

# A Patchwork Full of Holes: Facial Recognition Legislation in the United States\*

Anonymous Author

---

**ABSTRACT** This article explores the growing use of facial recognition technology by U.S. law enforcement in the absence of a coherent federal framework. It reviews federal initiatives, state and local legislation, and recent case law, highlighting constitutional issues concerning privacy, anonymity, due process and equal protection. It concludes by calling for comprehensive, technology-neutral privacy legislation to protect fundamental rights.

---

**KEYWORDS:** Facial Recognition Technology - U.S. Privacy Law - Constitutional Rights - Criminal Justice

---

**TABLE OF CONTENTS:** 1. Introduction: The U.S. facial recognition landscape, in numbers. – 2. Part I: Federal legislative efforts and the constitutional floor. – 2.1. Free speech and the right to anonymity. – 2.2. The right to privacy. – 2.3. The right to a fair trial. – 2.4. Equal protection under the laws. – 3. Part II: State and local legislative approaches. – 3.1. Bans. – 3.2. Moratoria. – 3.3. Regulation. – 4. Part III: Facial recognition in criminal courts. – 4.1. *Lynch v. Florida*. – 4.2. *New Jersey v. Arteaga*. – 5. Conclusion: Flipping the script.

---

## 1. Introduction: The U.S. facial recognition landscape, in numbers

In 2001, the sheriff's office in Pinellas County, Florida deployed the first facial recognition system in the United States, purchased using a grant from the Department of Defense Irregular Warfare Support Program.<sup>1</sup> Since then, police use of the technology has expanded exponentially. By 2016, more than a quarter of the 18,000 law enforcement agencies in the United States had access to a facial recognition system.<sup>2</sup> In 2020, at least twenty federal agencies used facial recognition in law enforcement activities, with many reporting plans to expand their use in the future.<sup>3</sup> By 2023, just

one company, Clearview AI, reported that its 3,100 U.S. law enforcement clients had searched its database - 40 billion images scraped from the Internet - almost one million times.<sup>4</sup>

Facial recognition is now a routine part of U.S. criminal investigations, and while the exact number of resulting arrests, charges, plea deals, and convictions is unknown, it is likely in the order of hundreds of thousands.<sup>5</sup> Yet despite this widespread and everyday use, today - more than twenty years after the first system went live - the U.S. legal framework for the technology remains in its infancy. No federal law explicitly governs the space, and while state and local legislatures in some jurisdictions have stepped in to fill this gap, most of the country remains with little to no legislative framework.

---

\* Article submitted to double-blind peer review.

The author of this contribution has chosen to remain anonymous for institutional reasons. The editors nevertheless wish to express their sincere gratitude for the author's expertise and the time devoted to sharing it.

<sup>1</sup> Pinellas County Sheriff's Office, Florida's Facial Recognition Network presentation, 26 March 2014, 5 available at: [www.nacdl.org/getattachment/d215b76f-0de0-4209-99ac-55e10d2582cc/1125\\_jowell\\_connectid-2014-fr-presentation.pdf](http://www.nacdl.org/getattachment/d215b76f-0de0-4209-99ac-55e10d2582cc/1125_jowell_connectid-2014-fr-presentation.pdf); Interview with Sheriff Bob Gualtieri and Technical Support Specialist Jake Roberto, 26 July 2016 (notes on file with author).

<sup>2</sup> C. Garvie, A. Bedoya and J. Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Center on Privacy & Technology at Georgetown Law, n. 25, 16 October 2016, [www.perpetuallineup.org](http://www.perpetuallineup.org).

<sup>3</sup> U.S. Gov't Accountability Office, GAO-21-518, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, 9 June 2021, [www.gao.gov/assets/gao-21-518.pdf](http://www.gao.gov/assets/gao-21-518.pdf).

---

<sup>4</sup> W. Knight, *Clearview AI Has New Tools to Identify You in Photos*, in *Wired*, 4 October 2021, [www.wired.com/story/clearview-ai-new-tools-identify-you-photos](http://www.wired.com/story/clearview-ai-new-tools-identify-you-photos); see C. Burt, *Clearview AI tops 40 billion reference images in facial recognition database*, in *Biometric Update*, 24 November 2024, [www.biometricupdate.com/202311/clearview-ai-tops-40-billion-reference-images-in-facial-recognition-databases](http://www.biometricupdate.com/202311/clearview-ai-tops-40-billion-reference-images-in-facial-recognition-databases); see J. Clayton and B. Derico, *Clearview AI used nearly 1m times by US police*, it tells the BBC, BBC, 27 March 2023, [www.bbc.com/news/technology-65057011](http://www.bbc.com/news/technology-65057011).

<sup>5</sup> See generally C. Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, in *Center on Privacy & Technology at Georgetown Law*, 6 December 2022, [www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations](http://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations).

*Anonymous Author*

This chapter provides a brief overview of the legislative landscape in which U.S. law enforcement agencies use facial recognition technology. Part I focuses on the federal level; in the absence of either technology-specific or comprehensive privacy legislation, this part looks to constitutional considerations. Part II outlines state and local facial recognition-specific legislation, highlighting the different regulatory approaches legislators have taken to date. Part III briefly examines the treatment of facial recognition in criminal courts. Absent germane legislation, defendants have asked courts to consider constitutional arguments and prior decisions on analogous forensic techniques to challenge facial recognition identifications, with varying success.

## **2. Part I: Federal legislative efforts and the constitutional floor**

There is no overarching federal framework for police use of facial recognition in the United States.<sup>6</sup> Over the past five years, several lawmakers on both sides of the aisle have proposed legislation to this effect. The Facial Recognition and Biometric Technology Moratorium Act, for example, first introduced in 2020 and again in subsequent years, proposed to halt federal use of the technology unless explicitly authorized by Congress and to withhold certain federal grants to state and local governments that use facial recognition systems.<sup>7</sup> The Facial, Accountability, Clarity, and Efficiency in Technology (FACE IT) Act,

<sup>6</sup> The Civil Rights Implications of the Federal Use of Facial Recognition Technology, U.S. Commission on Civil Rights, 1-2. September 2024, [www.usccr.gov/files/2024-09/civil-rights-implications-of-frt\\_0.pdf](http://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf). This is not to say that there is no applicable federal law; statutes addressing privacy; data collection, storage, and access; border security; civil rights; and more may well apply to certain facial recognition use cases. See, e.g., Pub. L. No. 93-579 (1974) (the Privacy Act of 1974, governing agencies' collection, disclosure, and use of personal information); see, e.g., Pub. L. No. 88-352 (1964) (the Civil Rights Act of 1964, prohibiting discrimination and denial of benefits on the basis of race, color, religion, sex, and national origin); see, e.g., 8 U.S.C. § 1365b (requiring the Department of Homeland Security to establish a biometric entry and exit system of records for foreign national arrivals to and departures from the United States).

<sup>7</sup> S.41084, 116th Cong. 2019-2020, available at: [www.congress.gov/bill/116th-congress/senate-bill/4084/text](http://www.congress.gov/bill/116th-congress/senate-bill/4084/text); S.2052, 117th Cong. 2021-2022, available at [www.congress.gov/bill/117th-congress/senate-bill/2052/text](http://www.congress.gov/bill/117th-congress/senate-bill/2052/text); S.681, 118th Cong. 2023-2024, available at: [www.congress.gov/bill/118th-congress/senate-bill/681/text](http://www.congress.gov/bill/118th-congress/senate-bill/681/text).

introduced in 2022, proposed best practices for facial recognition use, including disclosure, technology accuracy thresholds, and human adjudication of results.<sup>8</sup> The Facial Recognition Act of 2022 would have placed a warrant requirement on most law enforcement facial recognition searches.<sup>9</sup> None have successfully passed into law; many never even made it out of committee.<sup>10</sup>

In this relative legislative vacuum, and as with any government action, the Constitution provides crucial baseline parameters for facial recognition use in criminal investigative and surveillance contexts.<sup>11</sup> Across a range of use cases, the technology implicates several constitutional amendments:

### **2.1. Free speech and the right to anonymity**

The U.S. has a robust body of case law enshrining a right to anonymity within the First Amendment's free speech, association, assembly, and petition protections from undue government influence.<sup>12</sup> In 1958, the Supreme Court recognized a "vital relationship between the freedom to associate and privacy in one's associations" in a case striking down the compelled disclosure of organization membership lists.<sup>13</sup> In 1960, it held that identification requirements for political pamphlets distributed in public "would tend to restrict freedom to distribute information and thereby freedom of expression."<sup>14</sup> Perhaps

<sup>8</sup> S.5334, 117th Cong. 2021-2022, available at: [www.congress.gov/bill/117th-congress/senate-bill/5334/text](http://www.congress.gov/bill/117th-congress/senate-bill/5334/text).

<sup>9</sup> H.R. 9061, 117th Cong. 2021-2022, available at: [www.congress.gov/bill/117th-congress/house-bill/9061/text](http://www.congress.gov/bill/117th-congress/house-bill/9061/text).

<sup>10</sup> See G. Shea, *Face Recognition Technology Policy Landscape, Terms, and Definitions*, in *Bipartisan Policy Center*, 14 April 2023, <https://bipartisanpolicy.org/blog/frt-policy-terms-definitions>.

<sup>11</sup> For a more lengthy treatment of the relationship between constitutional rights and police use of facial recognition technology, see K.Y. Santamaria, *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*, Congressional Research Service, 24 September 2020, <https://crsreports.congress.gov/product/pdf/R/R46541/1>.

<sup>12</sup> The First Amendment states: "Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or 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." U.S. Const. Amend. I.

<sup>13</sup> NAACP v. Patterson, U.S. Supreme Court, 357 U.S. 449 (1958).

<sup>14</sup> Talley v. California, U.S. Supreme Court, 362 U.S. 60 (1960).

most famously, in 1995 the Court wrote in a case striking down a state law that prohibited anonymous campaign literature:

“Anonymity is a shield from the tyranny of the majority .... It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation - and their ideas from suppression - at the hand of an intolerant society.”<sup>15</sup>

Facial recognition is fundamentally a deanonymization tool.<sup>16</sup> It offers its users the ability to identify previously unknown faces in photos and videos, in the online and offline world, by comparing them to previously compiled identity databases. In more advanced deployments, it affords the government the unique capability of remote, secret biometric surveillance which, if turned on public protests or gatherings, would directly implicate the First Amendment.<sup>17</sup>

Early law enforcement policy documents acknowledged this risk. A 2011 Privacy Impact Assessment written by officials at the Federal Bureau of Investigation (FBI) and various state and local agencies stated, under the heading Identification: The Erosion or Compromise of Anonymity: “The potential harm of identification is that it increases the government’s power to control individuals through [] chilling effects .... It can further inhibit one’s ability to be anonymous;” and: “Anonymity is an important right in a free society in so far as it protects people from bias based on their identities and enables people to vote, speak, and associate more freely by protecting them from the danger of reprisal.”<sup>18</sup>

The relationship between police facial recognition use and the First Amendment has yet to be tested in court. Perhaps the most

directly relevant case predates police adoption of the technology by just two years. The City of Goshen, Indiana had enacted a law making it illegal for anyone over the age of eighteen to wear a mask or hood in public “for the purpose of disguising or concealing” his identity. In the resulting case brought by members of the Ku Klux Klan in 1999, the court struck down the law on the grounds that it unduly burdened the group’s right to anonymous speech, association, and public assembly beyond what was reasonably necessary to fulfill the city’s stated purpose of preventing violence.<sup>19</sup> While the case did not involve facial recognition technology, the decision is instructive, drawing a direct connection between the visibility of one’s face and the disclosure of personal information that the right to anonymity seeks to protect. When “facial recognition might be expected to disclose name, address and other commonly known information,”<sup>20</sup> government action requiring disclosure - or prohibiting obfuscation - may be found unconstitutional.

## **2.2. The right to privacy**

The constitutionally protected right to privacy, emanating from the language of the Fourth Amendment, may extend beyond the home to cover “reasonable expectations of privacy” to some public settings and activities.<sup>21</sup> In a 2018 case examining police access to historical cell site location information (CSLI) without a warrant, and departing somewhat from prior decisions,<sup>22</sup> the Supreme Court interpreted the Fourth Amendment as including a right to privacy to a person’s movements across time and space even as those movements occurred in public. “[N]ear perfect surveillance” that provides a “detailed log of [one’s] movements over an extended period of time” would implicate the

<sup>15</sup> *McIntyre v. Ohio Elections Commission*, U.S. Supreme Court, 514 U.S. 334 (1995).

<sup>16</sup> See C. Garvie, *Face Recognition and the Right to Stay Anonymous*, in *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge, Cambridge University Press, 2022, 139-152.

<sup>17</sup> See generally C. Garvie and L. Moy, *America Under Watch: Face Surveillance in the United States*, Center on Privacy & Technology at Georgetown Law, 16 May 2019, [www.americaunderwatch.com](http://www.americaunderwatch.com).

<sup>18</sup> Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, International Justice and Public Safety Network, 18 - 19, June 30, 2011, available at: [www.eff.org/files/2013/11/07/09\\_-\\_facial\\_recognition\\_pia\\_report\\_final\\_v2\\_2.pdf](http://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf).

<sup>19</sup> *American KKK v. City of Goshen*, U.S. District Court for N.D. Indiana, 50 F. Supp. 2d 835 (1999).

<sup>20</sup> *Id.*

<sup>21</sup> The Fourth Amendment states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. Amend. IV.

<sup>22</sup> See *Katz v. United States*, 389 U.S. 347, 351 (1967) (holding that “[w]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection”).

*Anonymous Author*

Fourth Amendment and require a warrant.<sup>23</sup>

With enough surveillance cameras and a large enough database, facial recognition technology could theoretically be used to track someone's activities, providing "an intimate window into [that] person's life, revealing not only his particular movements, but through them his 'familiar, political, professional, religious, and sexual associations.'"<sup>24</sup> And, unlike a cell phone that produced the CSLI information at issue in *Carpenter v. United States*, a person cannot leave his face at home.

While most U.S. police facial recognition systems are investigative, used to identify one or a few individuals from a static image or video, various departments have also explored facial recognition systems' ability to conduct broader forms of surveillance which could trigger Fourth Amendment privacy protections. In 2016, law enforcement and transit agencies in Chicago, Illinois purchased a system involving "Real Time Screening using Facial Recognition on Chicago's vast camera monitoring system which includes nearly 20,000 street, transit, and other video cameras."<sup>25</sup> The police department for Detroit, Michigan, acquired a similar "Real Time Video Feed Facial Recognition" system in 2017, paired with cameras at more than 500 gas stations, liquor stores, clinics, churches, apartment buildings, and other locations throughout the city before it was discontinued.<sup>26</sup> New York City briefly piloted a facial recognition program in 2019 to identify drivers through vehicle windshields as they entered the city, though the pilot failed to detect a single face.<sup>27</sup>

Facial recognition applications falling short

<sup>23</sup> *Carpenter v. United States*, U.S. Supreme Court, 138 U.S. 2206, 2217 (2018).

<sup>24</sup> *Id.* (quoting Justice Sotomayor's concurrence).

<sup>25</sup> See *supra* note 17.

<sup>26</sup> *Id.*

<sup>27</sup> E.C. Baig, *Facial recognition flunks ID test at New York City's RFK Bridge*, report says, USA Today, 8 April 2019, [www.usatoday.com/story/tech/talkingtech/2019/04/08/bridge-failure-facial-recognition-id-flunks-test-nycs-rfk-bridge/3401879002](http://www.usatoday.com/story/tech/talkingtech/2019/04/08/bridge-failure-facial-recognition-id-flunks-test-nycs-rfk-bridge/3401879002). Other facial recognition surveillance programs were piloted in Orlando, Florida, and Washington, DC. See B. Chappell, *Orlando Police End Test of Amazon's Real-Time Facial 'Rekognition' System*, in *NPR*, 26 June 2018, [www.npr.org/2018/06/26/623545591/orlando-police-end-test-of-amazons-real-time-facial-rekognition-system](http://www.npr.org/2018/06/26/623545591/orlando-police-end-test-of-amazons-real-time-facial-rekognition-system); see J. Schuppe, *Secret Service tests facial recognition surveillance system outside White House*, NBC News, 4 December 2018, [www.nbcnews.com/news/us-news/secret-service-tests-facial-recognition-surveillance-system-outside-white-house-n943536](http://www.nbcnews.com/news/us-news/secret-service-tests-facial-recognition-surveillance-system-outside-white-house-n943536).

of widespread surveillance less clearly trigger Fourth Amendment protections. Courts have not ruled on questions relating to whether the law enforcement agencies' creation and search of facial recognition databases is a constitutional "search." A person's physical characteristics, such as his voice or facial features, to the extent that they are "constantly exposed to the public," have not been afforded Fourth Amendment protection.<sup>28</sup> Similarly, the Supreme Court has upheld state "stop and identify" laws, today found in half of all U.S. states, if an individual is under "reasonable suspicion" of criminal activity by police.<sup>29</sup>

### 2.3. The right to a fair trial

Much of the Bill of Rights, comprising the first ten constitutional amendments, is focused on fair treatment of an individual once he has become the subject of a criminal investigation or has been charged with or convicted of a crime. The due process clause of the Fifth Amendment guarantees an individual "a fair opportunity to defend against the State's accusations."<sup>30</sup> That opportunity includes the right of the defense to review any evidence held by the state that is material to the person's guilt or punishment.<sup>31</sup> The Supreme Court has determined information to be material if it: 1) negates guilt;<sup>32</sup> 2) negates an element of the crime;<sup>33</sup> 3) impeaches a witness;<sup>34</sup> or 4) mitigates punishment.<sup>35</sup>

As a tool used to identify a suspect, police facial recognition searches definitionally produce information that is material to a defendant's case.<sup>36</sup> Any risk of mistake or

<sup>28</sup> See *United States v. Dionisio*, U.S. Supreme Court, 410 U.S. 1, 14 (1973).

<sup>29</sup> *Hiibel v. Sixth Judicial Dist. Court of Nev.* U.S. Supreme Court, 542 U.S. 177 (2004).

<sup>30</sup> See *Chambers v. Mississippi*, U.S. Supreme Court, 410 U.S. 284, 294 (1973). The Fifth Amendment states, in part: "No person shall be ... deprived of life, liberty, or property, without due process of law." U.S. Const. Amend. V.

<sup>31</sup> *Brady v. Maryland*, U.S. Supreme Court, 272 U.S. 83, 87 (1963) ("The suppression by the prosecution of evidence favorable to the accused upon request violates due process where the evidence is material either to guilt or to punishment").

<sup>32</sup> See, e.g., *Kyles v. Whitley*, U.S. Supreme Court, 514 U.S. 419, 421 (1995).

<sup>33</sup> See, e.g., *Miller v. Pate*, U.S. Supreme Court, 386 U.S. 1 (1967).

<sup>34</sup> See, e.g., *Giglio v. United States*, U.S. Supreme Court, 405 U.S. 150 (1970).

<sup>35</sup> See, e.g., *supra* note 31.

<sup>36</sup> For a more in-depth discussion of the relationship between police facial recognition searches and due process, see *supra* note 5, 39 - 46.

misidentification present in a facial recognition search undermines the confidence in the defendant's identification as the suspect, which would negate guilt.<sup>37</sup> Most systems are additionally designed to return multiple possible matches, further negating guilt by suggesting that other individuals may be the true perpetrator.<sup>38</sup> Facial recognition systems and the officers running the search further operate as a sort of witness against the accused, selecting him for further investigation or arrest from an array of possible suspects.<sup>39</sup> Under the Fifth Amendment, then, the defendant should be entitled to information about facial recognition technology and how the search was run if such a search contributed to his identification as the criminal suspect.

The Sixth Amendment holds that "the accused shall enjoy the right ... to be confronted with the witnesses against him"<sup>40</sup> and governs what - and how - evidence may be introduced in court.<sup>41</sup> When considering scientific evidence or other expert witness testimony, federal courts ask: 1) whether the theory or technique in question can be or has been tested; 2) whether it has been subjected to peer review and publication; 3) its known or potential error rate; 4) the existence and maintenance of standards controlling its operation; and 5) whether it has garnered widespread acceptance within the relevant scientific community.<sup>42</sup>

Facial recognition evidence fails to pass this inquiry, in large part due to the absence of regulatory or other widely followed rules governing how police should conduct searches.<sup>43</sup> To date, perhaps in recognition of these shortcomings, prosecutors have resisted introducing facial recognition search results directly in court, opting instead to consider it an "investigative lead" that is corroborated through additional evidence.<sup>44</sup> Nonetheless, in numerous criminal cases the prosecution has relied heavily, if not exclusively, on a facial recognition identification, at times resulting in

wrongful arrests.<sup>45</sup>

#### **2.4. Equal protection under the laws**

The Fourteenth Amendment prohibits states from denying "to any person within its jurisdiction the equal protection of the laws."<sup>46</sup> According to the Supreme Court, "[r]acial and ethnic distinctions of any sort are inherently suspect and thus call for the most exacting examination."<sup>47</sup> Such distinctions may not de facto be unconstitutional; rather, the equal protection clause triggers varying levels of scrutiny to be applied to the governmental action in question.<sup>48</sup>

People of color, particularly Black men, have historically disproportionately comprised U.S. police facial recognition databases due to widespread racial patterns in criminal arrests.<sup>49</sup> Communities of color may also disproportionately be subjected to police use of the technology. In an audit of police use of both facial recognition and automated license plate readers in its jurisdiction, the San Diego Association of Governments found that the tools were used up to 2.5 times more on communities of color than what their proportion of the overall city population would predict.<sup>50</sup> As summarized on a slide titled "Risk: Discriminatory surveillance," the audit also noted that men were twice as likely to be targeted, 15% of women were targeted for voyeuristic reasons, and 65% of teenagers

<sup>37</sup> See *id.*, 13-33.

<sup>38</sup> See *id.*, 22-33.

<sup>39</sup> See *id.*, 42-43.

<sup>40</sup> U.S. Const. Amend. VI.

<sup>41</sup> This right is expanded in the Federal Rules of Criminal Procedure and the Federal Rules of Evidence.

<sup>42</sup> *Daubert v. Merrell Dow Pharmaceuticals Inc.*, U.S. Supreme Court, 509 U.S. 579 (1993).

<sup>43</sup> For a more in-depth analysis of facial recognition under each of these factors, see *supra* note 5, 43-46.

<sup>44</sup> *Id.*

<sup>45</sup> See *id.*, 6-8. See D. MacMillan, D. Ovalle, and A. Schaffer, *Arrested by AI: Police ignore standards after facial recognition matches*, in *Washington Post*, 13 January 2025, [www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/](http://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/).

<sup>46</sup> U.S. Const. Amend. XIV. The Supreme Court has held that equal protection applies to the federal government via the Due Process Clause of the Fifth Amendment. *Bolling v. Sharpe*, 347 U.S. 497, (1954).

<sup>47</sup> *University of California Regents v. Bakke*, U.S. Supreme Court, 438 U.S. 265, 291, (1978).

<sup>48</sup> See *Clark v. Jeter*, U.S. Supreme Court, 486 U.S. 456, 461 (1988). For a more in-depth discussion of facial recognition and the equal protection clause, see *supra* note 6 at 16-29.

<sup>49</sup> See *supra* note 2, 56 (outlining arrest to population ratios in various jurisdictions that have paired facial recognition with mugshot databases). In jurisdictions that run police facial recognition searches on driver's license databases, or that use Clearview AI's system that runs against images collected from the Internet, these disparities may be diminished.

<sup>50</sup> Automated Regional Justice Information System, San Diego's Privacy Policy Development: Efforts & Lessons Learned (undated), available at: <https://drive.google.com/file/d/1ZR2jjiLcBMUKnHTRk1ZC248NbfUqNRww/view?pli=1>.

*Anonymous Author*

were targeted for no reason.<sup>51</sup>

These policing biases extend beyond the technology; what is unique to facial recognition is that it may perform differently - more or less accurately - depending on the race, sex, and age of the subject of the search. A 2024 report published by the National Academies of Sciences, Engineering, and Medicine noted that “[a]ll face recognition system components potentially have error rates that depend on the demographics of the subjects” and that “[f]or most algorithms [false positive, or misidentification] rates are higher in women than men, also in the very young and old, and in particular ethnic groups.” A law enforcement tool that places certain individuals at heightened risk of misidentification, and by extension wrongful arrest and possibly conviction, may trigger an equal protection inquiry. While this theory is the subject of much reporting, academic writing, and legislative debate, to date it remains untested by the courts.

### 3. Part II: State and local legislative approaches

Responding to growing concern over police use of facial recognition and to the absence of federal legislation, state and local legislators have introduced - and passed - several facial recognition laws over the past eight years. By the end of 2024, fifteen states had some form of legislation governing police facial recognition use; many more local jurisdictions had additionally passed their own ordinances.<sup>52</sup> Earlier efforts focused on wholesale prohibitions of the technology; more recent legislative activity has typically emphasized regulatory frameworks designed to find a balance between the investigative benefits of facial recognition and necessary constitutional protections. Overall, these approaches can be broadly grouped into three categories: complete bans, moratoria, and regulatory bills.<sup>53</sup>

<sup>51</sup> *Id.*

<sup>52</sup> States with police facial recognition legislation are: Alabama, Colorado, Illinois, Maine, Maryland, Massachusetts, Minnesota, Montana, New Hampshire, Oregon, Utah, Vermont, Virginia, and Washington. See Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, Tech Policy Press, Jan. 6, 2025, <https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations>.

<sup>53</sup> See J. Spivack and C. Garvie, *A Taxonomy of*

### 3.1. Bans

Several cities have taken the most stringent approach by banning the use of facial recognition by police or all government officials. In 2019, San Francisco became the first major U.S. city to prohibit its employees from using facial recognition, followed by a few dozen cities around the country.<sup>54</sup> Outlining the logic to its approach, the San Francisco law stated: “The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring.”<sup>55</sup>

### 3.2. Moratoria

Other jurisdictions have opted for moratoria rather than outright bans, covering all or select police uses of facial recognition technology. Moratoria have been time-bound, allowing the use of facial recognition to be reconsidered after a set period, or directive, predicating future use of the technology on specific legislative action. In Springfield, Massachusetts, a bill proposed in 2020 would have placed a time-bound prohibition on police use of the technology until 2025; the bill that ultimately passed was directive, banning the technology until the police department developed a policy that passed the approval of city council.<sup>56</sup>

Both approaches follow from a similar range of arguments: more research into the technology and its impacts on civil liberties is needed; the legislature should allow more robust public engagement prior to a permanent legislative approach; or the technology needs

*Legislative Approaches to Face Recognition in the United States*, in *Regulating Biometrics: Global Approaches and Open Questions*, AI Now Institute, 1 September 2020, 86, <https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions>.

<sup>54</sup> For a list of municipal bans, see Ban Facial Recognition Interactive Map, Fight for the Future, [www.banfacialrecognition.com/map/](http://www.banfacialrecognition.com/map/) (last accessed 28 January 2025).

<sup>55</sup> San Francisco Ord. No. 190110, *Acquisition of Surveillance Technology*, May 31, 2019, <https://sfgov.legistar.com/LegislationDetail.aspx?ID=3850006&GUID=12FC5DF6-AAC9-4F4E-8553-8F0CD0EBD3F6>.

<sup>56</sup> See Paul Tuthill, *Springfield Passes Moratorium On Face Surveillance Technology*, WAMC, 25 February 2020, available at: [www.wamc.org/new-england-news/2020-02-25/springfield-passes-moratorium-on-face-surveillance-technology](http://www.wamc.org/new-england-news/2020-02-25/springfield-passes-moratorium-on-face-surveillance-technology)

time to improve before the issue is ripe for legislation.<sup>57</sup> While directive moratoria may require the creation of a task force or commission to examine the technology, one obvious limitation to the time-bound approach is that ordinances may expire without meaningful progress made on any of these fronts.<sup>58</sup> California, for example, enacted a law in 2020 prohibiting the use of facial recognition in conjunction with body cameras until January 1, 2023. The legislative findings for the law stated: “Facial recognition and other biometric surveillance would corrupt the core purpose of officer-worn body-worn cameras by transforming those devices from transparency and accountability tools into roving surveillance systems.”<sup>59</sup> This decisive finding notwithstanding, the law was allowed to lapse, and any protections it afforded disappeared.

### **3.3. Regulation**

A growing number of legislators have opted to introduce regulatory bills that impose restrictions, procedural guardrails, and oversight mechanisms on facial recognition use rather than banning it outright. These laws contain many similar elements, including:

- Certain applications are prohibited, such as real-time or other surveillance uses or pairing the technology with body cameras or drones. In 2017, Oregon adopted the first state-level facial recognition restriction, prohibiting the use of the technology in conjunction with police body cameras.<sup>60</sup>
- Use requires a court order or probable cause determination. Montana’s law, passed in 2023, requires police to obtain a warrant prior to performing a facial recognition search, except in cases involving imminent threats.<sup>61</sup>
- Matches cannot be the sole basis for an

arrest and must be corroborated by additional investigative methods and evidence. Alabama passed a law in 2022 which states: “To establish probable cause in a criminal investigation or to make an arrest, a state or local law enforcement agency may use facial recognition technology match results only in conjunction with other lawfully obtained information and evidence.”<sup>62</sup>

- Use is restricted to investigating a specific subset of crimes, such as felonies, or is limited to suspects only and/or cannot be used to identify witnesses. Maryland’s facial recognition law, passed in 2024, restricts police facial recognition use to certain predefined crimes, including crimes of violence, human trafficking, weapons offenses, and importation of fentanyl.<sup>63</sup>
- Defendants must receive notice and disclosure of use in the case against them. Washington’s 2020 law requires government agencies to disclose their use of facial recognition to a defendant “in a timely manner prior to trial.” It also requires agencies to maintain records of their use of the technology to facilitate public reporting and auditing.<sup>64</sup>
- The technology or search processes must be tested for reliability or must meet minimum thresholds of reliability. Virginia’s law, passed in 2022 and effective until 2026, restricts agencies to purchasing systems that have been evaluated by the federal National Institute of Standards and Technology and have demonstrated “an accuracy score of at least 98 percent true positives within one or more datasets relevant to the application” in which they will be deployed.<sup>65</sup>
- The technology must be sufficiently free of racial or other demographic bias in performance. Virginia’s law also requires “minimal performance variations across demographics associated with race, skin tone, ethnicity, or gender.”<sup>66</sup>

### **4. Part III: Facial recognition in criminal courts**

Police throughout the United States continue to use facial recognition in criminal

<sup>57</sup> See, e.g., J. Cote, *Springfield City Council passes facial recognition moratorium*, in *MassLive*, 25 February 2020, [www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html](http://www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html) (describing that the moratorium would “allow police to come back to the council in the future if the software improves in accuracy and law enforcement wants to use it under limited circumstances”).

<sup>58</sup> See, e.g., WA S.B. 5528 (2019) (which would set up a task force to study the technology and deliver a report to the legislature about potential civil liberties impacts).

<sup>59</sup> Ca. A.B. 1215 (2019).

<sup>60</sup> O.R.S. 133.741.

<sup>61</sup> Mont. Code. Ann. 44-15-106 (2023).

<sup>62</sup> Ala. Code § 15-10-111.

<sup>63</sup> Md. S.B. 182 (2024).

<sup>64</sup> R.C.W. 43.386.070 (2020).

<sup>65</sup> Va. Code § 52-4.5 (2022).

<sup>66</sup> *Id.*

*Anonymous Author*

investigations, not waiting for legislative guardrails. As a consequence, trial courts increasingly arbitrate how to fit facial recognition within an incomplete and patchwork legal framework, primarily focusing on the due process rights of criminal defendants. Two cases illustrate the inconsistencies that may result from a court-driven approach to regulation:

**4.1. *Lynch v. Florida***

Willie Allen Lynch was convicted of selling drugs to two undercover officers in 2016. The evidence pointing to Lynch as the suspect consisted solely of a facial recognition search, which returned a photo of Lynch and four other possible matches, and a statement by the two officers - after viewing only Lynch's mugshot photo - that he was the suspect in question.<sup>67</sup> On appeal, Lynch argued that he was deprived of his due process rights, specifically that the due process clause, as interpreted by the Supreme Court in *Brady v. Maryland*, required the state to disclose the other four photos that the facial recognition system had produced as possible matches. Those photos amounted to other suspects, casting doubt on Lynch's guilt.<sup>68</sup>

The appellate court rejected the argument. In upholding the lower court conviction, the court reasoned: "...because he cannot show that the other photos in the database returned resembled him, he cannot show that they would have supported his argument that someone in one of those photos was the culprit."<sup>69</sup> In other words, Lynch would have needed to be able to describe what the other facial recognition result photos looked like in order for the court to permit him to view those same photos.

**4.2. *New Jersey v. Arteaga***

In 2023, an appellate court in New Jersey took on a similar question: whether the state was required to turn over information about the technology and procedures underlying a facial recognition search in accordance with

*Brady v. Maryland*.<sup>70</sup> Departing from the court's approach in the *Lynch* case, the *Arteaga* court held that the defense is entitled to this information, even when the search was used as an investigative lead and not introduced as evidence in court. It concluded that "defendant ... provide[s] us convincing evidence of FRT's [facial recognition technology] novelty, the human agency involved in generating images, and the fact FRT's veracity has not been tested or found reliable on an evidential basis by any New Jersey Court."<sup>71</sup>

These are the only two appellate cases to date to substantively consider questions surrounding police use of facial recognition technology and its impacts on the rights of defendants. Numerous other criminal defendants have raised similar questions; most cases, however, result in a plea negotiation before these questions can be examined in full.<sup>72</sup> It is abundantly apparent that the U.S. cannot rely on its criminal judicial system to establish comprehensive privacy and civil liberties protections around police use of facial recognition; legislation is essential.

**5. Conclusion: Flipping the script**

Over the past twenty years, police adoption of facial recognition technology has vastly outpaced legislative efforts. In the absence of comprehensive federal legislation, courts and local governments have admirably navigated complex determinations of technological benefits, constitutional protections, and what Americans believe the appropriate balance between the two might be - and yet most of the country remains without meaningful guardrails. Renewed and growing calls for more comprehensive, technology-neutral, privacy legislation may provide an alternative approach to piecemeal and reactive efforts seeking to address each new technology as - or twenty years after - it has already been adopted. Legislators may be more successful focusing on the broader societal interests at stake and the rights they are seeking to promote and protect than a piece of technology. Legislation will always lag behind technological innovation; rights protections should not.

<sup>67</sup> See B. Conarck, *How a Jacksonville man caught in the drug war exposed details of police facial recognition*, Florida Times Union, 26 May 2017, [www.jacksonville.com/news/metro/public-safety/2017-05-26/howjacksonville-man-caught-drug-war-exposed-details-police](http://www.jacksonville.com/news/metro/public-safety/2017-05-26/howjacksonville-man-caught-drug-war-exposed-details-police). See Initial Brief of Appellant, 14, *Lynch v. State of Florida*, 2017 WL 11618201 (Fla. App. 1 Dist. 2017).

<sup>68</sup> Initial Brief of Appellant, 14, *Lynch v. State of Florida*, 2017 WL 11618201 (Fla. App. 1 Dist. 2017).

<sup>69</sup> *W.A. Lynch v. State of Florida*, No. 1D16-3290, 2017 WL 11618201 (Fla. App. 1 Dist. 2017).

<sup>70</sup> *New Jersey v. Arteaga*, Sup. Ct. N.J. No. A-3078-21T1 (2023).

<sup>71</sup> *Id.*

<sup>72</sup> See Testimony of C. Garvie, *Before the U.S. Commission on Civil Rights*, 8 March 2024, available at: [www.nacdl.org/getattachment/0725bfd1-6567-4d81-b980-f1bf150f349c/garvie\\_testimony\\_civil-rights-commission\\_on\\_face-recognition.pdf](http://www.nacdl.org/getattachment/0725bfd1-6567-4d81-b980-f1bf150f349c/garvie_testimony_civil-rights-commission_on_face-recognition.pdf).