amendment: Defining Reasonable Expectations of Privacy in Algorithmic Policing

Authors:

Bakht Munir: (Corresponding Author)
Postdoctoral Fellow, The University of Kansas School of Law, USA.
(Email: bakht.munir@ku.edu)
Ahmed Raza: LLM Scholar, Pennsylvania State University, USA.
Ali Nawaz Khan: Assistant Professor, University Law College, University of the Punjab, Lahore, Punjab, Pakistan.

Contents

Abstract

Facial recognition technology (FRET) has completely transformed the manner of surveillance by introducing continuous and automatic identification of individuals in both digital and physical environments. This technological growth poses a challenge to the sufficiency of the Fourth Amendment, as its definition of reasonable expectation of privacy was designed in an analogue world of physical searches and physical evidence. This study proposes a technological proportionality and accountability framework (TPAF) that aims at balancing constitutional privacy rights with contemporary algorithm-based surveillance. Based on the principles of scale, persistence, and inference, TPAF provides a comprehensive mechanism that enables the courts and lawmakers to determine the proportionality, intent, and responsibility of digital surveillance operations. Recommending statutory and administrative changes in addition to transparency, fairness, and independent control, this article proposes that the Fourth Amendment should be interpreted dynamically in a way that conserves democratic values along with technological advancement in modern policing.

Keywords:

Facial Recognition Technology, Fourth Amendment, Algorithmic Policing, Constitutional Privacy, Artificial Intelligence and Law, Surveillance and Civil Liberties, Technological Proportionality

Introduction

The architecture of surveillance has been revolutionized by artificial intelligence. One of the most radical forms of it is facial recognition technology (FRT), a system that converts human faces into measurable information, which can be identified and tracked retrospectively. What started as a convenience of biometrics turned into an instrument of state power. FRT is now being used by law enforcement agencies in the United States to scan live feeds, compare photographs with databases, and rebuild movement histories of millions of people. Such systems combine the predictive capabilities of machine learning with the preventive capabilities of the state to create

something of a surveillance that is omnipresent, predictive, and mostly undetectable (Phillips et al., 2018; Garvie, Bedoya, and Frankle, 2016).

The emergence of facial recognition has produced both operational excitement and constitutional fear. Proponents argue that it makes criminal investigations more efficient, more accurate, and helps to strengthen the safety of the citizens. However, its critics point to the fact that it can be used to engage in mass surveillance, racial discrimination, and the destruction of civil liberties. The Next Generation Identification (NGI) system of the FBI alone contains tens of millions of biometrics belonging to Americans, and the state and local agencies are increasingly outsourced to private firms like Clearview AI that scraped social media feeds of over 20 billion faces without permission (Hill, 2020). Such technology has advanced faster than the state in undertaking legal reform, and courts are left to understand constitutional protection, which is specifically planned for a pre-digital age.

The text of the Fourth Amendment, which provides protection against unreasonable searches of persons, houses, papers, and effects, was developed in a time when breaches of privacy had to be done through physical means. The digital revolution has made this framework ineffective. In contrast to the warrants that allow the search of homesteads or cars, the algorithmic surveillance is immaterial, is not intruded, is not notified, and has no limits. According to Andrew Ferguson (2017), the system of big data policing has broken the barrier of practicality that previously restricted the ability of states to observe. The key element in this new paradigm is that privacy is lost not by coercion but by inference, the process of linking together data points into the profile of behavior and identity.

This article places facial recognition at the point of intersection of constitutional law, technology, and ethics. It contends that the established Fourth Amendment jurisprudence, at least the reasonable expectation of privacy test of Katz v. United States (1967), does not fit the qualitative differences of algorithmic surveillance. FRT does not just see, but analyzes, predicts, and remembers. The constitutional value of its seeing is not its seeing itself but its size and continuance of seeing. Once the government has the need to locate anybody anywhere in any place all the time, privacy is no longer a social construct, and it is the privilege of technological restraint.

The article follows along four lines. First, it follows the history of the development of the privacy doctrine in the Fourth Amendment, in which courts have lagged behind in adapting to new technologies. Second, it analyzes its challenge to the principles upon which that doctrine was founded, especially its capability in aggregating, automating, and outsourcing surveillance. Third, it examines new judicial and legislative reactions to algorithmic policing. Lastly, it provides a normative solution, the Technological Proportionality and Accountability Framework (TPAF), which combines constitutional arguments with statutory reformation and administrative regulation.

The framework is a way of assessing digital searches, and so that reasonable under the Fourth Amendment is not fixed and static but is dynamic and principled.

Trespass to Technology: Exploring the Historical Foundations of the Fourth Amendment

The Fourth Amendment came about due to the opposition of the colonists to the general warrants and writs of assistance, which enabled British officers to search homes without the provision of a particular reason. It is based on the idea of limited government and entrenches a devotion to individualized suspicion and judicial review. But with the development of technologies, the spatially defined wording in the Amendment was getting harder and harder to enforce. The initial jurisprudence defined privacy as property; only bodily intrusion was a search. This opinion prevailed up to the middle of the twentieth century.

In Olmstead v. In the case of the United States (1928), the Supreme Court ruled that wiretapping did not infringe on the Fourth Amendment since no physical incursion was made. The majority opinion written by Chief Justice Taft followed a tangible-intrusion test on the rationale that intangible data voices carried over telephone lines were not persons, houses, papers, or effects. The dissent by Justice Brandeis, though, was the harbinger of an impending transformation to the Constitution. He cautioned that science was not to be halted with wiretapping on providing the government with spying tools, and instead, the Constitution had to

evolve to guard against the perniciousness of unregulated technological authority.

The opposition of Brandeis came true. By the 1960s, technology made the physical-intrusion test unnecessary. In Katz v. In the case of the United States (1967), the Court ruled that wiretapping of a public phone booth amounted to a search since it interfered with the reasonable expectation of privacy by Katz. The two-pronged test, which held that a subjective expectation was necessary and that an expectation that was named as reasonable by society was also required, was affirmed by Justice Harlan in his concurring opinion. This conceptual transformation in the Amendment is the change in viewing of property to privacy due to this doctrinal shift. But it also put forward an interpretive paradox: the expectations of privacy are not established. They change along with culture, technology, and law. The concept of surveillance becoming normalized can result in the contraction of what is considered reasonable by society, compromising constitutional protection (Solove, 2021).

Digital Explosion and the Mosaic Conversion

The shift to digital created both the elasticity and weakness of the reasonable-expectation standard. The jurisprudence of the Court was between the conservation and adaptation of technology. In United States v., the Court faced the issue of GPS tracking, and it decided that an extended surveillance of a car was a search (Jones, 2012). Though most of them depended on trespass, there was an opinion among people to concur on the temporal aspect of surveillance. The concurrence of Justice Sotomayor cautioned that endless surveillance exposes an abundance of information regarding family, political, professional, and religious affiliations.

This understanding of aggregation as a constitutional damage was fused in Carpenter v. United States (2018). The Court concluded that the Fourth Amendment was violated by obtaining historical cell-site location data without a warrant since such records give a close look into the life of a person. The opinion of Chief Justice Roberts redefined privacy in the terms of inference: the compilation of information, despite its publicity individually, will create a private mosaic. Orin Kerr (2018) called this the mosaic theory of the Fourth Amendment, according to which the surveillance system as a whole is more constitutional than the sum of its components.

The mosaic structure offers the doctrinal transitional point to facial recognition. Similar to cell-site data, FRT transforms discrete publicly observable behavior patterns into detailed behavior profiles. An image of one camera might be harmless, but with millions of automated images, combined, indexed, and cross-referenced, one can see what is moving, what is associated, and what is believed in. The constant process of facial recognition is thus not a search due to the fact that it does not entail the capturing of a face, but the creation of an identity map. This argument concurs with the fact that privacy is relative, accumulative, and technologically restrictive as realized by Carpenter.

The Constitutional Inadequacy of the Current Doctrines

In spite of such evolutions, there are a number of doctrines that still undermine Fourth Amendment in the face of algorithmic surveillance. The former is the public-exposure doctrine, which was based on Smith v. Maryland (1979) and United States v. The argument that people should not expect a reasonable level of privacy in information that is disclosed to the public, which is observed in Knots (1983). The second is the third-party doctrine, which does not provide the constitutional protection of information that is provided voluntarily to third parties. These principles give the state the chance to capitalize on omnipresent visibility and privatized data gathering in relation to FRT without any judicial review.

Neil Richards and Jonathan King (2013) state that these doctrines are not well adapted to the digital era since they mix visibility with accessibility. The status of being visible to others is not the same as an algorithmic analysis that is unending. In an environment filled with surveillance cameras, there is no longer any implication of consent to constant identification with the presence of people. Likewise, the third-party doctrine does not consider the coercive character of the current data sharing. The people have no way of consenting to facial capture in areas surveilled by the state and the private sector. In cases where the involvement in public life is

accompanied by regular exposure to biometrics, the voluntariness turns into fiction.

Ryan Calo (2017) has suggested that privacy harms not only result from the gathering of information but also from the perceived surveillance. Human beings alter their behavior when they suspect that they are being observed. This chilling is wider than privacy to include both expressive and associative freedoms guaranteed by the First Amendment. Constant identifiability makes political participation and protest mobile, which in turn causes a feedback cycle of self-censorship (Selinger & Hartzog 2020). The constitutional principles of face recognition are thus way beyond the issue of privacy; they involve autonomy, dignity, and democratic engagement.

Algorithmic Policing, Due Process and the Constitutional Solution:

Algorithmic Policing and the Growth of State Power

Facial recognition is not an autonomous technology; it is the engine of analysis of a wider policing environment called algorithmic policing. Police nowadays combine biometric information with predictive analytics to place probabilistic risk scores on any person or neighborhood (Lum and Isaac, 2016; Munir, 2024). The consequent merging of the outputs of FRT, social-media metadata, and traces of geolocation turns the classic role of investigation into the role of anticipation.

According to Andrew Ferguson (2017), Big Data policing changes the relationship between the individual and the state as it introduces the locus of suspicion onto probability. This predictive disposition, despite its apparent efficiency, is disturbing two constitutional pillars, the individualized suspicion pre-requisite and the warrant's particularity. As the state activities are based on algorithmic forecasting as opposed to human observation, it makes the distinction between prevention and pre-emption indistinct. It is not merely a confusion of the identities, but a silent normalization of the pre-crime government, which is a system of control that cannot coexist with the Fourth Amendment mistrust of the use of general warrants.

The Crisis of Evidentiality: Openness and Competitiveness

The utilization of machine-learning tools creates an evidentiary dilemma at the essence of criminal procedure. Most of the time, defendants who are arrested or convicted using FRT matches have been unable to access the algorithms to question their own reliability. Proprietary software falls under trade-secret protection, putting the defendants in an epistemic blind place. Danielle Citron and Frank Pasquale (2014) define this non-transparency as the failure of algorithmic due process and believe that contests with fairness demand that the evidence produced by algorithms be contestable, i.e. they must be contestable.

Viable impacts in the Real-world have already been seen. Clare Garvie (2020) lists numerous false arrests in Detroit and New Jersey, where wrong recognition by facial-recognition software resulted in illegal detention. In both instances, the courts originally regarded algorithmic matches as final and not as probable, which was against the evidentiary requirements expressed in Daubert v. Merrell Dow Pharmaceuticals (1993). When probabilistic code replaces the use of a sworn testimony, the right to be put before witnesses against him (U.S. Const. amend. VI) becomes hollow. In this way, the problem of algorithmic surveillance concerns not only the Fourth but also the Sixth Amendment and serves as an example of the interdependence of procedural fairness and the transparency of information.

The Crisis of Constitution & Privatization

Excessive contracting of state functions to the services of data brokers is a hallmark of twenty-first-century surveillance. Clearview AI, Palantir, and Vigilant Solutions are some of the companies that generate enormous amounts of biometric or behavioral data that is sold or accessed by police departments through subscriptions. The benefit of this privatization is that it enables governments to circumvent constitutional constraints, a phenomenon that scholars call constitutional laundering (Richards & Hartzog, 2019). Since the information originates in the individual's hands, Court usually considers the retrieval of government beyond the scope of Fourth Amendment under the doctrine of third-party role.

The outcome is an accountability gap: the state enjoys the advantages of privatized surveillance without having to assume any constitutional responsibilities. Including government use of

privately obtained biometric information under Fourth Amendment protection would recover the idea that it is the consequences of the state action that are subject to the Constitution, and not just its shape. The jurisprudence of state action should then change to include the cases in which private agents play the role of functional agents of the state (Ferguson, 2023).

Judicial Indications of a Doctrinal Change

The federal and state courts are starting to recognize the uniqueness of technological surveillance in the Constitution. Leaders of a Beautiful Struggle v. The Fourth Circuit, 2021 which invalidated an aerial-imaging program allowing 24-hour surveillance of the entire city, decided that the Baltimore Police Department's plan to use so-called encyclopedic surveillance is not congruent with Carpenter. The reasoning of this opinion can be used directly in the case of FRT: by the ability to survey someone and provide a detailed re-creation of the movements of the individual, this amounts to a search, despite this act was done in the street.

In the case of Lynch (2021), the algorithmic-match data had to be disclosed to meet the due-process rights, and the integration of human testimony in the case could not be substituted by the black-box evidence without visibility. In such rulings, Andrew Ferguson (2023) writes of such rulings as having identified the machine testimony, requiring the algorithmic systems to pass the evidentiary test of reliability that is just as high as that of a human witness. These cases taken together suggest a technological-proportionality approach-the one that employs constitutional scrutiny to the strength and endurance of the tool of surveillance.

Public Anonymity

Traditional jurisprudence supposes that information that is in the sight of everyone in the world is said to be without any promise of privacy, Maryland (1979). However, in a time of ubiquitous cameras, this assumption breaks down. Introducing visibility does not mean accessibility, as Richards and King (2013) describe: what a casual observer may glimpse, an algorithm can remember, catalog, and recall forever. FRT eliminates the anonymity that used to shield citizens against constant scrutiny and reduces the presence of public in the streets to a data occurrence.

There are systemic social impacts of this breakdown of anonymity. Evan Selinger and Woodrow Hartzog (2020) show that the understanding of unremitting identification inhibits protest activity and religion. The Fourth and First Amendments are thus connected in the resulting chilling effect, where the loss of privacy translates to the loss of expressive freedom. This interdependence must be judicially acknowledged; constitutional analysis of privacy must view privacy as not a stand-alone right but as the structural requirement of democratic action.

Moving towards a Technological-Proportionality Framework

These shortcomings are mitigated by this article by proposing the Technological Proportionality and Accountability Framework (TPAF), an institutional and doctrinal framework that attempts to adapt the reasonableness standard of the Fourth Amendment into an age of artificial intelligence. The framework is based on three mutually supportive pillars of analysis that include scale, persistence, and inference. Scale is the extent of surveillance, which acknowledges that when government surveillance is no longer applied to the specific individuals being investigated, but to the entire population, it starts to look like a general warrant and should be presumed as being constitutionally unreasonable. An example of how surveillance is supposed to be subjected to strict scrutiny is the application of city-wide facial recognition grids and mass biometric monitoring systems. Persistence is grounded in length and permanence; a continuous or retrospective watch that can enable to recreate the travels or routine of a man throughout a time span should be preceded by judicial consent, with the same rationale as upheld in Carpenter v. United States (2018). Inference considers the sophistication level of the technology, and it is important to note that systems that can produce predictions of behaviors, Evaluation of probabilistic risks, or personality analysis, that is, beyond identification, represent a qualitatively different type of search since systems that do so retrieve meaning instead of mere data points. When these three dimensions coincide under TPAF there exists a constitutional presumption of unreasonableness unless backed by

a narrowly focused warrant based on probable cause. By doing that, the framework will convert imprecise ethical calls to be reasonable to a principled inquiry, technology-conscious and flexible to the new innovations without altering the constitutional relationship between freedom and law enforcement.

Legislative Implementation

Even judicial doctrine will not guarantee constitutional sufficiency in the era of algorithmic surveillance; therefore, a Federal Biometric Privacy and Accountability Act need to be enacted by Congress to establish proportionality in the form of explicit procedural and substantive protections. The first step in such legislation is a requirement of a warrant to use persistent facial recognition, which requires any use beyond a short period of identification to be pre-approved by the court, with the specific boundaries, duration, and scope of the search being spelled out in the warrants. It is also supposed to initiate compulsory bias and accuracy audits, to be conducted by the National Institute of Standards and Technology (NIST, 2019). Face Recognition Vendor Test (2019) should be supervised to make sure that agencies regularly conduct independent audits with the capacity to identify disparities in algorithm performance on the basis of race, gender, or age. Also, the Act should introduce algorithmic-transparency reports, which require vendors providing FRT systems to government agencies to publish adequate technical documentation to permit adversarial testing, which meets Daubert evidentiary standards. To enhance accountability, the law ought to establish civil penalties and a compensation system, which can allow individuals who have suffered unlawfully or illegally authorized facial recognition to demand damages and the prevention of contaminated evidence use in court. Lastly, it must also create an autonomous oversight board, following the example of the Privacy and Civil Liberties Oversight Board (PCLOB), to audit surveillance programs and issue annual transparency reports, as well as advise Congress on the new biometric technologies. Taken together, these provisions would make the Technological Proportionality and Accountability Framework (TPAF) a standard element of the law and ex ante protection and remedies of a global best-practice privacy regulation, without wholesale importation of foreign legal frameworks.

Administrative and Ethical Oversight

In addition to reforms enacted by law, ethical governance should be institutionalized by the administrative agencies. Adding to the five concepts presented by Floridi and Cowls (2021): beneficence, non-maleficence, autonomy, justice, and explicability, internal AI-ethics codes should be applied to all technology procurements by the federal and state departments. Abstract ethics can be brought into enforceable accountability through transparency reports, community-consultation process, and routine algorithmic-impact assessment.

This administrative aspect is supported by the public-trust theory. Tom Tyler (2019) demonstrates that compliance with the law is not maintained by coercion but perceived fairness. Surveillance should not appear prohibited or discriminatory to citizens, as this will undermine effectiveness. Placing TPAF in the workings of the agencies thus not only helps to limit abuse, but also to maintain institutional credibility.

Learning lessons from comparative perspective

Even though the United States is practicing a separate constitutional tradition, comparative insight can still help. The General Data Protection Regulation (GDPR) of the European Union and the proposed Artificial Intelligence Act (European Commission, 2023) use ex ante proportionality in biometric processing, which is ultimately banned unless it is proved necessary and proportionate towards a legitimate end (Irfan, et. al., 2024). This precautionary reason may educate the American reform without copying the European bureaucracy. The U.S. courts may succeed in similar outcomes by introducing the analysis of proportionality into the appraisal of warrants, instead of supranational regulation.

This is exactly the synthesis that is promoted by Schulhofer and Stevenson (2022), the combination of reactive remedies of the Fourth Amendment and preventive measures based on administrative law. TPAF reflects that strategy: it does not ignore American constitutionalism, but, on the contrary, it considers international norms of accountability.

Revisiting the Constitutional Framework

What is more significant in the contribution of TPAF is the redefining of reasonableness as a dynamic balance between technological potential and human dignity. The framers of the Amendment did not anticipate machine learning, but their driving force behind the document, insourcing against unchecked authority, will never change. The definition of a search has to be broadened accordingly when the instruments of search become autonomous. Elevating technological amplification to the constitutional variable status, courts will be able to maintain the good faith to the purpose of the Amendment without becoming victims of formalism.

This convenient philosophy is reminiscent of the "Olmstead dissent by Justice Brandeis": The rights guaranteed by the Constitution should not be undermined by the advancement of science. It is now high time to make that warning institutional. Constitutional privacy, as a result of proportionality, transparency, and accountability, can change its focus on protection of physical spaces into protection of informational selves. It is only at that point that the Fourth Amendment will be a breathing document of freedom and not a product of the analogue era.

Operationalizing Technological Proportionality: A Dive from Doctrine to Democratic Governance:

Reconsideration of Reasonableness as a part of the Constitutional Approach

The persistent dilemma facing the Fourth Amendment is how to bring an eighteenth-century document into agreement with twenty-first-century technology. It provided no rule but a flexible rule of proportional restraint in its main idea, reasonableness. Reasonableness in their world involved the restriction of armed invasion of physical space; in ours, it would have to involve the restriction of digital omniscience. The same reasoning that necessitated a warrant by a magistrate before they could enter a home also needs to be applied to the state, so that it can be required to obtain judicial permission before the state can intrude on its informational analogue: the biometric and behavioral information that allows a person to constitute a digital self.

This revision is not a renunciation of the original meaning, but its expansion. The proportionality today calls on the courts to balance the severity of technological surveillance against its utility to the safety of the citizens. In this regard, the history of the Fourth Amendment since Olmstead up to Katz, Jones, and Carpenter is a progressive shift between the material intrusion and the exposure of information. The common thread in each of these decisions was that it was not just the discrete intrusion that was harmful, but totalization, that is; the ability to create an intimate mosaic of life.

The Judicial Path Forward: A systematic trial of technological Searches

To escape the doctrinal uncertainty, the application of the TPAF by the courts must be sequential, with four steps of analysis in consideration of the algorithmic surveillance.

Technological Amplification

The initial question involves the extension of state perception beyond the normal human being by the technology. Thermal imaging in Kyllo v. United States (2001) already indicated that the augmentation of the sense of the human being attracts the constitutional examination. A thousand face identifications in seconds increase the perception exponentially with facial recognition. The fourth amendment should be applied once a tool can be used to conduct surveillance which is otherwise impossible or impractical.

Test Scale, Perseverance, and Inference

Then the judges assess the three-factor matrix as stated in Part II. Scale is used to determine the breadth of the population of the information to be captured by the measurement; persistence determines the continuity over time; and inference is used to determine the depth of the analysis. Where surveillance is general, omni static, and prospective, it cannot be assumed reasonable without an individualized suspicion. This converts privacy harms in form of abstract policy to concrete constitutional standards.

Judicial Intention

Although surveillance may have a valid purpose, judges need to pose the question of whether there

are alternatives that are less invasive. Reasonableness, which is based on proportionality analysis in constitutional law (Schulhofer and Stevenson, 2022), requires that the power of the state be the less restrictive to fulfill its purpose. An example would be the case where a facial-recognition network of the city is constitutionally excessive should it be necessary to verify every face manually or a specific warrant be targeted.

The Demand of Accountability Mechanisms

Approval must be based on evidence of protective measures: algorithmic audit logs, tests of demographic bias, retention constraints, and reporting obligations to the public (Munir, et. al., 2025). Failure to do so would make any evidence inadmissible, similar to physical search exclusionary rules. Responsibility therefore turns out to be a constitutional condition and not a policy choice.

This way of operationalizing reasonableness in these steps enables the courts to leave the old dichotomy of search and no search and to perceive surveillance as a continuum of technological intensity. This model fosters national coherence which will reduce the existing division of jurisdictions as to FRT admissibility and evidentiary standards.

Aligning Tech Legislation with Constitution Principles

The privacy cannot be maintained only through judicial interpretation in the times of rapid innovation; the Congress should codify the proportionality in the positive law. The three levels of protection ought to be institutionalized by a holistic Federal Biometric Privacy and Accountability Act (FBPAA).

Procedural Safeguards

Any persistent or predictive systems of biometrics must demand judicial warrants to define the scope of the target, duration of time of their relevance, and the data-storage boundaries. Franks v.--notice provisions. Disclosures of Delaware (1978)- must disclose to individuals after investigation where possible and non-probe information must be destroyed by adjudication.

Substantive Safeguards

Statute must prohibit persistent, live FRT surveillance of groups of people except in exigencies which are narrowly or strictly defined: terrorism threats or Amber Alerts, certified by a court. These rules allow the flexibility of the emergency without normalizing dragnet surveillance.

Institutional Safeguards

The Congress is to create a National Algorithmic Accountability Office (NAAO) with the mandate to audit the federal and state biometric systems, release bias reports on an annual basis, and communicate with the Privacy and Civil Liberties Oversight Board. This organ would act as administrative custodian of TPAF and make sure that there are continual assessment and not sporadic investigation.

Collectively, the provisions would bring the reasoning of the 1974 Privacy Act and the 1986 Electronic Communications Privacy Act into the biometric age. The constitutional entrenching of values makes the expectations more stable and translates the judicial philosophy into governance that is binding.

Innovation and Federalism

Since the authority of policing is not centralized between states and municipalities, federalism does not act as a hindrance but as an asset to constitutional adaptation. The Biometric Information Privacy Act (BIPA) of Illinois illustrates the possibility of state experimentation as a national norm-setter, offering a right of action on privacy and massive statutory damages in the violation of an unauthorized use of biometric data. Transparency or consent statutes have been passed in other states, such as Washington, Maine, and California, as a result of bi-partisan acceptance of privacy being a structural value shared by all, not a value of partisan.

A federal law must therefore offer minimum protection without taking away state latitude in taking it a step further. This can be compared to environmental law in the sense that federal minimums exist alongside standards that are more stringent in the state level. In addition, civic constitutionalism is implemented in the local ordinances that prohibit or limit FRT, including San Francisco, Boston, and Portland. These ordinances satisfy Madison, who wrote the dictum that only the people themselves are the proper source of power by enabling them to discuss the policy of surveillance.

Incorporation of TPAF principles in municipal decision-making will make constitutional renewal participatory and not judicial.

Algorithms and Administrative Law

The bridging matter between the ideals of constitution and the practice is administrative oversight. Algorithms should not be an exception since the Administrative Procedure Act (APA) already stipulates that agencies must take reasonable decisions. To expand APA review on FRT deployments, agencies would need to defend their actions using empirical evidence that would prove their accuracy, necessity, and fairness.

As a way of operationalizing this obligation, it should make agencies develop Algorithmic Impact Statements (AIS) similar to Environmental Impact Statements in the National Environmental Policy Act. Each AIS would fully explain the algorithmic system and the purpose of such a system, including how information is processed, what outputs are produced, and how data are communicated with the infrastructure of the current administrative or law-enforcement systems. It would also determine the possible constitutional, civil-rights, and equity ramifications of the system to determine any foreseeable threats to privacy, due process, or equal protection. Moreover, the AIS would also contain quantitative bias measures obtained through independent testing in order to have accuracy differences between the demographic groups, which would guarantee empirical transparency. Lastly, it would describe formal mitigation measures and sunset provisions, including how the detected harms will be dealt with, the period during which the system will be allowed to use it and under what circumstances the system will be re-assessed or cancelled. In such a way, the AIS would introduce constitutional proportionality and accountability into the life cycle of algorithmic governance directly into the administrative sphere.

Reviewing AIS filings by judicial authorities would put in place a form of iterative consultation between courts and agencies, putting proportionality in the administrative state. This would create an over time record of common-law technological reasonableness, increasing the predictability of both the regulators and the innovators.

The Civic Oversight and the Ethical Integration

Legitimacy cannot be achieved by simply being legal, but must be achieved through the ability of the surveillance to meet the ethical accountability. As a continuation of Floridi and Cowls (2021), there are five normative principles, including beneficence, non-maleficence, autonomy, justice, and explicability, which should be internalized by agencies and private vendors. It can be implemented by contractual requirements of open-model documentation, third-parties ethics audits, and community advisory board bodies which are enabled to annually review deployments. Public Transparency is a democratic protection measure. When the citizens know the purpose and the methods of surveillance, they will be able to exercise informed oversight. This reconsiders a new definition of consent, not the illusionary acceptance of information policies but active discussion of technological authority. Any surveillance regime is thus based on the legitimacy of reciprocity, the state is allowed to watch, but must be watchable.

In order to make this reciprocity operational, agencies might have real-time public registries of accepted FRT systems, with purpose, duration, and data-retention schedules specified. External auditing that occurred in a continuous manner could then be done by civil-society organizations and the journalists which would maintain transparency that would be maintained by plural accountability.

Resolution of the concerns of Security and Liberty

Those who are against stricter restrictions on privacy frequently put the discussion in terms of a kind of zero-sum game between security and freedom. This dichotomy is opposed by history. The excesses of the post-9/11 surveillance as outlined in the USA PATRIOT Act and later revelations by Edward Snowden proved that secrecy only undermines rights and the trust of the people to the point of hampering their cooperation with law enforcement.

The relevance of proportionality in a framework enhances instead of diminishing valid security work by defining boundaries and reliability of evidence.

Procedural fairness of police is empirically verified by Tyler (2019), who stated that communities with perceived procedural fairness have an increased compliance and reduced crime. The integrating of the TPAF standards, which include judicial warrants, transparency, and audit, converts the constitutional principle to practical value. By doing this, protection of privacy and policing success are mutually enhancing and not mutually exclusive.

Professional Culture, Education, and Training

Proportionality will be implemented at the end according to the professionals enforcing it. Technological-literacy curricula on algorithmic bias, data provenance and statistical inference need to be introduced into police-academies, prosecutor-offices, and judicial-education-institutes. Knowing how FRT works has become a necessity in the execution of the Constitution as much as the knowledge of probable cause.

The model policies reflecting the TPAF principles, including the necessity to document the algorithmic decisions, verify the work of the vendor system, and reveal the error rates, can be promulgated by professional bodies such as the International Association of Chiefs of Police and the American Judges Association. Continuing-legal-education programs are to be used to train attorneys to be able to litigate cases of algorithmic-evidence in a competent case that grants adversarial balance.

Making education an institution makes proportionality a matter of doctrine rather than an ethic of the profession. In the long term, the change in culture of the justice system can shift it away toward an active prevention, rather than a reactive correction of the violation of rights, instilling the constitutional mindfulness into the daily decision-making process.

The Broader Constitutional Significance

Facial recognition surveillance is not just a technological breakthrough; it is a constitutional point of inflection. It is a test that the United States is capable of reinterpreting the guarantees upon which it is based without undermining it. The Fourth Amendment has endured revolutions in transportation, communication and computation, since the reason behind its existence, the restriction on state power, has always been the same. The further phase of that development requires the acknowledgment of the informational privacy as a part of the personal security.

As Shoshana Zuboff (2019) cautions, surveillance capitalism is potentially endangering the privacy of the freedom that the Constitution was meant to guarantee. The public constitutional authority through TPAF restores the sovereignty of the democratic organizations to handle data. The framework thereby carries the promise of the fourth amendment concerning physical protection to the issue of digital self-determination, ensuring innovation provides service to citizenship and not oppression.

Conclusion

The strife between effectiveness and freedom that characterizes contemporary rule is captured through facial recognition technology. Its accuracy and scope provoke policymakers to lose constitutional interpretation in favor of administrative ease. But it is the genius of the Fourth Amendment that it is not a limitations document but a flexibility document because it does not locked the past but rather translates principle into new circumstances.

The proposed Technological Proportionality and Accountability Framework can provide a practical way out. It turns abstract reasonableness into quantifiable constitutional standards by assessing surveillance in terms of scale, persistence, and inference. It can help to regain transparency, contestability, and instill trust once again in the population, along with reforms in legislation and administration.

The problem of the algorithmic age is that convenience has become the mutation of control. The work of the Constitution, as Justice Brandeis anticipated it is to secure the right to be left alone, the broadest right which can be conceived, and the one which is necessary for the progress of nations. Vigilance, proportionality, and accountability are needed to preserve that right in a world dominated by intelligent machines. By these principles, it is once again possible to have the Fourth Amendment become the 'Living sheild' between the ruled and the ruling eye.

References

Citron, D. K., & Pasquale, F. A. (2014). The scored society: Due process for automated predictions. *Washington Law Review, 89*(1), 1–33. https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2
Google Scholar Worldcat Fulltext

European Commission. (2023). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM (2021) 206 final.* https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence
Google Scholar Worldcat Fulltext

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement.* New York: NYU Press. https://nyupress.org/9781479892822
Google Scholar Worldcat Fulltext

Ferguson, A. G. (2023). Machine testimony and the Fourth Amendment. *Georgetown Law Journal, 111*(5), 1211–1262.
Google Scholar Worldcat Fulltext

Floridi, L., & Cowls, J. (2021). A unified framework of five principles for AI in society. *Harvard Data Science Review, 3*(1). https://doi.org/10.1162/99608f92.8cd550d1
Google Scholar Worldcat Fulltext

Garvie, C. (2020). *Garbage in, garbage out: Face recognition on flawed data.* Washington, DC: Georgetown Law Center on Privacy & Technology. https://www.flawedfacedata.com
Google Scholar Worldcat Fulltext

Garvie, C., Bedoya, A., & Frankle, J. (2016). *The perpetual line-up: Unregulated police face recognition in America.* Washington, DC: Georgetown University. https://www.perpetuallineup.org
Google Scholar Worldcat Fulltext

Hill, K. (2020, January 18). The secretive company that might end privacy as we know it. *The New York Times.* https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
Google Scholar Worldcat Fulltext

Irfan, M., Yasin, A., Hussain, R. A., Bashir, N., & Munir, B. (2024). Artificial intelligence, data protection and transparency: A comparative study of GDPR and CCPA. *Journal of Media Horizons, 5*(3), 76–85.
Google Scholar Worldcat Fulltext

Katz v. United States, 389 U.S. 347 (1967).
Google Scholar Worldcat Fulltext

Kerr, O. S. (2018). Implementing *Carpenter*. *Harvard Law Review Forum, 132*, 23–42. https://harvardlawreview.org/forum/vol-132/implementing-carpenter/
Google Scholar Worldcat Fulltext

Leaders of a Beautiful Struggle v. Baltimore Police Department, 979 F.3d 219 (4th Cir. 2021).
Google Scholar Worldcat Fulltext

Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x
Google Scholar Worldcat Fulltext

Munir, B. (2024). *Artificial intelligence and legal decision-making in the USA and Pakistan: A critical appreciation of regulatory frameworks.* SSRN. https://ssrn.com/abstract=4999590
Google Scholar Worldcat Fulltext

Munir, B., Khalid, S., & Noreen, U. (2025). Exposing Islamophobia in machine learning: A critical analysis of the existing theories and biases. *Center for Management Science Research, 3*(3), 1–9.
Google Scholar Worldcat Fulltext

National Institute of Standards and Technology (NIST). (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic effects.* Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8280
Google Scholar Worldcat Fulltext

Phillips, P. J., Jiang, F., Narvekar, A., Ayyad, J., & O'Toole, A. (2018). Face recognition accuracy of forensic examiners, super-recognisers, and algorithms. *Proceedings of the National Academy of Sciences, 115*(24), 6171–6176. https://doi.org/10.1073/pnas.1721355115
Google Scholar Worldcat Fulltext

Richards, N. M., & Hartzog, W. (2019). A duty of loyalty for privacy law. *Duke Law Journal, 69*(3), 881–948.
Google Scholar Worldcat Fulltext

Richards, N. M., & King, J. H. (2013). Three paradoxes of big data. *Stanford Law Review Online, 66*, 41–46. https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/
Google Scholar Worldcat Fulltext

Schulhofer, S. J., & Stevenson, M. T. (2022). Reconsidering the Fourth Amendment's remedies in the age of surveillance. *Columbia Journal of Law & Social Problems,* 55(4), 445–489.
Google Scholar Worldcat Fulltext

Selinger, E., & Hartzog, W. (2020, June 12). Surveillance and the chilling effect. *The Atlantic.* https://www.theatlantic.com/technology/archive/2020/06/surveillance-protests/613024/
Google Scholar Worldcat Fulltext

Smith v. Maryland, 442 U.S. 735 (1979).
Google Scholar Worldcat Fulltext

Tyler, T. R. (2019). Trust and legitimacy in policing. *Annual Review of Criminology, 2*, 453–472. https://doi.org/10.1146/annurev-criminol-011518-024638
Google Scholar Worldcat Fulltext

United States v. Jones, 565 U.S. 400 (2012).
Google Scholar Worldcat Fulltext

Zuboff, S. (2019). *The age of surveillance capitalism.* New York: PublicAffairs. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395700/
Google Scholar Worldcat Fulltext