THE PRICE OF PRIVACY: A CALL FOR A BLANKET BAN ON FACIAL RECOGNITION IN THE CITY OF ST. LOUIS

Sylvia Waghorne*

INTRODUCTION

On September 9, 2020, Portland, Oregon passed the broadest ban on the use of facial recognition technology to date in any United States city, prohibiting both governmental and private sector use of facial recognition.[1] Generally speaking, facial recognition technology identifies individuals by mapping the unique features of their face and comparing that information to a database in order to find a match or confirm an identity. Major urban centers such as Boston and San Francisco had previously banned use of facial recognition technology by city governments, but Portland's ordinance was the first to prevent private entities from utilizing the technology.[2] A year later in September 2021, the city of Baltimore followed suit by banning use of facial technology in the private sector, but this ban did not extend to the public sector.[3] The discussion on whether facial recognition is a boon or a bane has been hotly contested, with strong advocates on both sides.

For those who oppose facial recognition, the question of whether facial recognition can continue to be used is one that demands immediate and swift action. In the words of Evan Greer, a vehement critic of facial recognition technology and deputy director for Fight for the Future,[4] "[f]acial recognition is like nuclear or biological weapons. It poses such a threat to

---

* J.D. (2022), Washington University School of Law.

1. *See* Rachel Metz, *Portland Passes Broadest Facial Recognition Ban in the US*, (Sept. 9, 2020), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html [https://perma.cc/CQB7-NVAJ].

2. *See id.*

3. Michael Borgia & Kristen Bertch, *Baltimore City's Ban on Facial Recognition Now in Effect*, DAVIS WRIGHT TREMAINE: PRIV. & SEC. L. BLOG (Sept. 8, 2021), https://www.dwt.com/blogs/privacy--security-law-blog/2021/09/baltimore-facial-recognition-ban [https://perma.cc/WL2A-X8MA].

4. Fight for the Future is a non-profit advocacy group that defends the rights of marginalized peoples in the digital age. *See* FIGHT FOR THE FUTURE, https://www.fightforthefuture.org/about [https://perma.cc/7K62-FXEN].

the future of human society that any potential benefits are outweighed by the inevitable harms."[5] Facial recognition, once something thought only to appear in science fiction novels, has quickly become a regular part of our everyday lives—even if we do not always realize it.[6] As its prevalence grows, it is necessary to take a definitive stance on the use of facial recognition in society. Numerous cities across the United States have begun to recognize the danger that facial recognition presents for their citizens and have passed legislation that limits or outright bans the use of the technology in certain circumstances, but others are forging ahead and embracing the use of facial recognition by law enforcement and in areas that require heightened security such as airports.[7]

Portland, Oregon, Boston, and San Francisco[8] have already declared their position against facial recognition, and other cities[9] are following in their footsteps. By May 2021, seven states and roughly two dozen cities across the country took steps to limit the use of facial recognition

5. Makena Kelly, *Feds Would be Banned from Using Facial Recognition Under New Bill*, VERGE (June 25, 2020, 2:04 PM), https://www.theverge.com/2020/6/25/21303355/facial-recognition-ed-markey-ayanna-pressley-ban-federal-agencies-fed-law-enforcement [https://perma.cc/7GDF-22CC].

6. *See* Nikki Gladstone, *How Facial Recognition Technology Permeated Everyday Life*, CTR. FOR INT'L GOVERNANCE INNOVATION (Sept. 19, 2018), https://www.cigionline.org/articles/how-facial-recognition-technology-permeated-everyday-life [https://perma.cc/9CC2-ACG4] ("In reality, facial recognition technology has already permeated our day-to-day activities. It unlocks phones, tags friends on Facebook and secures homes. But personal engagement with a technology doesn't always translate into a full understanding of how that technology collects and uses data.").

7. For an interactive map on where facial recognition is in use and where it has been banned, *see* BAN FACIAL RECOGNITION, https://www.banfacialrecognition.com/map/ (last visited Feb. 12, 2022).

8. *See supra* Metz, note 1.

9. Portland, Maine passed a ballot initiative that bans use of facial recognition by police and city agencies on November 3, 2020; the ordinance does not apply to private sector use of the technology. *See* Russel Brandom, *Portland, Maine had Voted to Ban Facial Recognition*, VERGE (Nov. 4, 2020, 2:04 AM), https://www.theverge.com/2020/11/4/21536892/portland-maine-facial-recognition-ban-passed-surveillance. Minneapolis likewise has adopted a ban on use of facial recognition technology by city agencies. *See* Kim Lyons, *Minneapolis Prohibits Use of Facial Recognition Software by Its Police Department*, VERGE (Feb. 13, 2021, 9:48 AM), https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy [https://perma.cc/E2HS-PBUX].

technology,[10] while others rejected attempts to curtail the technology.[11] The response to the use of facial recognition has varied widely, partly due to the lack of a federal regulatory scheme that would necessitate consistency. This Note proposes that St. Louis should, given the present absence of federal or state level guidance, enact measures similar to those adopted in Portland, Oregon and ban the use of facial recognition technology by both governmental and private entities. Citizens have a stake in both the commercial use of their facial data and in the use by public agencies such as law enforcement; therefore, any meaningful ban must take on both private and public uses of facial recognition technology. Advocates for facial recognition argue that banning the use of facial recognition would come at cost—particularly, proponents emphasize the role it can play in increasing security and safety[12]—but this Note challenges its reader to consider if the technology truly provides the benefits it promises, and the values at stake if the use of facial recognition is allowed to continue and proliferate. Ultimately, a ban on facial recognition technology is necessary to protect individual privacy, to curtail bias and abuse that is already rampant within our criminal justice system, and to countervail the pervasive impact that surveillance has on a healthy democracy.

Part I of this Note defines what facial recognition technology entails and outlines the various ways facial recognition technology has been used in the United States at large by both private and governmental bodies, and more specifically in St. Louis, Missouri. This section will highlight the costs and benefits of having such technologies in place with regards to security, privacy, and individual autonomy. Additionally, this section will detail some notable attempts to regulate the use of facial recognition thus far at the local, state, and national level. Part II will analyze the aforementioned

10. Julie Carr Smyth, *States Push Back Against Use of Facial Recognition by Police*, ABC NEWS (May 5, 2021, 4:32 PM), https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175 [https://perma.cc/8EN2-DHKU].

11. Jake Parker, *Most State Legislatures Have Rejected Bans and Severe Restrictions on Facial Recognition*, SEC. INDUS. ASS'N (July 9, 2021), https://www.securityindustry.org/2021/07/09/most-state-legislatures-have-rejected-bans-and-severe-restrictions-on-facial-recognition/ [https://perma.cc/SSD8-HJP4].

12. Bernard Marr, *Facial Recognition Technology: Here Are The Important Pros And Cons*, FORBES (Aug 19, 2019, 12:31 AM), https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#4d0bdf9514d1 ("One of the major advantages of facial recognition technology is safety and security. Law enforcement agencies use the technology to uncover criminals or to find missing children or seniors.").

uses of facial recognition technology and argue that, while there are potential benefits, particularly increased safety and lowered crime rates, the potential misuse or abuse of such technology is too great a cost to the individual privacy and expression fundamental to a democratic society. This Note will then propose that St. Louis follow in the footsteps of Portland by banning both private and public entity use of facial recognition and argue that it is the best course of action to take in light of the realities of having facial recognition technology in use. In Part III, this Note will conclude by rearticulating a proposal to ban facial recognition in St. Louis and the imperative of dealing with facial recognition technology with decisive and drastic action.

I. FACIAL RECOGNITION TECHNOLOGY USES AND CONTROVERSY

a. Defining Facial Recognition

In order to discuss the use of facial recognition technology, it is necessary to have an understanding how facial recognition technology works. According to Professors Evan Selinger, Rochester Institute of Technology, and Woodrow Hartzog, Northeastern University School of Law:

> [w]hen we use the term face surveillance, we mean the use of facial recognition technologies and faceprint or name-faceprint databases to monitor behavior, identify people, or gain insight or information for the purposes of influencing, managing, directing, or deterring people.[13]

Typically, facial recognition identification is accomplished in one of two ways: one-to-many recognition or one-to-one recognition.[14] One-to-many recognition involves determining who an unknown individual is by comparing their image to a database of images and identifying a match

13. Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 101, 103 (2020).

14. *See* Eifeh Strom, *Facing Challenges in Face Recognition: One-to-One vs. One-to-Many*, ASMAG.COM (Sept. 19, 2016), https://www.asmag.com/showpost/21158.aspx [https://perma.cc/SQZ5-DWGD].

through the use of "distinct geometric characteristics of a person's facial features," such as the distance between their eyes or the same of their nose.[15] One-to-one facial recognition attempts to verify the identity of a specific individual using data within the system about that individual.[16] A common example of one-to-one recognition is the use of facial recognition to unlock a cell phone or computer.[17] One-to-one facial recognition is becoming increasingly popular as a security measure at airports and for border control to ensure people attempting to travel are who they say they are.[18]

There are two common types of errors in facial recognition—false negatives and false positives. When a false negative occurs, the system fails to realize that two identical faces are the same.[19] A false positive, on the other hand, is when a system inaccurately identifies two different faces as being identical.[20] Both of these errors can have severe consequences for the individual who is inaccurately identified, such as false arrests.[21]

b. Facial Recognition – Regulation and Legislation in the United States

Currently, there are no federal guidelines to standardize the use of facial recognition technology. Few states have enacted laws to regulate its use, leaving municipalities with significant leeway to decide what, if anything, to do about use of this technology within their jurisdictional limits.[22] The lack of a federal regulatory regime does not mean the federal government is unaware of the issue—there have been numerous proposals and bills drafted

15. Gladstone, *supra* note 6.

16. Seth Lazar, Clair Benn & Mario Günther, *Large-Scale Facial Recognition is Incompatible with a Free Society*, THE CONVERSATION (July 9, 2020, 3:59 PM), https://theconversation.com (search "Large-Scale Facial Recognition is Incompatible with a Free Society") [https://perma.cc/2TKT-QHB5].

17. Strom, *supra* note 14.

18. *See* Gladstone, *supra* note 6 ("US Customs and Border Protection announced in late August that new facial recognition technology that had been implemented just a few days earlier at the Washington Dulles International Airport was instrumental in identifying a man using false documents.").

19. PATRICK GROTHER, ET AL., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS, NISTIR 8280, 2 (Dec. 2019).

20. *Id.*

21. See discussion *infra* Part I.d.ii for further elaboration on the consequences of false identification by facial recognition technology.

22. *See* Metz, *supra* note 1.

in an attempt to solve the issue of a federal privacy scheme.[23] Indeed, the enactment of a "[f]ederal privacy law isn't a matter of if, it's a matter of when."[24]

For example, there have been numerous proposed bills to address the issue of facial recognition technology by both governmental and private entities at the federal level. In June 2020, the Facial Recognition and Biometric Technology Moratorium Act of 2020[25] was introduced by Senators Edward Markey and Jeff Merkley. The proposed legislation would have banned the use of facial recognition by federal agencies, and encouraged state and local police to follow suit by conditioning the receipt of federal grants on the passage of similar laws prohibiting facial recognition at the local level.[26] Even earlier, in March 2019, the Commercial Facial Recognition Privacy Act[27] was introduced before the Senate as a measure to protect consumers and regulate the commercial use of facial recognition.[28] This bill would have prohibited the collection, storage, or controlling of facial recognition data unless the entity explained the capabilities of the facial recognition technology, obtained consent, and gave explicit notice of the reasonably foreseeable uses of the data collected.[29] The bill defined facial recognition data as "any unique attribute or feature of the face of an end user that is used by facial recognition technology to assign a unique, persistent identifier or for the unique personal identification of a specific individual."[30] Senator Brian Schatz, the Democratic sponsor of the bill, argued that requiring consent would put control over data back into the hands of consumers.[31] This framework of

23. ONE TRUST, *Update About Proposed Federal Privacy Laws* (July 31, 2020), https://www.onetrust.com/blog/update-about-proposed-federal-privacy-laws/ [https://perma.cc/WA8S-D25R].

24. *Id.*

25. The Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2020).

26. *See* Kelly, *supra* note 5.

27. Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. § 3 (2019).

28. Taylor Hatmaker, *Bipartisan Bill Proposes Oversight for Commercial Facial Recognition*, TECH CRUNCH (Mar. 14, 2019, 6:25 PM), https://techcrunch.com/2019/03/14/facial-recognition-bill-commercial-facial-recognition-privacy-act/ [https://perma.cc/LPB9-U27K].

29. S. 847.

30. *Id.* § 2.

31. *See* Hatmaker, *supra* note 28 ("Our faces are our identities. They're personal. So the responsibility is on companies to ask people for their permission before they track and analyze their

requiring notice and consent can be seen in many of the proposed federal legislation for privacy more generally, such as the Consumer Online Privacy Rights Act (COPRA),[32] the Online Privacy Act, [33] and the Consumer Data Privacy and Security Act of 2020.[34] One of the most significant differences between the various proposed federal privacy law schemes, and of the utmost importance to the discussion in this Note, is the question of whether the proposed federal laws preempt privacy law at the state level. According to Peter Swire, a professor of law and leading expert in privacy, and Pollyanna Sanderson, a Policy Counsel at Future of Privacy Forum:

> [t]he political controversy is well known: Industry emphasizes the need for a uniform national law, while privacy advocates emphasize the role that states play in providing new protections for consumers. One major political question will be whether the federal law will preempt new and comprehensive state laws, such as the California Consumer Privacy Act or the similar Nevada legislation.[35]

Enacting legislation that allows for the preservation of state law innovation in the face of a federal regulatory scheme, such as COPRA,[36] is a necessary

---

faces . . . . Our bill makes sure that people are given the information and–more importantly–the control over how their data is shared with companies using facial recognition technology.").

32. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

33. Online Privacy Act, H.R. 4978, 116th Cong. (2019).

34. Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020).

35. Peter Swire & Pollyanna Sanderson, *A Proposal to Help Resolve Federal Privacy Preemption*, INT'L ASSOC. OF PRIV. PROS. (Jan. 12, 2020), https://iapp.org/news/a/a-proposal-to-help-resolve-federal-privacy-preemption/ [https://perma.cc/8LHF-KHV2].

36. *See* S. 2968 § 302(b) (2019).

> State Law Preservation.—Nothing in this Act shall be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements: (1) Consumer protection laws of general applicability such as laws regulating deceptive, unfair, or unconscionable practices. (2) Civil rights laws. (3) Laws that govern the privacy rights or other protections of employees, employee information, or students or student information. (4) Laws that address notification requirements in the event of a data breach. (5) Contract or tort law. (6) Criminal laws governing fraud, theft, unauthorized access to information or unauthorized use of information, malicious behavior, and similar provisions, and laws of criminal procedure. (7) Laws specifying remedies or a cause of action to individuals. (8) Public safety or sector specific laws unrelated to privacy or security.

step in allowing states and municipalities to enact laws that are more stringent than what a baseline federal privacy law might minimally require.[37]

One state has already taken up the task of enacting privacy legislation to protect its citizens against the use of facial recognition—Illinois. Right across the river from St. Louis, Illinois passed its Biometric Information Privacy Act[38] (BIPA) in 2008, becoming one of the first states to enact laws protecting biometric data.[39] BIPA does not prevent the collection of biometric data entirely, but requires notice and consent before such data can be collected.[40] The Illinois legislature found that biometric identifiers, which includes the facial scans necessary for facial recognition,[41] are uniquely vulnerable forms of data and in specific need of protection.[42] Biometrics, unlike other unique identifiers such as social security numbers, cannot be changed; "therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[43] The Act provides for a private right of action,[44] which makes it a uniquely important law in the realm of privacy protection.[45] Since BIPA was enacted in 2008, the law has been

---

Id.

37. *See id.* § 302(c) for an example of a federal law that allows for states to retain their higher levels of protection:

> Preemption Of Directly Conflicting State Laws.—Except as provided in subsections (b) and (d), this Act shall supersede any State law to the extent such law directly conflicts with the provisions of this Act, or a standard, rule, or regulation promulgated under this Act, and then only to the extent of such direct conflict. Any State law, rule, or regulation shall not be considered in direct conflict if it affords a greater level of protection to individuals protected under this Act.

38. 740 ILL. COMP. STAT.14/1 et. seq. (2008).

39. *See* Kristine Argentine & Paul Yovanic, *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*, JDSUPRA (June 9, 2020), https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/ [https://perma.cc/P5VM-38MA].

40. 740 ILL. COMP. STAT. 14/15 (2008).

41. For the full definition of biometric identifiers under the act, *see id.* § 10.

42. *Id.* § 5(c).

43. *Id.*

44. *Id.* § 20.

45. *See* Woodrow Hartzog & Neil Richards, *Getting the First Amendment Wrong*, BOS. GLOBE (Sept. 4, 2020, 3:03 AM), https://www.bostonglobe.com/2020/09/04/opinion/getting-first-amendment-wrong/ ("BIPA is the most important biometric privacy law in America because it allows people to sue companies directly for violations.").

successful in vindicating the privacy rights of Illinois residents regarding facial recognition technology and other biometric data.

There has been a surge in the number of BIPA lawsuits since the Illinois Supreme Court decided *Rosenbach v. Six Flags Entertainment Corporation*[46] in 2019.[47] Plaintiffs in privacy litigation often struggle to demonstrate an injury in fact sufficient to establish standing to sue,[48] but the Illinois Supreme Court eliminated this problem by holding that an individual need not have sustained actual damages beyond violation of his or her rights to seek relief pursuant to the Act.[49] Strong legal protection for biometric data can make it expensive for companies to flout regulations and impermissibly collect such data, as demonstrated by a recent BIPA suit against Facebook in which the company agreed to pay out a $650 million settlement to Illinois residents.[50] The lawsuit alleged that Facebook used facial recognition for the purposes of tagging individual users in photos without the users' consent in violation of BIPA.[51] This is but one example of how BIPA's private right of action has enabled citizens of Illinois to

46. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019).

47. *See* Richard R. Winter, Rachel C. Agius & William F. Farley, *BIPA Update: Class Actions on the Rise in Illinois Courts*, HOLLAND & KNIGHT (July 22, 2019), https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts [https://perma.cc/59QA-P2HN].

48. Priscilla Fasoro & Lauren Wiseman, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIV. (Dec. 7, 2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview/ [https://perma.cc/YT65-2Y2M] ("In the context of data breach litigation, plaintiffs may struggle to sufficiently allege many of these elements due to the nature of the data breach itself. For example, a plaintiff may face difficulties in demonstrating that a theft of their data resulted in an injury in fact, especially if the information has not yet been misused by a third party.").

49. *Rosenbach*, 129 N.E. 3d at 1207 ("Contrary to the appellate court's view, an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."). For more information on the *Rosenbach* holding and its impact on biometric privacy laws more broadly, see Chloe Stepney, *Actual Harm Means It Is Too Late: How* Rosenbach v. Six Flags *Demonstrates Effective Biometric Information Privacy Law*, 40 LOY. L.A. ENT. L. REV. 51 (2020).

50. *See Facebook Raises Settlement to $650 Million in Facial Recognition Lawsuit*, REUTERS (July 31, 2020, 3:49 PM), https://www.reuters.com/article/us-facebook-privacy-lawsuit/facebook-raises-settlement-to-650-million-in-facial-recognition-lawsuit-idUSKCN24W313 [https://perma.cc/9EEV-B83R].

51. *See id.*; *see also* Lauren Gurley, *If You Live in Illinois, Facebook Probably Owes you $400*, VICE (Sept. 24, 2020, 1:04 PM), https://www.vice.com/en/article/z3eam5/if-you-live-in-illinois-facebook-probably-owes-you-dollar400.

vindicate their rights under the act and protect their biometric data in Illinois courts.[52]

At the city level, Portland, Oregon set a new standard in privacy protection by being the first city to pass ordinances banning facial recognition by both public and private actors within the city's jurisdiction in September 2020.[53] The first ordinance[54] went into effect on September 9, 2020, banning Portland city bureaus from using facial recognition technology except in very limited circumstances, such as for verification purposes of bureau staff to access their own personal or city issued technological devices.[55] A second ordinance banning private entities from using facial recognition in places of public accommodation went into effect on January 1, 2021.[56] A place of public accommodation is defined as "[a]ny place or service offering to the public accommodations advantages, facilities, or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise," excepting private residences.[57] The Portland ban, like BIPA, provides a private right of action, stating that

> [a]ny person injured by a material violation of this Chapter by a Private Entity has a cause of action against the Private Entity in any court of competent jurisdiction for damages sustained as a result of the violation or $1,000 per day for each day of violation, whichever is greater and such other remedies as may be appropriate.[58]

In enacting the ordinance banning city governmental agencies from using facial recognition, the City of Portland was specifically concerned that use of facial recognition technology is especially harmful to people of color,

52. The issue of federal standing for BIPA cases that allege mere procedural violations, however, continues to evolve and is beyond the scope of this Note. For a further discussion on how federal courts have dealt with this issue, *see* Michael McMahon, *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts*, 65 ST. LOUIS U.L.J. 897 (2021).

53. Metz, *supra* note 1.

54. PORTLAND, OR., Ordinance 190112 (Sept. 9, 2020).

55. Press Release, The City of Portland, City Council Approves Ordinances Banning Use of Face Recognition Technologies by City of Portland Bureaus and by Private Entities in Public Spaces (Sept. 9, 2020), https://www.portland.gov/smart-city-pdx/news/2020/9/9/city-council-approves-ordinances-banning-use-face-recognition [https://perma.cc/2XXT-JXCR].

56. *Id.*

57. PORTLAND, OR., CITY CODE ch. 34 § 10.0020 (2021).

58. *Id.*

stating that an "emergency exists because of the need to respond to the immediate concerns of Black, Indigenous and People of Color (BIPOC) and to center the safety and well-being of BIPOC communities."[59] Ted Wheeler, the mayor of Portland, reiterated the importance of these ordinances for protecting BIPOC, stating that such measures were "necessary" until there is "more responsible development of technologies that do not discriminate against Black, Indigenous and other people of color."[60]

The numerous proposed federal regulatory schemes, current state laws, and city-wide bans concerning facial recognition and data privacy more generally show that there is a real concern among the American people that their data, particularly biometric data, be protected by law from inappropriate collection and use. This concern is well founded, as the next two subsections will discuss the prevalence of facial recognition use in the United State at large and in St. Louis specifically.

c. Use of Facial Recognition Technology

i. Current Uses of Facial Recognition in the United States

Right now in the United Sates, facial recognition technology is used in privately owned spaces such as stores and airports, in public spaces such as parks, and in law enforcement departments to track, observe, and identify individuals in real-time.[61] As Nicole Ozer, the Technology and Civil Liberties Director for the ACLU of Northern California, argues: "[f]ace recognition technology gives governments the unprecedented power to spy on us wherever we go."[62] The use of facial recognition technology by law enforcement departments is increasing rapidly. According to the Georgetown Law Center on Privacy and Technology, by 2016 more than one in four American state and law enforcement agencies had access to

59. PORTLAND, OR., Ordinance 190112 (Sept. 9, 2020).
60. Press Release, *supra* note 54.
61. Selinger & Woodrow, *supra* note 13.
62. Karen Weise & Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html [https://perma.cc/CM83-EXAN].

facial recognition software.[63] For example, Clearview AI developed a facial recognition software available to police departments for purchase.[64] The application allows an officer to plug in a picture of an individual and identify them through facial recognition technology.[65] The software depends on a database of billions of images Clearview has scraped from social media platforms such as Facebook and YouTube, which enables it to identify given individuals.[66] Scraping user images from social media sites is prohibited by many of the sites' terms of service, but Clearview continues the practice.[67] Clearview has declined to provide a specific list of law enforcement offices that have access to the technology, but the company stated that more than six hundred law enforcement agencies utilized their software as of February 2020.[68]

Law enforcement agencies are not the only entities proliferating the use of facial recognition. Private businesses employ facial recognition technology for a wide variety of uses as well. For example, Clearview AI's technology has been licensed to a number of private companies for security purposes.[69] Covergirl uses facial recognition to facilitate virtual makeup testing through its Custom Blend App.[70] Rite Aid has facial recognition systems installed in over two hundred of their stores, largely in lower-income, non-white neighborhoods.[71] Schools across the country use facial

63. Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, *The Perpetual Line Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/L5RU-HS7U].

64. Angie Ricono & Bill Smith, *Some Metro Police Departments Considering Controversial Facial Recognition Tech*, KCTV 5 NEWS (Feb. 12, 2020), https://www.kctv5.com/news/investigations/some-metro-police-departments-considering-controversial-facial-recognition-tech/article_f02192c0-4e0b-11ea-bac3-dfb4120b43b7.html [https://perma.cc/F3B2-LRST].

65. *Id.*

66. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/SJ4J-US89].

67. *Id.*

68. *Id.*

69. *Id.*

70. Amanda Cosco, *Cover Girl Launches AI-Driven Customization App*, WWD (Feb. 6, 2017), https://wwd.com/beauty-industry-news/color-cosmetics/cover-girl-launches-ai-driven-customization-app-10777590/ [https://perma.cc/27S6-G5AU].

71. Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, REUTERS (July 28, 2020, 11:00 AM), https://www.reuters.com/investigates/special-report/usa-riteaid-software/ [https://perma.cc/96J2-CS9R].

recognition for security purposes.[72] Facial recognition in schools is not a new phenomenon—as early as 2007, a school district in Nashville, Tennessee installed facial recognition in its buildings.[73] Use of this technology, however, has evolved from purely security purposes to more intrusive uses. For example, a New York Company has developed a facial recognition software called EngageSense, which applies algorithms to interpret students' levels of engagement in the classroom.[74] Airports have begun implementing facial recognition and other biometric technology in the boarding process, potentially leading the way for the obsolescence of boarding passes and ID checks.[75] As the aforementioned examples demonstrate, facial recognition has become deeply embedded in both private and public institutions in the United States.

ii. Facial Recognition in St. Louis

There are few limitations in place on the use of facial recognition technology in the city of St. Louis, or in Missouri more broadly. The St. Louis Metropolitan Police Department headquarters features a Real Time Crime Center (RTCC), providing a hub for all of the city's surveillance technology.[76] From the time it became operational in 2015, there have been "inadequate" privacy policies regarding access to and storage of the surveillance footage.[77] Alicia Hernandez, St. Louis resident and community organizer for the ACLU of Missouri, remarked that:

> since the launch of the Real Time Crime Center, St. Louis' embrace of surveillance technologies has felt more like a

72. *See* Nila Bala, *The Danger of Facial Recognition in Our Children's Classrooms*, 18 DUKE L. & TECH. REV. 249, 249–50 (2020).

73. Christine Byers, *St. Mary's High School Adds Facial Recognition Locks*, ST. LOUIS POST-DISPATCH (Mar. 9, 2015), https://www.stltoday.com/news/local/crime-and-courts/st-marys-high-school-adds-facial-recognition-locks/article_db488bb5-44f2-5301-b131-8a7ebe04bba9.html.

74. Bala, *supra* note 72.

75. *See* Francesca Street, *How Facial Recognition is Taking Over Airports*, CNN (Oct. 8, 2019), https://www.cnn.com/travel/article/airports-facial-recognition/index.html [https://perma.cc/JJ2Z-VFAW].

76. Rebecca Rivas, *Surveillance Privacy Bill Advances on Heels of Spy-Plane Resolution*, ST. LOUIS AM. (Jul. 15, 2020), http://www.stlamerican.com/news/local_news/surveillance-privacy-bill-advances-on-heels-of-spy-plane-resolution/article_82172078-c6de-11ea-9572-bf592da26c17.html [https://perma.cc/QJZ6-N78Y].

77. *See id.*

> runaway train. There is no existing oversight, and no agreed upon framework for uses of surveillance technologies, which are permissible and which are not.[78]

St. Louis Alderman John Collins-Muhammad introduced legislation in 2017, 2018, and 2019 that would have given the Board of Aldermen oversight of any surveillance technology that law enforcement agencies deploy in the city,[79] but as of March 2022, there is no indication any of these bills were enacted.

In July 2020, Board Bill 95 was introduced by Alderwoman Annie Rice—another attempt to regulate the use of surveillance technology, including facial recognition, by the city government of St. Louis.[80] The bill would increase oversight by requiring that the Board approve specific surveillance technologies as well as their uses, rules, regulations, and guidelines before they could be utilized, and creating opportunity for public input.[81] The purpose of the bill is to "ensure that City Entities only use surveillance technologies for the benefit of the public's safety and welfare, and [to] implement affirmative measures to ensure such uses do not infringe upon the public's or individuals' civil rights and liberties."[82] According to the ACLU of Missouri, there are already over 1100 surveillance cameras in St. Louis, and the city of St. Louis has spent over $4 million increasing surveillance technology in the last several years.[83] While the RTCC does not currently utilize facial recognition technology, it would be "technically easy" to overlay facial recognition technology to cameras already installed throughout the city.[84] Board Bill 95 would not prevent this use of facial recognition, but merely would require oversight from the Board of Alderman.[85]

---

78. *Id.*

79. *See* Jackie Snow, *Communities Come Face-to-Face with the Growing Power of Facial Recognition Technology*, PBS (Dec. 9, 2019), https://www.pbs.org/wgbh/nova/article/growing-power-facial-recognition-technology/ [https://perma.cc/JTM6-QAW5].

80. CITY OF ST. LOUIS, MO. Board Bill 95 (2020).

81. *Id.*

82. *Id.* § 2.

83. ACLU MISSOURI, *Community Control Over Police Surveillance in St. Louis, Board Bill 95*, https://www.aclu-mo.org/en/community-control-over-police-surveillance [https://perma.cc/M8V3-LWFD].

84. Snow, *supra* note 79.

85. *See* CITY OF ST. LOUIS, MO. Board Bill 95 (2020).

In 2017, Missouri Representative Jeff Pouge introduced a bill before the Missouri House that would modify an existing statute[86] to prohibit Missouri school districts from collecting biometric information—including facial characteristics—of students without the written consent of their parents or legal guardians.[87] However, as of March 2022 there has been no indication this bill was enacted into law.[88] Despite these aforementioned efforts to regulate surveillance, facial recognition, and biometric data collection, there remains little regulation on the books regarding these practices.

Notwithstanding the lack of oversight regarding its use, facial recognition software has been and continues to be utilized in the city every day. Blue Line Technology, a St. Louis-based facial recognition software company founded by retired St. Louis police officers,[89] has been in use in several private and public buildings in St. Louis—including schools.[90] St. Mary's High School, located in St. Louis, was the first school in the country to use Blue Line Technology's facial recognition program.[91] The one-to-one system requires that each individual who wants to enter the building must stand in front of the camera, and if there is not a match to a student or staff member in the system, the doors will not open.[92] A handful of St. Louis stores use Blue Line's facial recognition software for security, such as a 7-

86. MO. REV. STAT. § 161.096 (2014).

87. H.B. 201, 99th Gen. Assemb., 1st Reg. Sess. (Mo. 2017) ("School districts shall not collect biometric information on any student without the express written consent of the student's parent or legal guardian. For purposes of this section, 'biometric information' means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, including fingerprints, retina and iris patterns, voice prints, DNA sequence, newborn screening information, facial characteristics, and handwriting.").

88. *See* 99TH GENERAL ASSEMBLY, 1ST REGULAR SESSION HB 201, https://house.mo.gov/BillContent.aspx?bill=HB201&year=2017&code=R&style=new [https://perma.cc/CHD7-UKKB].

89. Blue Line's facial recognition software is not only used in St. Louis, but also has been purchased by schools and businesses around the United States. One such purchaser was Jackson Food Stores in Portland, Oregon—a city that has subsequently banned such stores from employing the technology. As a result of the ban, software like Blue Line's cannot be used by stores within the city. *See* Kate Kay, *This Facial Recognition System Was Built By Former St. Louis Police Officers*, REDTAIL (July 21, 2020), https://redtailmedia.org/2020/07/21/this-facial-recognition-system-was-built-by-former-st-louis-police-officers/ [https://perma.cc/S6G3-QTDQ].

90. Lauren Trager, *Local Former Cops Create Facial Recognition Technology to Fight Crime, but Critics Are Concerned*, KMOV4 (May 15, 2019), https://www.kmov.com/news/local-former-cops-create-facial-recognition-technology-to-fight-crime-but-critics-are-concerned/article_e7694d3a-7689-11e9-ab41-939fb5bbfa86.html [https://perma.cc/L679-YY2Z].

91. *Id.*

92. *Id.*

Eleven on Kingshighway.[93] The store reported that within the first year of installation, crime at the store was reduced by ninety-eight percent.[94]

As early as 2014, the St. Louis Circuit Court piloted Blue Line's software, using it to flag any individuals deemed to pose a threat and prevent their entrance into the building.[95] The desire to prevent violence in courthouses—fueled by dangerous situations like James Palmer firing seventy rounds in an Arkansas courthouse—spurred the implementation of such software.[96] Although the potential for increased safety is a possible benefit, the use of facial recognition at courthouses generates concern. In response to the pilot program, Jeffry Mittman, Executive Director of the ACLU of Missouri, expressed apprehension toward targeting individuals with this technology and the criteria to be considered a threat for such targeting and flagging.[97] He found the very idea of preventing access to the courts inherently problematic, stating, "the courthouses are public buildings that belong to the people . . . . To test something that has the potential to keep the public out is very concerning."[98]

d. Concerns about Facial Recognition

i. Constitutional Concerns

While the potential for increased security and crime-solving capabilities might make facial recognition appear desirable, it is necessary to consider what is at stake when private and public entitles implement this technology. Increased surveillance capabilities inhibit privacy, which, for many, can be too high a cost. Timothy Birch, Police Services Manager for the Oakland Police Department, expressed his discomfort regarding the implementation of facial recognition in 2018—"we don't see the benefit of facial recognition software in terms of the cost, the impact to community privacy . . . . Until we identify an incredible benefit for facial recognition,

93. *Id.*
94. *Id.*
95. Jennifer Man, *St. Louis Courthouse Becomes Test Site for Facial Recognition Security Program*, GOV'T TECH. (Feb. 24, 2014), https://www.govtech.com/public-safety/St-Louis-Courthouse-Becomes-Test-Site-for-Facial-Recognition-Security-Program.html [https://perma.cc/5KMC-BTSG].
96. *Id.*
97. *Id.*
98. *Id.*

the cost is just too high."[99] One year later in 2019, Oakland would become the third American city to ban facial recognition in public places.[100]

The effects of facial recognition on individual privacy implicate important constitutional concerns, particularly with respect to the First and Fourth Amendments. There are currently no Supreme Court cases that indicate how the court might apply the First or Fourth Amendment to the use of facial recognition by law enforcement or other governmental agencies,[101] but it is not difficult to supply reasons why such technology might impinge on constitutional rights. Selinger and Hartzog argue that

> [t]he technology can be used to create chill that routinely prevents citizens from engaging in First Amendment protected activities, such as free association and free expression. They could also gradually erode due process ideals by facilitating a shift to a world where citizens are not presumed innocent but are codified as risk profiles with varying potentials to commit a crime.[102]

Along that vein, Jeramie Scott remarked that facial recognition signals "a change and a shift that undermines our democracy, because everyone becomes suspicious."[103] One can easily imagine how facial recognition might affect freedom of expression or assembly—police use of facial recognition during the summer 2020 protests in response to police brutality against Black Americans provides a stark example. Throughout the tumultuous summer, multiple instances of police using facial recognition to track and arrest protesters were reported by news stations.[104] There has been

---

99. Jon Schuppe, *Facial Recognition Gives Police a Powerful New Tracking Tool. It's also Raising Alarms*, ABC NEWS (July 30, 2018, 3:08 AM), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936 [https://perma.cc/9AVP-FH3B].

100. Caroline Haskins, *Oakland Becomes Third U.S. City to Ban Facial Recognition*, VICE (July 17, 2019, 6:41 AM), https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz [https://perma.cc/LG5X-Y4US].

101. Garvie, Bedoya & Frankle, *supra* note 63, at 16.

102. Selinger & Hartzog, *supra* note 13, at 43.

103. Trager, *supra* note 90.

104. *See* Connie Fossi & Phil Pranzan, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC MIAMI (Aug. 7, 2020, 7:14 PM), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/ [https://perma.cc/P5R8-UH6U]; *see also* James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activists*, VERGE (Aug. 18, 2020, 5:26 AM),

a long history of using surveillance on social activists, especially Black activists, going back to the Civil Rights activists of the 1960s.[105] Facial recognition technology makes the tracking of political activists easier than ever before, meaning that people could become less comfortable partaking in constitutionally protected activities for fear of retribution from state authorities. Some facial recognition software companies argue that the First Amendment protects and justifies their facial recognition business.[106] According to Neil Richards and Woodrow Hartzog, however, this is a perversion of what the First Amendment is meant to protect and not an accurate interpretation of the law. The authors argue that:

> [t]he core of the First Amendment's commitment to free speech is protecting individual speakers like protestors and journalists form government oppression, not giving constitutional protection to dangerous business models that inhibit expression and give new authoritarian tools to governments.[107]

The increasing use of facial recognition in public and private spaces likewise threatens a core tenant of the Fourth Amendment. The Fourth Amendment was written largely in response to the British Crown's use of Writs of Assistants, general warrants that allowed generalized, suspicionless searches of Colonists homes.[108] The Fourth Amendment is meant to prevent such unreasonable searches, but according to a report from the Georgetown Law Center on Privacy and Technology, different uses of facial recognition present a range of threats to these Fourth Amendment rights.[109] The types of practices deemed to pose a "moderate risk" to Fourth Amendment protections involve circumstances where police employ a targeted search with a targeted database, and thus are "conducting a targeted search pursuant to a particularized suspicion."[110] The risk increases the

---

https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram [https://perma.cc/C9QP-VZEA].

105. *See* Malkia Devich-Cyril, *Defund Facial Recognition*, ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ [https://perma.cc/E3GB-RDV5].

106. *See* Hartzog & Richards, *supra* note 45.

107. *Id.*

108. Garvie, Bedoya & Frankle, *supra* note 63, at 16.

109. *Id.* at 17–18.

110. *Id.* at 19.

more generalized a database becomes—for example, a law enforcement agent attempting to identify a suspect can perform face recognition searches against the photos of every registered driver in a state database to find a match, thus creating "a virtual line-up of millions of law-abiding Americans" who are often unaware how their personal data is being used.[111] The risk to Fourth Amendment protections is at its highest level when facial recognition technology is applied to real-time or historical surveillance of the general public, enabling law enforcement to conduct indiscriminate and instantaneous searches of any individuals that happens to walk down the street.[112]

The ability of law enforcement to utilize new technology in the name of stopping crime has been both protected and prevented by the Supreme Court.[113] An example of the court protecting novel police crime solving methods includes the 1971 case *United States v. White*, where the Court held that a police informant using a concealed recording device to record conversations did not require a warrant for such surveillance nor violate the Fourth Amendment.[114] Even with the limited technology available at the time, some members of the court recognized the danger this holding could pose to all Americans. In his dissent, Justice Douglas cautioned: "Today no one perhaps notices because only a small, obscure criminal is the victim. But every person is the victim, for the technology we exalt today is everyman's master." [115] Douglas' words ring true today; with facial recognition, it is not only the "obscure criminal" whose privacy and constitutional rights are at stake. According to the Georgetown Law Center report, by 2016, *half* of all U.S. adults—117 million people—were already included in police facial-recognition data bases, many of whom are law-abiding citizens.[116] Although facial recognition comes with the potential benefits of increased security and crime prevention, the potential detriment to First and Fourth Amendment rights is too high a price to pay.

111. *Id*. at 19–20.

112. *Id*. at 18, 22.

113. *Compare* California v. Ciraolo, 476 U.S. 207, 207 (1968) (holding that aerial surveillance of the curtilage of defendant's home was not a search within the meaning of the Fourth Amendment), *with* Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018) (holding that accessing ones location data over the course of several days through cellphone records was a search within the meaning of the Fourth amendment).

114. United States v. White, 401 U.S. 745, 745 (1971).

115. *Id*. at 757 (Douglas, J., dissenting).

116. Garvie, Bedoya & Frankle, *supra* note 63, at 1–2.

ii. Bias and False Matches in Facial Recognition

A second major concern is the existing bias within facial recognition technology, particularly when it comes to people of color. In response to "assertions that demographic dependencies could lead to accuracy variations and potential bias,"[117] the National Institute of Standards and Technology (NIST) conducted research to quantify the accuracy of facial recognition algorithms for demographic groups defined by sex, age, and race.[118] The 2019 report confirmed what many had already believed to be true—facial recognition algorithms are susceptible to both racial and gender bias. The study revealed that Asian and African American individuals are up to one hundred times more likely to be misidentified than white men, and that Native Americans had the highest false-positive rate of all ethnicities.[119] Overall, false positives were higher for women than for men.[120] The compounded bias toward women and people of color leave women of color in a particularly vulnerable position when facial recognition technologies are utilized. According to NIST's findings, "[t]he faces of African American women were falsely identified more often in the kinds of searches used by police investigators where an image is compared to thousands or millions of others in hopes of identifying a suspect."[121] Rep. Bennie G. Thompson, chairman of the Committee on Homeland Security, stated that the report revealed that "facial recognition systems are even more unreliable and racially biased than we feared."[122]

False matches can have serious consequences—according to Jay Stanley, a policy analyst for the ACLU, "[o]ne false match can lead to missed flights, lengthy interrogations, tense police encounters, false arrests, or worse."[123] Such a result occurred in January 2020, when Detroit police

117. GROTHER, *supra* note 19, at 1.

118. *Id.*

119. Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 5:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use [https://perma.cc/R9QQ-SWTR].

120. GROTHER, *supra* note 19, at 2.

121. Harwell, *supra* note 119.

122. *Id.*

123. *Id.*

arrested Robert Julian-Borchak Williams for a crime he did not commit.[124] Detectives ran grainy footage from security videos through facial recognition software after a retail store was robbed; the software incorrectly identified the man in the footage to be Williams, who was subsequently arrested.[125] He spent thirty hours in a jail cell before being released on bond, and ultimately all charges were dropped due to insufficient evidence.[126] Williams' experience received media attention due to its novelty, being potentially the first known account of a wrongful arrest based on a false match by facial recognition software in the United States.[127]

Law enforcement is often adamant that facial recognition is just one tool to identify suspects, but it is difficult to be certain how large of a role facial recognition plays in an investigation, given that police do not often reveal whether facial recognition technology was utilized in an investigation.[128] According to former Solicitor General of the United States Paul Clement, who was hired by Clearview AI, law enforcement "don't have to tell defendants that they were identified via Clearview's technology as long as it isn't the sole basis for getting a warrant to arrest them."[129]

While false matches are particularly a concern for people of color due to the racial bias present in in many of the algorithms used today,[130] errors in facial recognition technology are a serious concern for people of all races, ages, and genders. In 2018, civil liberties groups in the United States tested Amazon's facial recognition software, Amazon Rekognition, which had already been utilized by various police departments and organizations across the country.[131] The test compared the photos of all federal lawmakers

---

124. Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led To False Arrest Of Black Man*, NPR (June 24, 2020, 8:00 AM), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/FNE7-LV7C].

125. *Id.*

126. *Id.*

127. *See, e.g.*, Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/G5LV-ZZPV].

128. *See* Allyn, *supra* note 123 ("Most of the time, people who are arrested using face recognition are not told face recognition was used to arrest them.").

129. Hill, *supra* note 66.

130. *See generally* GROTHER, *supra* note 19.

131. *See* Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, N.Y. TIMES (July 26, 2018), https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html [https://perma.cc/U4AR-ZYME].

against a database of 25,000 mugshots.[132] The software mismatched twenty-eight members of Congress in total, incorrectly identifying them as individuals featured in the mugshot photos.[133] Furthering concerns about racial bias, Black and Latino members of Congress were disproportionately identified as the individuals in the mug shot—for example, the late Representative John Lewis was incorrectly identified.[134] Two years later in June 2020, Amazon would announce a one-year moratorium on police use of Rekognition.[135] The short blog post did not give an explanation for the reasoning behind the sudden pause on the use of the software, other than to say that it "might give Congress enough time to implement appropriate rules" regarding the ethical use of facial recognition technology.[136]

Larger databases, such as Clearview AI's database with billions of photos, increase the risk that misidentification will occur due to the doppelgänger effect.[137] Doppelgängers "usually refer to biologically unrelated lookalikes. Apart from demographic attributes, doppelgängers also share facial properties such as facial shape."[138] Studies have indicated that automatic facial recognition algorithms can fail to distinguish lookalikes, which "may lead to serious risks in various scenarios, *e.g.* blacklist checks, where innocent subjects may have a higher chance to

132. *Id.*

133. *Id.*

134. *Id.*

135. *We Are Implementing a One-Year Moratorium on Police Use of Rekognition*, AMAZON (June 10, 2020), https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition [https://perma.cc/ZA9N-B6HF].The moratorium on the facial recognition software would not apply to organizations such as the International Center for Missing and Exploited Children, which use the product to help find trafficking victims and missing children. *Id.*

136. *See id*. Amazon is not the only company to take steps to put a pause on their facial recognition software—IMB likewise said it would stop selling facial recognition products in June 2020. *See* Hannah Denham, *IBM's Decision To Abandon Facial Recognition Technology Fueled By Years Of Debate*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/ [https://perma.cc/8NVF-G8RV]. The prior summer in June 2019, Axon, a leading maker of police body cameras in the United States, banned the use of facial recognition software on its devices due to ethical concerns that such software is not sufficiently reliable. *See* Charlie Warzel, *A Major Police Body Cam Company Just Banned Facial Recognition*, N.Y. TIMES (June 27, 2019), https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html [https://perma.cc/D65U-F6L5].

137. Hill, *supra* note 66.

138. Christian Rathgeb et al., Impact of Doppelgangers on Face Recognition: Database and Evaluation, at 2 (2021 International Conference of the Biometrics Special Interest Group), https://dl.gi.de/bitstream/handle/20.500.12116/37454/biosig2021_proceedings_02.pdf?sequence=1&isAllowed=y [https://perma.cc/ZGC3-SF78].

match to a lookalike in the list."[139] The reality is that technology is not fool-proof, and we cannot expect it to be. As Nila Bala, Associate Director of Criminal Justice Policy and Civil Liberties at R Street Institute, articulates, "[t]echnology is seen as immune to the racial biases that humans possess, and individuals view artificial intelligence with blind faith. But artificial intelligence is only as smart as the data used to develop it."[140]

II. ANALYSIS AND PROPOSAL

As the prior sections show, the use of facial recognition technology is pervasive throughout the United States and within the St. Louis community, and there are serious concerns about these uses in our schools, in our stores, and in our communities more generally. Although some states and cities have taken it upon themselves to regulate the use of facial recognition and biometric data more generally, there is no federal privacy scheme and no protection at the state or local level for the citizens of St. Louis. Permitting such unrestricted use of facial recognition technology creates privacy and constitutional concerns that cannot continue to be ignored.

The current uses of facial recognition in St. Louis pose a serious risk to freedom of expression, freedom of assembly, and freedom from unreasonable searches. Facial recognition technology makes it easier than ever before to target protesters and to keep certain individuals out of stores or public buildings such as courthouses. The chilling effect of knowing that one can be identified and flagged by law enforcement may prevent people from associating with certain individuals, visiting certain locations, or attending demonstrations. While the current uses of facial recognition throughout the city may seem sporadic, as previously stated, the countless surveillance cameras around the city could easily be converted to support facial recognition technology, [141] enabling real-time surveillance and identification of unsuspecting people all over St. Louis. Such real-time identification capabilities threaten the Fourth Amendment rights of all citizens.[142]

139. *Id.*
140. Bala, *supra* note 72, at 258–59.
141. Snow, *supra* note 79.
142. Garvie, Bedoya & Frankle, *supra* note 63, at 16–18.

Furthermore, the continued spread of facial recognition technology amplifies concerns over racial bias within the algorithms it relies upon. According to 2019 United States Census Bureau estimates, 45.3% of the population of the City of St. Louis identifies as Black or African American.[143] Even if the constitutional concerns raised above could somehow be adequately addressed, it is simply unacceptable for businesses, schools, and city officials in St. Louis to rely on or expand the use of facial recognition despite clear evidence that it is less accurate when identifying people of color.[144] Nearly half of the population of the city is at serious risk of inaccurate identification that can lead to denial of services, unnecessary searches, and inaccurate arrests.[145] The city has been unsuccessful thus far in passing adequate privacy legislation to address the surveillance technologies already in place,[146] generating little confidence that the city will pass meaningful legislation to prevent the abuse of future increases in surveillance made possible by the growth of facial recognition. So long as the software itself remains riddled with biases against people of color, there is no amount of oversight that could adequately protect all citizens equally from facial recognition.

Given the significant threat that facial recognition technology poses to the constitutionally protected liberties of all St. Louis citizens, and the even greater threat posed specifically to people of color, the city should ban facial recognition technology. It is true that there are potential benefits to the use of facial recognition technology, especially when it comes to law enforcement and security. However, the use of such technology does not actually solve the underlying issues in society, it merely moves the target. While some stores may enjoy a decrease in robberies, the fundamental social problems contributing to crime go ignored. As Jeramie Scott, Senior Counsel at the Electronic Privacy Information Center, argues, "[y]ou are implementing a technology that pushes us closer to a total surveillance state, and it's a technology that actually doesn't address the underlying issues."[147] As a society, we often look toward technology to provide easy solutions to

143. *QuickFacts St. Louis City, Missouri*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/stlouiscitymissouri/PST045219 [https://perma.cc/Y9VS-YZQW].

144. *See* GROTHER, *supra* note 19, at 2.

145. *See* Harwell, *supra* note 119.

146. *See* Rivas, *supra* note 76; *see also* Snow, *supra* note 79.

147. Trager, *supra* note 90.

the problems that plague us—but quick fixes seldom deliver on their lofty promises, and can obscure the root cause for why we looked for a fix in the first place. Indeed, "[p]atching social problems with technological solutions is easier than mustering the will to solve harder issues around inequality, education, and opportunity. The drumbeat of security stokes fear."[148] Increased surveillance through facial recognition does not ultimately serve our communities, but rather puts a Band-Aid on some of our deepest wounds while simultaneously opening up new ones.

Like Portland, St. Louis should institute a ban of facial recognition technology by both private and public entities through city ordinances. Because of the lack of a federal regulatory scheme, there is an opportunity at the local level to make sweeping reform. In the face of an abdication on the part of both the federal government and the state government of Missouri to pass necessary laws to protect the citizens of St. Louis, the city itself must take action. Attempts to regulate existing surveillance in the city have been met with failure, painting a bleak picture of the invasions of privacy and deprivations of constitutional rights that may occur if facial recognition technology continues and proliferates in the city without action. Cities, such as Portland, Oregon have seen the writing on the wall and have taken the necessary steps to protect their citizens from the dark side of facial recognition. St. Louis should likewise seize the opportunity to ban facial recognition before its presence becomes even more entrenched within its boundaries.

Additionally, in order for such a ban to be effective, there should be a private right of action for citizens whose rights are violated in contradiction to the ban. As discussed previously, the inability to point to a concrete harm is often a barrier to redress of privacy violations.[149] A ban will only be successful in vindicating the rights of St. Louis citizens if the procedural violation of the ordinance constitutes an injury in fact, so that there is no need for an additional harm to establish standing. In making a violation of the facial recognition ban satisfactory to pursue the private right of action, St. Louis can demonstrate a commitment to the idea that the unlawful use of one's unique facial data is a harm by its very nature.

148. Selinger & Hartzog, *supra* note 13, at 112.
149. *See* Fasoro & Wiseman, *supra* note 48.

CONCLUSION

The city of St. Louis should follow in the footsteps of Portland, Oregon[150] and ban the use of facial recognition technology by both private and governmental entities. This Note has charted the various uses of facial recognition in the United States broadly and in St. Louis itself. Facial recognition has bled into every part of our lives, from our cell phones, to airports, to schools, to law enforcement—facial recognition can be seen everywhere. Attempts to legislate and regulate facial recognition in the United States have resulted in some impressive laws that offer sweeping protections for citizens, such as BIPA, but most have been unsuccessful, inadequate, or both. The legislative failures to pass meaningful safeguards against the collection of biometric data through facial recognition in St. Louis and Missouri provide stark examples. Right now, there are essentially no protections in place to protect those living in St. Louis from the harms posed by facial recognition.

The utilization of facial recognition threatens essential First and Fourth Amendment rights. So long as unfettered use of facial recognition continues and grows, the likelihood that people will feel as if they can no longer protest, assemble, or otherwise openly and publicly express themselves will increase. Failure to take action now could increase the risks associated with facial recognition and result in the sweeping, real-time identification of anyone, anywhere through cameras installed all over the city. Decisive action is needed to guarantee freedom of expression, freedom of speech, and freedom from unreasonable search.

Troubling biases and inaccuracies also occur when facial recognition software is implemented. Many people like to believe that science and technology are always impartial, but the facial recognition software Americans increasingly rely is only as reliable and infallible as the people who create it. Unfortunately, the racial biases present in our society likewise plague the data that drives facial recognition software. As a result, people of color are at a greater risk of suffering from the inaccurate aspects of facial recognition, including false positive and false negative identification. Due to the large population of people of color in St. Louis, it is especially imperative that the city take this step to ban facial recognition. Allowing

150. *See* Metz, *supra* note 1.

both private and governmental entities to use facial recognition unfairly disadvantages almost half of the population of the city, who can never be confident that they will not be wrongly identified so long as the software fails to identify people of color accurately at disproportionate rates. Mere regulation or oversight of such a flawed technology will never be enough to guarantee equal protection for all citizens of St. Louis. A ban of facial recognition by both governmental and private entities is a necessary step toward protecting the rights of all members of the St. Louis community.