The Legal Implications of Sexual Orientation-Detecting Facial Recognition Technology

Phillip H.C. Wilkinson

Abstract

Facial recognition technology now has the proven power to publicly out those in the LGBTQ community with a high level of accuracy.[1] A 2018 Stanford study highlights the relative ease with which computer coders can produce these algorithms.[2] While no publicly available sources have proven that sexual orientation-detecting facial recognition technology is currently being put to use, the Stanford study proves that it is possible and serves as a call for regulation anticipating this possibility.

Various public and private entities are already putting facial recognition technology to use. This type of artificial intelligence will only become more sophisticated as a result. Facial recognition technology, should it be developed to target the LGBTQ community, could have significant implications for gay, lesbian, bisexual, and transgender individuals in many areas of their lives. We must adapt our system of legal protections for the LGBTQ community to anticipate the consequences of this technology and enact new regulations to protect against its harms.[3]

This is the first Note of its kind to address the legal challenges that facial recognition artificial intelligence technology presents to the LGBTQ community. This is a new technology that implicates many bodies of law. This Note analyzes caselaw, statutes, and administrative rulings at both the

[1] Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images*, 114 J. Personality & Soc. Psychol. 246, 246–57 (2018).

[2] *Id.* at 255.

[3] This Note frequently refers to the LGBTQ community inclusively because the effects of facial recognition technology will have an impact on all members of the community. As discussed below, however, the Wang and Kosinski study only analyzed lesbian and gay individuals. Therefore, in-depth discussions of the unique challenges that bisexual and transgender individuals may face with regard to this technology are beyond the scope of this Note. Notwithstanding that limitation, artificial intelligence technology could develop in ways that more directly target bisexual and transgender individuals using similar methods to those seen in the Wang and Kosinksi study. For that reason, it is important for regulators, activists, and scholars to consider the LGBTQ community as a whole. Where relevant, this Note attempts to highlight areas where issues unique to bisexual and transgender individuals arise.

state and federal level that could become relevant in deciding LGBTQ-related disputes caused by this technology. This Note spots relevant legal issues in the realms of employment discrimination, privacy rights, and constitutional jurisprudence to help the LGBTQ community protect the rights, dignity, and equal treatment of its members. These areas are not meant to be an exhaustive list of issues surrounding use of this new technology. Instead, this Note aims to start a legal conversation about some of the technology's most pressing anticipated impacts on the LGBTQ community.

About the Author

Stanford Law School, J.D. 2021; MPhil, University of Cambridge; B.A., Yale College. I am indebted to many professors and peers at Stanford Law School who supported me during the initial drafting of this note. I want to thank Jane Schacter for allowing me to explore this topic as my research paper for her seminar on sexual orientation and gender identity law. I am also deeply grateful to Mariano-Florentino Cuéllar for introducing me to many cutting-edge developments in facial recognition technology during his class on regulating artificial intelligence. Pam Karlan provided me with invaluable insights into civil rights litigation and the landscape of LGBTQ legal protections. Michal Kosinski kindly discussed his research findings and methods with me. Andrew Lubash provided helpful feedback and welcome encouragement before I submitted my work for publication. I would like to extend my gratitude to all the editors and advisors of the *Dukeminier Awards Journal*. Luis Vasquez, Skyler Ross, Emily Owen, AK Shee, and Matt Gardner in particular provided substantive and thoughtful feedback, which enhanced my arguments. Finally, I want to thank my friends and family for supporting me throughout my educational and professional journey. I dedicate this note to those in the LGBTQ community who have faced invidious discrimination in their pursuit of happiness.

Table of Contents

> "There is something fatal about a portrait. It has a life of its own."
> –Oscar Wilde, *The Picture of Dorian Gray*

Introduction

Facial recognition technology is beginning to transform how individuals interact with government and society. This technology can identify and classify human faces by mapping facial features from photographs or videos and comparing them to images in a database of known faces to produce a result.[4] The ACLU has defined facial recognition technology as "the automated or semi-automated process by which the characteristics of an individual's face are analyzed to determine the individual's sentiment, state of mind, and/or other propensities . . ."[5] There are many scholars, policymakers, and law enforcement officials who celebrate the development of this new form of artificial intelligence (AI) for the benefits it can provide in the realms of public health, crime prevention, data

[4] Steve Symanovich, *How Does Facial Recognition Work?*, Norton (Feb. 8, 2019), https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html [https://perma.cc/4YX3-S9PA].

[5] Nathan F. Wessler & Brett M. Kaufman, *Freedom of Information Act Request*, ACLU (Jan. 18, 2019), https://www.aclu.org/sites/default/files/field_document/doj_face_recognition_foia_final_1.18.19.pdf [https://perma.cc/8Q7R-QEFL].

verification, medical treatment, and more.[6] Clearview AI, a startup company that has pioneered the use of AI technologies in the area of facial recognition, is an example of a company that has drawn praise for using AI to help law enforcement identify child sexual abuse suspects, a serial mailbox thief, and multiple suspects in identify-fraud cases.[7]

Others, however, are more equivocal about facial recognition technology's promise, highlighting the technology's potential to violate privacy rights and lead to discrimination. Clearview AI's technology, for example, allows access to databases of approximately three billion images. The largest FBI databases, by contrast, contain a maximum of 411 million images.[8] Clearview AI is facing numerous lawsuits for privacy rights violations as a result.[9] The ACLU has gone so far as to assert that "[n]ever before has the government possessed a surveillance tool as dangerous as face recognition technology" and has called on the Biden Administration to impose a federal moratorium on its use.[10] Increased access to previously unavailable or uncompiled records by governments and private actors raises a litany of privacy concerns and has produced pushback from the LGBTQ community.[11]

[6] Elizabeth McClellan, *Facial Recognition Technology: Balancing the Benefits and Concerns*, 15 J. BUS. & TECH. L. 363, 371–72 (2020); *see also* Ashley Deeks & Shannon Togawa Mercer, *Facial Recognition Software: Costs and Benefits*, LAWFARE (Mar. 27, 2018), https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits [https://perma.cc/78XT-P9ZG]; Kara Rubashkin, *Facial Recognition Technology: A Problem or a Solution?*, BERKELEY J. CRIM. L. BLOG (May 4, 2020), https://www.bjcl.org/blog/facial-recognition-technology-a-problem-or-solution [https://perma.cc/C5SZ-FVWY] (citing Eugene O'Donnell, professor and former police officer, as crediting facial recognition technology with helping to solve violent rape and kidnapping cases).

[7] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020, rev. Mar. 18, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/CNK3-KUHN]; *see also* Jake Parker, *Facial Recognition Success Stories Showcase Positive Use Cases of the Technology*, SEC. INDUS. ASS'N (July 16, 2020), https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology [https://perma.cc/9HTJ-MJBX] (citing examples of facial recognition technology helping to identify terrorists, human traffickers, sex traffickers, and other criminals).

[8] U.S. GOV'T ACCOUNTABILITY OFF., GAO-16–267, FACIAL RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY (2016).

[9] Press Release, *ACLU Sues Clearview AI*, ACLU (May 28, 2020) (on file with author); *see also* Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1243 (7th Cir. 2021).

[10] Kate Ruane, *Biden Must Halt Face Recognition Technology to Advance Racial Equity*, ACLU: NEWS & COMMENTARY (Feb. 17, 2021), https://www.aclu.org/news/privacy-technology/biden-must-halt-face-recognition-technology-to-advance-racial-equity [https://perma.cc/5E7Z-ALJL].

[11] Lou Chibbaro Jr., *LGBTQ Advocates Raise Alarm Over 'Facial Recognition' Technology*, WASHINGTON BLADE (Aug. 13, 2019), https://www.washingtonblade.com/2019/08/13/lgbt-advocates-raise-alarm-over-facial-recognition-technology [https://perma.cc/HA9J-DXWU].

The growing sophistication of facial recognition software has the power to impact minority groups such as the LGBTQ community by facilitating discrimination and compromising privacy. These negative side effects of the technology could stymie efforts by the LGBTQ community to achieve equality. In particular, a 2018 Stanford Graduate School of Business study by Yilin Wang and Michal Kosinski detailed facial recognition technology's ability to detect sexual orientation with a significantly higher accuracy rate than that of humans.[12] The capacity of this artificial intelligence to detect patterns across images has the power to reveal individuals' sexual orientation, which is particularly worrisome when the revelation of one's sexual orientation is nonconsensual. Nonconsenting disclosure of sexual orientation will open the door to new forms of discrimination, privacy violations, and reduced autonomy over how LGBTQ individuals construct and share their identity. Law must adapt to protect LGBTQ rights and dignity in light of this new technological development.

The goals of this Note are threefold: to illustrate some of the most concerning possible applications of this facial recognition technology; to anticipate some of the technology's legal consequences; and to suggest some approaches for mitigating the technology's potential harms through regulation, legislation, and litigation. This Note aims to spot relevant legal issues across various bodies of law to help the LGBTQ community protect the rights, dignity, and equal treatment of its members.[13] While there are many avenues to explore, this Note aims to start a legal conversation about some of the technology's most pressing applications in the realms of employment discrimination and privacy rights law.

Part I of this Note provides an overview of the Wang and Kosinski study, explains the current landscape of LGBTQ-detecting facial recognition technology, and illustrates the ease with which this technology could be refined. Part II examines this technology's ability to exacerbate discrimination against LGBTQ individuals with a focus on employment settings. It analyzes issues arising in public and private hiring regimes. Part III discusses how this technology threatens privacy rights, which could lead to situations involving bullying, harassment, hate crimes, and deceptive advertising practices. Part IV summarizes proposed legislative, regulatory, and judicial approaches that should be adopted in response to

[12] Wang & Kosinski, *supra* note 1, at 257.

[13] This Note is not meant to be an exhaustive list of the possible uses of this new technology; there are other areas of law beyond the scope of this Note where sexual orientation-detecting facial recognition technology will likely yield concern. International law, constitutional law, criminal investigations, police powers, jury selection, government surveillance, suits brought under 42 U.S.C. § 1983, religious exemptions from generally applicable laws, cyberbullying, hate crimes, adoption policies, and child custody disputes could all feasibly implicate this new technology. Those possibilities should be explored in future research on this topic.

this technology's increasing availability and use. It argues that without robust federal privacy laws, facial recognition technologies will continue to proliferate since "there is no monopoly on math," meaning the technological prowess required to create facial recognition systems is open to the masses.[14] Regulation of these technologies is needed to preserve facial recognition's limited benefits without harming vulnerable communities, including the LGBTQ community.

I. The Wang and Kosinski Study in the Context of the Current AI Landscape

Private and public actors in the United States are beginning to embrace facial recognition technology.[15] Yet, beyond a handful of state and local jurisdictions with robust privacy laws, there are very few regulations in place to guard against its unfettered use.[16] Clearview AI is a notable example of a company that has begun both to profit off this technology and to face lawsuits for its privacy violations.[17] The growing use of facial recognition technology by companies and governments led Yilun Wang and Michal Kosinski to examine the dangerous and present power of facial recognition technology for the LGBTQ community.[18] They programmed "off-the-shelf" facial recognition technology with "publicly available data[] and methods well known to computer vision practitioners" to detect sexual orientation, which demonstrated that the technology can determine an individual's sexual orientation with a level of accuracy much higher than the average human.[19] They hoped for their study to serve as a warning call to the legal and policymaking communities to take action to safeguard the civil liberties, privacy, and equality of the LGBTQ community in light of the technology's potential for abuse.[20] This Note takes up their call.

A. *The Current Landscape of Facial Recognition Technology*

Use of facial recognition technology is increasing globally.[21] Anyone who has unlocked an iPhone using Apple's Face ID function, or who has used Apple Pay in lieu of a physical credit or debit card, can appreciate

[14] Hill, *supra* note 7 (highlighting the ease with which technologically savvy individuals can create AI systems with readily available software on their own).

[15] *Facial Recognition Technology*: *Hearing Before the H. Comm. On Oversight and Reform*, at 00:50, 01:30, 116th Cong., C-SPAN (Jan. 15, 2020), https://www.c-span.org/video/?468165–1/facial-recognition-technology [https://perma.cc/9W5H-WS9W].

[16] *Id.* at 02:09, 2:26:42.

[17] *See* Hill, *supra* note 7.

[18] Wang & Kosinski, *supra* note 1, at 246.

[19] *Id.* at 255.

[20] *Id.*

[21] Iman Ghosh, *Mapped: The State of Facial Recognition Around the World*, Visual Capitalist (May 22, 2020), https://www.visualcapitalist.com/facial-recognition-world-map [https://perma.cc/G2AL-R9TK].

the extent to which companies have perfected facial recognition technology.[22] Clearview AI is but one example of a company working to make facial recognition more widely integrated into American society. Its technology allows users to input a picture of a person into a database of over three billion images scraped from websites such as Facebook, YouTube, and Venmo to obtain other public photos of that person along with links to where these photos originated.[23] Another example of facial recognition technology in the United States is the FBI's Facial Analysis, Comparison and Evaluation (FACE) program, which aggregates millions of mug shots, driver's license photos, and juvenile booking photos for use in law enforcement investigations.[24] It has Memoranda of Understanding with 16 states who share their photo repositories and assist with FACE requests.[25]

Large tech companies have tended to take a more cautious approach than governmental entities to the unfettered development of facial recognition technology. Google announced the development of its own facial recognition software, but declined to make it public out of fear that it could be used "in a very bad way."[26] While larger tech companies like Google have refrained from releasing their facial recognition technologies out of an apparent sense of corporate social responsibility, smaller companies, such as Clearview AI, have declined to self-regulate on ethical grounds.[27] In 2019, Clearview AI had already raised $7 million from investors, which is an early sign of the profit potential of this industry should it remain unregulated.[28]

Like Google, Facebook declined to release its facial recognition technology to the general public, but still uses the technology to allow advertisers to exclude certain users—determined by its software to be part of a specific "ethnic affinity"—from viewing their ads.[29] In 2019, the

[22] *See, e.g.*, *About Face ID Advanced Technology*, Apple (Feb. 26, 2020), https://support.apple.com/en-us/HT208108 [https://perma.cc/6W49-MSH5].

[23] Hill, *supra* note 7.

[24] U.S. Gov't Accountability Off., GAO-16–267, *supra* note 8, at i. Florida state law enforcement pioneered an early version of the program starting in 2000 and received approximately $15 million in federal grants through 2014. Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. Times (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/SHL4–7BTY].

[25] U.S. Gov't Accountability Off., GAO-16–267, *supra* note 8, at 50.

[26] Hill, *supra* note 7.

[27] *See id.*

[28] *Id.*

[29] Julia Angwin & Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, ProPublica (Oct. 28, 2016), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race [https://perma.cc/4KVS-EKKR]; *see also* Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica (Nov. 1, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin [https://perma.cc/

U.S. Department of Housing and Urban Development charged Facebook with violating the Fair Housing Act on these grounds.[30] This case foregrounds the concern that sexual orientation-detecting facial recognition technology could lead to impermissible discrimination, if not now then likely sometime soon.

No publicly available sources have proven that any of these companies have already developed facial recognition technology that detects sexual orientation. But the Wang and Kosinski study, detailed below, shows that it is possible that Facebook, Google, Apple, Clearview AI or other tech companies could easily do so in the near future.[31] Wang and Kosinksi used off-the-shelf AI software to make their sexual orientation-detecting facial recognition software.[32] Just imagine what multibillion-dollar companies with thousands of engineers could produce. Facebook, for example, could better refine its internal facial recognition software to detect sexual orientation to more effectively target (or exclude) the LGBTQ community from seeing certain ads.[33] Facebook has already settled several discrimination lawsuits alleging discrimination in its advertising practices based on sexual orientation and other protected classes.[34] While the exact methods used by companies like Facebook are unclear, continued development of this technology without individuals' consent is a privacy violation. Under this backdrop, Wang and Kosinksi set out to illustrate just how easily this erosion of privacy could occur.

B. *Wang and Kosinski Study on Sexual Orientation-Detecting Facial Recognition Technology*

In their study, Wang and Kosinski used thousands of photos from publicly-available dating application profiles.[35] The deep learning facial recognition software they used was able to detect gay men's faces when compared with those of straight men with a classification accuracy rate ranging from 81 to 91 percent.[36] It could detect lesbian women's faces when compared with straight women at rates ranging from 71 to 83 percent.[37] These percentages are much higher than the average human, who

CTM9-T2H2].

[30] Katie Paul & Akanksha Rana, *U.S. Charges Facebook With Racial Discrimination in Targeted Housing Ads*, REUTERS (Mar. 28, 2019), https://www.reuters.com/article/us-facebook-advertisers/u-s-charges-facebook-with-racial-discrimination-in-targeted-housing-ads-idUSKCN1R91E8 [https://perma.cc/V8RF-3A7F].

[31] *See* Wang & Kosinski, *supra* note 1, at 255.

[32] *Id.*

[33] *See* Spencer Overton, *State Power to Regulate Social Media Companies to Prevent Voter Suppression*, 53 U.C. DAVIS L. REV. 1793, 1812 (2020).

[34] *Summary of Settlements Between Civil Rights Advocates and Facebook*, ACLU (Mar. 19, 2019), https://www.aclu.org/other/summary-settlements-between-civil-rights-advocates-and-facebook [https://perma.cc/X52Q-QX6P].

[35] Wang & Kosinski, *supra* note 1, at 248.

[36] *Id.* at 250.

[37] *Id.*

can correctly detect sexual orientation at a rate of about 55 to 65 percent.[38] The low end of the AI ranges was based on one photo of the individual and the upper end of the range was based on an analysis of five photos of that same individual.[39] Wang and Kosinski then ran regression analyses of the algorithm's findings to try to identify which facial features the technology relied on to make its sexual orientation determinations.[40]

Wang and Kosinski started with a widely available software called VGG Face that they describe as "off-the-shelf."[41] They then input thousands of gay and straight dating profile images into the software and programmed it to learn to identify the individual's stated sexual orientation based on facial recognition. VGG Face is a "deep neural network" that mimics the neocortex of the human brain by simulating large "multi-level networks of interconnected neurons" to recognize patterns in vast, unstructured data.[42] Deep neural network technology mimics the human brain in this respect, but can analyze digital images, sounds, text, and other signals on a deeper level of complexity with higher speed and accuracy than the human brain. Because this type of deep neural network AI teaches itself to be more accurate over time, it is difficult for humans to explain the technology's methods in full.[43] "Explainability" is a term of art used to describe this phenomenon in AI, by which humans aim to describe the complex methods AI uses to analyze data, identify patterns, and produce results. Wang and Kosinski hypothesize, however, that their sexual orientation-detecting technology likely identifies patterns in facial characteristics and features that "might be missed or misinterpreted by the human brain."[44]

There are many problematic assumptions made in Wang and Kosinski's article and their methods can be subject to valid critiques. Wang and Kosinski, for instance, argue that their findings could support the prenatal hormone theory of sexual orientation, which links the underexposure of male fetuses or the overexposure of female fetuses to androgens in the

[38] *Id.* at 247 (citing Nalini Ambady, Mark Hallahan, & Brett Conner, *Accuracy of Judgments of Sexual Orientation From Thin Slices of Behavior*, 77 J. Personality & Soc. Psych. 538 (1999)).

[39] *Id.*

[40] For a reader-friendly description of the study, see *Advances in AI are Used to Spot Signs of Sexuality Machines that Read Faces are Coming*, Economist (Sept. 9, 2017), https://www.economist.com/science-and-technology/2017/09/09/advances-in-ai-are-used-to-spot-signs-of-sexuality [https://perma.cc/6GD3–5Q8B].

[41] Wang & Kosinski, *supra* note 1, at 249, 255.

[42] *Id.* at 247.

[43] *See* David Gunning, *Explainable Artificial Intelligence (XAI)*, DARPA, https://www.cc.gatech.edu/~alanwags/DLAI2016/(Gunning)%20IJCAI-16%20DLAI%20WS.pdf; *see also* Andreas Holzinger et al., *Causability and explainability of artificial intelligence in medicine*, WIREs: Data Mining Knowledge Discov., July–Aug. 2019 (providing further background on explainability in AI systems).

[44] Wang & Koskinski, *supra* note 1, at 247.

womb to sexual orientation.[45] This theory is highly controversial in the medical community.[46] It also has unsavory echoes of so-called "race science" and the debunked field of phrenology, which attempted to derive character traits from skull shape.[47] It may be the case that the algorithm relied on superficial grooming features in combination with or in lieu of genetic features.[48] Yet, the nature of deep learning algorithms is such that humans cannot always explain with complete certainty how the technology arrives at its conclusions.[49]

Wang and Kosinski do not discuss in great depth the extent to which dating profiles photos might more obviously present one's sex orientation than the average photo of an individual. Openly gay and lesbian individuals seeking partners might be especially likely to consciously style their dating profile photos in ways that they might emphasize less in other digital spaces or in everyday life. The study that Wang and Kosinski cite for the proposition that humans are able to accurately detect sexual orientation from photos 55 to 65 percent of the time did not rely just on dating profile photos.[50] Wang and Kosinki, however, did conduct their own study with humans reviewing their dating profile photos, which produced accuracy rates of 61 percent for male images and 54 percent for female images.[51] These figures resembled those of the cited study.

While the average human judge exhibits similar accuracy rates in detecting sexual orientation photos regardless of the photographs' sources, how would Wang and Kosinksi's software function when analyzing photos of individuals derived from sources other than dating profiles? Could grooming be the main feature the facial recognition technology is

[45] *Id.*

[46] Heather Murphy, *Why Stanford Researchers Tried to Create a 'Gaydar' Machine*, N.Y. TIMES (Oct. 9, 2017), https://www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html [https://perma.cc/N5NT-ASE4] (citing Rebecca Jordan-Young, Chairwoman of Women's, Gender and Sexuality Studies at Barnard College, who said, "that theory is a mess").

[47] Sigal Samuel, *Some AI Just Shouldn't Exist*, Vox (Apr. 19, 2019), https://www.vox.com/future-perfect/2019/4/19/18412674/ai-bias-facial-recognition-black-gay-transgender [https://perma.cc/Z7CC-CD3Y].

[48] Wang & Kosinski, *supra* note 1, at 251.

[49] Bernard Marr, *What is Deep Learning AI? A Simple Guide With 8 Practical Examples*, FORBES (Oct. 1, 2018), https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/#104886c78d4b [https://perma.cc/RZY7–4CRF]. "Deep learning," or "reinforced learning," refers to the type of artificial intelligence algorithm that learns over time through its experience processing data. In other words, as the algorithm learns from its mistakes, it becomes more accurate over time. This self-perpetuating change in methods over time can make explaining a reinforced learning artificial intelligence algorithm's methods difficult. *Id.*

[50] Wang & Kosinksi, *supra* note 1, at 253 (citing Nalini Ambady, Mark Hallahan, & Brett Conner, *Accuracy of Judgments of Sexual Orientation From Thin Slices of Behavior*, 77 J. PERSONALITY & SOC. PSYCH. 538 (1999)).

[51] Wang & Kosinski, *supra* note 1, at 253.

analyzing to arrive at its determinations? Wang and Kosinksi through various regression analyses and studies conclude that the technology must be relying on fixed facial features and not just grooming.[52] But further studies using photographs from sources other than dating profiles would likely be required to show how broadly applicable this technology in its current form could be.

Wang and Kosinski acknowledge some of the limitations of their study.[53] For instance, a major limitation results from the study's focus on white gay and lesbian individuals since they could not isolate a statistically significant number of photos of nonwhite gay and lesbian individuals from the dating profile images they purchased.[54] They therefore conducted the study based solely on the images of white, cisgender men and women without expanding their scope to other racial groups.[55] Were the technology to be trained with photos of a sufficient number of people of color, the authors assert, based on their technological background and reference to statistical outcomes in biological studies, that the technology would be able to detect their sexuality with similarly high levels of accuracy.[56] In the context of sexual orientation-detecting facial recognition technology, however, where fears of privacy erosion dominate, the study's failure to include racial minorities is perhaps not as harmful as similar exclusions might be elsewhere.[57] Before more inclusive studies are undertaken that demonstrate facial recognition AI's potential to detect the sexual and gender identities of people of color, bisexuals, and transgender individuals, increased regulation and restrictions should be enacted to account for these fears.

Moreover, Wang and Kosinski's study has itself been controversial. During Wang and Kosinksi's publication process, the Gay and Lesbian Alliance Against Defamation (GLAAD) and the Human Rights

[52] *Id.* at 250–52.

[53] Wang & Kosinski, *supra* note 1, at 255.

[54] *Id.*

[55] *Id.*

[56] *Id.*; *see also* Melissa Hines, *Sex-Related Variation in Human Behavior and the Brain*, 14 Trends in Cognitive Sciences 448 (2010) (cited by Wang & Kosinski as evidence that the prenatal hormone theory of sexual orientation applies across racial groups and should therefore support the conclusion that facial recognition technology could be taught to detect sexual orientation across racial groups); Wang & Kosinski, *supra* note 1, at 255. *But see* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use,* Wash. Post (Dec. 19, 2019), 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/WPM5-LPKP] (casting doubt on Wang and Kosinski's assertion since other studies have shown facial recognition to generally be less accurate when identifying the faces of people of color with darker skin tones).

[57] *See Design Bias is Harmful, and in Some Cases May be Lethal*, Economist, (Apr. 10, 2021), https://www.economist.com/leaders/2021/04/10/design-bias-is-harmful-and-in-some-cases-may-be-lethal [https://perma.cc/5N2Y-AVDT].

Campaign (HRC) issued a statement calling their study "dangerous and flawed."[58] The statement asserted that "technology cannot identify someone's sexual orientation" and went on to list a number of the study's limitations.[59] It is true, as these critiques suggest, that facial recognition technology as it currently stands cannot identify sexual orientation with perfect accuracy and may never reach such a threshold. False classifications are a feature of this technology, some of the legal implications of which are discussed below. Nonetheless, even an imperfect tool to detect sexual orientation could be used by companies and governments that harbor animus toward the LGBTQ community. Imperfections will not necessarily prevent them from deploying the technology or from trying to further improve it.

Wang and Kosinski agree with GLAAD and HRC that erosion of privacy rights and discrimination are two major problems this technology poses.[60] Yet governments and companies around the world are "already deploying face-based classifiers aimed at detecting intimate traits."[61] Wang and Kosinksi argue that "delaying or abandoning the publication of these findings could deprive . . . policymakers the ability to introduce legislation to protect people."[62] Furthermore, their work does not "offer any advantage to those who may be developing or deploying classification algorithms" because they used "widely available off-the-shelf tools, publicly available data, and methods well known to computer vision practitioners."[63]

The main takeaway from the study is that facial recognition technology now has the proven power to "out" members of the LGBTQ community with high levels of accuracy. Because this AI can train itself to produce more accurate results the longer it analyzes specific datasets, explainability becomes more difficult even for the programmers who develop the AI. This type of AI will only become more sophisticated in the absence of regulation. Wang and Kosinski highlight the relative ease with which computer coders could produce these algorithms.[64] After all,

[58] Drew Anderson, *GLAAD and HRC Call on Stanford University & Responsible Media to Debunk Dangerous and Flawed Report Claiming to Identify LGBTQ People Through Facial Recognition Technology*, GLAAD (Sept. 8, 2017), https://www.glaad.org/blog/glaad-and-hrc-call-stanford-university-responsible-media-debunk-dangerous-flawed-report [https://perma.cc/Q9BR-Q6KL].

[59] The Statement also echoed the exact concerns that Wang and Kosinksi themselves cited in their study, namely that this technology could threaten the privacy of LGBTQ individuals and could support brutal regimes efforts to persecute LGBTQ people. *Compare id.*, *with* Wang & Kosinski, *supra* note 1, at 255.

[60] *Id.*

[61] Wang & Kosinski, *supra* note 1, at 255 (citing Josh Chin & Liza Lin, *China's All-Seeing Surveillance State is Reading Its Citizens' Faces*, WALL ST. J. (June 26, 2017), https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1498493020 [https://perma.cc/AQ75-F47S]).

[62] Wang & Kosinski, *supra* note 1, at 255.

[63] *Id.*

[64] *Id.*

their technology was developed by using a publicly available AI program. Wang and Kosinski believe that their technology would be easy to replicate and expand upon to apply to other LGBTQ subpopulations.[65]

This new power could have significant implications for the legal protections of LGBTQ individuals in many areas of their lives. While the Wang and Kosinksi study only analyzed lesbian and gay individuals, it is likely that others could use their methods to classify bisexual or transgender individuals as well. We must adapt our system of legal protections to anticipate the consequences of this technology and reform our regulations to protect against its harms.

LGBTQ people have privacy interests that this facial recognition technology will violate. While this Note mainly focuses on the legal issues facing gays and lesbians who are directly implicated by Wang and Kosinski's study, many of the same issues could apply similarly to the transgender community and other minority groups if the technology develops without regulation or restriction. There are many circumstances in which transgender individuals, for instance, might wish to keep their trans status a secret. This technology could infringe upon that autonomy. The legal regimes protecting lesbians and gays differ in some ways from those protecting transgender individuals. While exploration of those differences falls beyond the scope of this Note, lawmakers should anticipate and plan for the differing needs of various groups within the LGBTQ community. Although this technology is still in its infancy and has not achieved perfect accuracy, Wang and Kosinski's study sounds the alarm that the technology is possible.

II. Facial Recognition Technology Can Facilitate Discrimination Against the LGBTQ Community Through Surreptitious or Unintentional Means

This Part begins with an overview of facial recognition technology's discriminatory track record and emphasizes the continuing discrimination that the LGBTQ community faces. While there are a number of laws in place to protect LGBTQ individuals against discrimination in the workplace and in public spaces, unregulated facial recognition technology could obstruct the full realization of those protections. This Part explains how facial recognition technology could intentionally or unintentionally yield discrimination against LGBTQ individuals, with a particular focus on discrimination in public and private sector employment. This Part concludes with an overview of select approaches taken by certain jurisdictions to mitigate these possibilities.

[65] *Id.*

A. *Facial Recognition Technology's Relationship to Intentional and Unintentional Discrimination*

Facial recognition technology already has had discriminatory effects.[66] While publicized examples of facial recognition being used to *intentionally* discriminate against people based on their membership in a marginalized group remain rare, instances of *unintentional* discrimination based on such membership have begun to emerge.[67] A 2019 study by the National Institute of Standards and Technology discovered that many current facial recognition algorithms more frequently falsely identify women and people of color as compared to white males.[68] These false identifications show that facial recognition technology can make errors unintended by its human programmers. Even if programmers fully intend to make their AI technology free of discriminatory bias, however, technical glitches, the subconscious bias of the programmers, and bias in the datasets used can each lead to unintentionally discriminatory outcomes.[69]

While the use of facial recognition to intentionally discriminate against individuals based on a protected trait is both legally and morally repugnant, unintentional discrimination can be even more difficult to thwart. These problems are explored below and should give pause both to law enforcement divisions from continuing to pioneer the use of facial recognition technology in the criminal investigations realm and to those in the public and private sectors who use the technology to inform or supplement employment decisions. The LGBTQ community can easily suffer from the use of facial recognition technology with discriminatory intent, or from use that produces discriminatory effects even in the absence of such intent.

B. *The Current Status of LGBTQ Discrimination*

Discrimination against the LGBTQ community persists in the United States today. The Center for American Progress (CAP) recently released a study showing that 36 percent of LGBTQ people reported experiencing some form of discrimination in the past year.[70] Approximately

[66] *Facial Recognition Technology*, *supra* note 15 at 2:27:50 (Representative Ocasio-Cortez stating that, "these technologies are almost automating injustices . . . but also automating biases that compound on the lack of diversity in Silicon Valley . . . ").

[67] *Id.* (citing examples of facial recognition technology that incorrectly classified individuals from racial minority groups as criminals and noting that error rates are higher for racial minorities); *see also Design Bias*, *supra* note 54.

[68] Harwell, *supra* note 53.

[69] AI programs have recently had difficulty accurately identifying non-binary individuals. *See* Molly Millar, *Facial Recognition Technology Struggles to See Past Gender Binary*, Reuters (Oct. 30, 2019), https://www.reuters.com/article/us-usa-LGBTQ-facial-recognition/facial-recognition-technology-struggles-to-see-past-gender-binary-idUSKBN1X92OD [https://perma.cc/RE92–4MVZ].

[70] Sharita Gruberg, Lindsay Mahowald & John Halpin, *The State of the LGBTQ Community in 2020: A National Public Opinion Study*, Center for American

51 percent of LBGTQ respondents reported experiencing discrimination in public spaces, including at work and in school.[71] Notably, 36 percent of LGBTQ respondents reported avoiding accessing health care due to fear of discrimination, a rate which is both higher than that of non-LGBTQ respondents (20 percent)[72] and which supports past research that even the *expectation* of experiencing discrimination can negatively impact LGBTQ people.[73] As such, laws should ensure that LGBTQ individuals retain decisional control over when and how they come out publicly.

Experiences with, and even the expectation of, discrimination can wreak psychological harm on many LGBTQ individuals and force them to modify their behavior, including, for one, by hiding their intimate relationships as a defense mechanism.[74] These psychological harms contribute to high rates of suicide and mental illness in the LGBTQ community.[75] Increased visibility of LGBTQ individuals also puts them at risk for hate crimes: the LGBTQ community has been cited as being the minority group in America most often targeted for such crimes,[76] which is likely supported by the lack of coverage for sexual orientation and/or gender identity across many states' hate crime laws.[77]

One way in which this persistent discrimination against LGBTQ individuals impacts their lives is in their ability to get a job. Over one-third of LGBTQ respondents to the CAP study said that discrimination

Progress (Oct. 6, 2020), https://www.americanprogress.org/issues/LGBTQq-rights/reports/2020/10/06/491052/state-LGBTQq-community-2020 [https://perma.cc/JB9U-HT4P].

[71] *Id.*

[72] *Id.*

[73] *See, e.g.*, Adam P. Romero et al., *LGBT People and Housing Affordability, Discrimination, and Homelessness*, Williams Inst. at 21 (Apr. 2020), https://williamsinstitute.law.ucla.edu/wp-content/uploads/LGBT-Housing-Apr-2020.pdf [https://perma.cc/BH2H-TXGL] (summarizing past research on the impact of the expectation of discrimination on LGBTQ people in the context of housing).

[74] *Id.*

[75] *Mental Health and the LGBTQ Community*, Human Rights Campaign Foundation (Jul. 2017), https://suicidepreventionlifeline.org/wp-content/uploads/2017/07/LGBTQ_MentalHealth_OnePager.pdf [https://perma.cc/VN7E-NRPR].

[76] Haeyoun Park & Iaryna Mykhyalyshyn, L.G.B.T. People Are More Likely to Be Targets of Hate Crimes Than Any Other Minority Group, N.Y. Times, (Jun. 16, 2016), https://www.nytimes.com/interactive/2016/06/16/us/hate-crimes-against-LGBTQ.html [https://perma.cc/EH9D-67RX]; *see also* FBI, *Hate Crime Statistics 2019*, Incidences and Offenses, https://ucr.fbi.gov/hate-crime/2019/topic-pages/incidents-and-offenses [https://perma.cc/L758–9K63] (finding that out of 1,395 hate crime offenses based on sexual-orientation biases, 62.2 percent were anti-gay (male), 24.5 percent were prompted by LGBT mixed group bias, 10.2 percent classified as anti-lesbian bias, 1.9 percent classified as anti-bisexual bias, and 1.2 percent were classified as anti-heterosexual bias. Out of 224 offenses grounded in gender-identity bias, 173 were anti-transgender in nature and 51 were anti-gender non-conforming).

[77] Christy Mallory et al., *Banning the Use of Gay and Trans Panic Defenses*, Williams Inst. 18–19 (Apr. 2021), https://williamsinstitute.law.ucla.edu/wp-content/uploads/Gay-Trans-Panic-Apr-2021.pdf [https://perma.cc/GL74-ELD9].

against their community had moderately or significantly harmed their ability to be hired.[78] For transgender individuals, that number rose to 53 percent.[79] Should discriminatory employers have facial recognition tools at their disposal to determine the LGBTQ status of a job applicant or employee against their will, any progress made in eradicating employment discrimination against the LGBTQ community could be at risk.

C. *Existing LGBTQ Anti-Discrimination Protections*

In June of 2020, the Supreme Court in *Bostock v. Clayton County* ruled that Title VII of the Civil Rights Act of 1964 protects against employment discrimination based on sexual orientation and gender identity.[80] The Court reasoned that making hiring or firing decisions based on the gender that an employee was sexually attracted to or based on the gender identity of the employee implicated Title VII's ban on making employment decisions "because of sex."[81] Courts have already begun to apply *Bostock* to employment law cases challenging dismissals or refusals to hire based on sexual orientation.[82] Courts have also expanded *Bostock*'s reasoning to non-employment statutes such as Title IX, which contains the same "because of sex" language,[83] as well as to non-federal statutes.[84]

Bostock's outcome relied in large part on the 1989 Supreme Court ruling in *Price Waterhouse v. Hopkins*.[85] In *Price Waterhouse*, the Court had held the employer liable under Title VII for denying an applicant a promotion because she did not adhere to the perceived stereotypes of her gender.[86] These two cases will likely complement one another to enable those seeking to bring LGBTQ-related employment discrimination claims to do so successfully.

Upon entering office, President Biden signed an executive order requiring agencies to apply *Bostock*'s textualist reading of the meaning of "sex discrimination" to all other areas of the law where sex

[78] Gruberg, Mahowald & Halpin, *supra* note 67.

[79] *Id.*

[80] Bostock v. Clayton Cty., 140 S. Ct. 1731 (2020).

[81] 42 U.S.C. § 2000e-2(a) (2012).

[82] *See* Redmon v. Yorozu Auto. Tenn., Inc., 834 F. App'x 234 (6th Cir. 2021).

[83] *See* Grimm v. Gloucester Cty. Sch. Bd., 972 F.3d 586 (4th Cir. 2020).

[84] *See, e.g.*, *NDDOLHR Now Accepting and Investigating Charges of Discrimination Based on Sexual Orientation and Gender Identity*, N.D. (June 18, 2020), https://www.nd.gov/labor/news/nddolhr-now-accepting-and-investigating-charges-discrimination-based-sexual-orientation-and [https://perma.cc/ACN2-J8ML]; Henry Cordes, *State Agency Applies U.S. Supreme Court Ruling on LGBT Job Rights to Housing Cases*, OMAHA WORLD HERALD (Aug. 12, 2020), https://omaha.com/news/local/govt-and-politics/state-agency-applies-u-s-supreme-court-ruling-on-lgbt-job-rights-to-housing-cases/article_2d42d906–1aca-5938–8b8e-d954d2b757c2.html [https://perma.cc/9UA7–2AVR].

[85] Oral Argument at 3:10, Bostock v. Clayton Cty., 140 S. Ct. 1731 (2020), https://www.oyez.org/cases/2019/17–1618 [https://perma.cc/VBR9–9XAT].

[86] Price Waterhouse v. Hopkins, 490 U.S. 228, 250 (1989).

discrimination is already prohibited, including in education, housing, and health care.[87] The Equality Act, which the House has passed numerous times only for the bill to languish in the Senate, is an attempt to codify that interpretation of sex discrimination across all federal laws and to prevent easy rescission of President Biden's Executive Order by a future administration.[88]

Many state and local jurisdictions across the United States have codified employment protections for LGBTQ individuals.[89] In 2020, the Human Rights Campaign identified twenty-two states and Washington D.C. that had prohibited discrimination against LGBTQ individuals; six states that had adopted *Bostock*'s rationale into their reading of their existing state non-discrimination laws; six states that prohibited discrimination by government employers against public employees based on LGBTQ status; one state that prohibited discrimination based on sexual orientation only; and one state that prohibited discrimination by government employers against public employees based on sexual orientation only. The remaining fourteen states did not have any employment related anti-discrimination laws on the books to explicitly protect the LGBTQ community.[90] If states that prohibited sex discrimination were to interpret their state laws in the same manner as the *Bostock* majority did Title VII, approximately 3.6 million LGBTQ individuals would stand to gain protections against discrimination under state law as well.[91]

These developments should make courts more amenable to claims of discrimination through the use of facial recognition technology brought by LGBTQ individuals. One difficulty for claimants, however, will be providing solid evidence of discrimination enabled through the use of such technology. Another pertains to the changing landscape of religious exemptions to generally applicable laws, such as antidiscrimination provisions. Currently pending before the Supreme Court is *Fulton v. City of Philadelphia*, which will determine whether a Catholic adoption agency is entitled to an exception to Philadelphia's nondiscrimination policy on

[87] *The Equality Act*, Human Rights Campaign (Mar. 13, 2021), https://www.hrc.org/resources/the-equality-act [https://perma.cc/P2G9-R52E]; Chris Johnson, *Biden Falls Short of 100-Day Goal to Sign Equality Act Into Law*, Washington Blade (Apr. 28, 2021), https://www.washingtonblade.com/2021/04/28/biden-unlikely-to-fulfill-campaign-pledge-to-sign-equality-act-in-100-days [https://perma.cc/6JAA-S67Y].

[88] *Id.*

[89] *2020 State Equality Index: A Review of State Legislation Affecting the Lesbian, Gay, Bisexual, Transgender, and Queer Community and a Look Ahead in 2021*, Human Rights Campaign Foundation (2020), https://www.hrc.org/resources/state-equality-index [https://perma.cc/Z247–29DJ].

[90] *Id.*

[91] Christy Mallory, Luis A. Vasquez & Celia Meredith, *Legal Protections for LGBT People After* Bostock v. Clayton County, Williams Inst. (Aug. 2020) https://williamsinstitute.law.ucla.edu/wp-content/uploads/Bostock-State-Laws-Jul-2020.pdf [https://perma.cc/GPX6-YUZD].

free exercise grounds.[92] If the Court holds that it is, religious entities that provide certain public services may be able to refuse LGBTQ clients as a matter of constitutional law depending on how the Court constructs its ruling. Religious institutions already have an exception to employment nondiscrimination provisions through the so-called "ministerial exception," insulating religious entities from employment discrimination claims for roles that "convey the Church's message" and "carry out its mission."[93] Religious exemptions may soon apply to nonreligious organizations, too. LGBTQ individuals wishing to work for religious entities and individuals may be at an even greater risk of discrimination should those entities and individuals employ LGBTQ-detecting facial recognition technology.

D. *Facial Recognition's Power to Discriminate Against LGBTQ Individuals in the Employment Context*

The following Subparts focus on how LGBTQ-detecting facial recognition technology could impact the employment discrimination landscape. There are a few reasons for focusing on this type of legal claim. First, as described above, companies are already beginning to integrate facial recognition technology into their hiring decisions.[94] Technology companies like Clearview AI are building facial recognition software to facilitate background checks not only on behalf of law enforcement, but also for private entities wishing to purchase their services.[95] Second, employment discrimination against the LGBTQ community remains a present and widespread concern, as *Bostock* and its consolidated cases demonstrate. Third, the reasoning and policy suggestions discussed in the employment context can easily translate into other spheres where this technology could threaten the fight for LGBTQ equality more broadly. Regulations and restrictions on the use of facial recognition technology in the employment realm could also be applied to uses by law enforcement, schools, families, and other entities.

Facial recognition technology poses two types of concerns for the LGBTQ community with regard to employment decisions: intentional and unintentional discrimination. The first concern is that employers who harbor animus toward LGBTQ candidates could use facial recognition technology surreptitiously to scan applicants' faces, determine

[92] *See* Fulton v. City of Phila., 140 S. Ct. 1104 (2020); Brief for Respondents, Fulton, 140 S. Ct. 1104 (No. 19–123), 2020 WL 4819956, at *i.

[93] *See* Hosanna-Tabor Evangelical Lutheran Church & Sch. v. E.E.O.C., 565 U.S. 171, 192 (2012); *see also* Our Lady of Guadalupe Sch. v. Morrissey-Berru, 140 S. Ct. 2049, 2052–53 (2020).

[94] Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job*, WASH. POST (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job [https://perma.cc/WPM5-LPKP].

[95] Hill, *supra* note 7.

their likely sexual orientation or gender identity, and reject their application as a result. This would be an intentionally discriminatory use. The second concern is that the technology's algorithms could contain inherent bias against LGBTQ applicants through programming errors, biased data, or other technical deficiencies. In other words, the scoring mechanisms in facial recognition software could unintentionally assign lower score assessments to LGBTQ candidates unbeknownst to an employer that relies on the technology to make hiring decisions. This Subpart gives an overview of the potential issues that might arise in private and public sector hiring and how courts and lawmakers might deal with them.

E. *Private Sector Hiring*

Facial recognition technology is already being deployed in a number of employment contexts. Companies such as Hirevue, Pymetrics, and Trueface provide facial recognition analyses for human resource offices looking to streamline their hiring processes.[96] Hirevue, for example, boasts over 600 clients, including companies like Goldman Sachs, Unilever, Under Armour, and Vodafone.[97] While working-class employers have not yet taken up facial recognition software to aid in their hiring processes—possibly due to price and accessibility—it is only a matter of time before this technology becomes more widely utilized. Larger corporate employers generally use the facial recognition service as supplements to first-round screener interviews for entry-level positions, serving an important gatekeeping function in the hiring process.[98] At the screener stage, employers may be looking for general social skills, fit with the company, stated skills relevant for the position, and other basic requirements.

The normalization of facial recognition software used in the hiring process exacerbates the concern about surreptitious intentional use of the technology to discriminate against LGBTQ applicants. Employers will now have access to photo and video datasets on applicants that can easily be processed by other facial recognition software in a covert manner. For example, the large dataset amassed by Clearview AI could be accessible to employers willing to purchase its technology. Because these hiring programs assess applicants across a wide variety of characteristics, skills, and traits, it will be much easier for employers to disguise the true reasoning for their employment decisions behind non-discriminatory justifications.

[96] HireVue, https://www.hirevue.com [https://perma.cc/W4E3-LLPU] (last visited Mar. 28, 2021); Pymetrics, https://www.pymetrics.com/about [https://perma.cc/FC2H-Q2EV] (last visited Mar. 28, 2021); TrueFace, https://www.trueface.ai [https://perma.cc/M5AH-Y4JH] (last visited Mar. 28, 2021).

[97] Richard Feloni, *I Tried the Software That Uses AI to Scan Job Applicants for Companies Like Goldman Sachs and Unilever Before Meeting Them – and It's Not as Creepy as It Sounds*, Bus. Insider (Aug. 23, 2017), https://www.businessinsider.com/hirevue-ai-powered-job-interview-platform-2017–8 [https://perma.cc/B5FM-LM82].

[98] *See id.*

One way this could play out is as follows. A discriminatory employer could use Hirevue to assess applicants' personality traits for a position, then secretly use sexual orientation-detecting software to discover that the applicant is a lesbian and choose not to hire her because of that fact. Yet, the employer could then justify its decision based on some other characteristic analyzed by Hirevue's official recognition technology. If the lesbian applicant suspects she was not hired because of her sexual orientation, it could be difficult for her to muster sufficient proof to draft a well-pleaded compliant strong enough to withstand a motion to dismiss.[99]

The second concern is that the facial recognition technology used by employers is unintentionally but still inherently biased against LGBTQ applicants. Services such as Hirevue, Pymetrics, and Trueface, along with many others, claim that technological protections are in place to ensure unbiased scoring and assessment of applicants.[100] While it may be the case that these facial recognition software systems actually can increase diversity in hiring by cutting down on implicit interviewer bias, these systems are not foolproof. There are myriad studies that show how inherently biased AI programs are and how difficult it is to successfully de-bias them.[101]

Wang and Kosinski emphasized in their piece just how easy sexual orientation-detection technology is to develop.[102] Companies such as Hirevue, Pymetrics, and Trueface have not proven that their software cannot be adapted to perform other assessments that amount to discriminatory treatment of applicants. While all three companies highlight the ability of their products to enhance workplace diversity, they do not offer a clear explanation of how their algorithms work, nor do they provide convincing evidence that their products are free from bias.

How exactly does inherent bias manifest in facial recognition algorithms? One possibility is rooted in response to popular opinion. Employers in service industries, for example, want to hire employees that will get along well with customers. An employer might input statistical data about customer satisfaction preferences into its facial recognition

[99] *See, e.g.*, Guess v. Phila. Hous. Auth., 354 F. Supp. 3d 596, 599 (E.D. Pa. 2019), *appeal dismissed sub nom.* Doe v. Phila. Hous. Auth., No. 19–2004, 2019 WL 5791221 (3d Cir. July 17, 2019) (granting motion to dismiss for failure to state a claim based on employment discrimination despite supervisor calling employee a "fucking faggot" in three separate instances and disparate pay compared to peers).

[100] *See Increase Diversity and Mitigate Bias*, HIREVUE, https://www.hirevue.com/why-hirevue/foster-diversity [https://perma.cc/9WLE-6X92] (last visited Mar. 28, 2021); *Cross-Functional Innovation*, PYMETRICS, https://www.pymetrics.com/science [https://perma.cc/E3BB-J95U] (last visited Mar. 26, 2021).

[101] *See* Sarah M. West et al., *Discriminating Systems: Gender, Race, and Power in AI*, AI NOW INSTITUTE 10–12 (2019), https://ainowinstitute.org/discriminatingsystems.pdf [https://perma.cc/478M-Q2N3]*; see also* Samuel, *supra* note 47.

[102] *See* Wang & Kosinski, *supra* note 1, at 255.

hiring algorithm. That data could implicitly contain patterns that show general customer preferences for interacting with feminine-acting female employees, as opposed to women who display more masculine mannerisms. If facial recognition software is used to calculate the degree of "femininity" displayed by female applicants' faces in interviews, and a certain lesbian applicant who presents as more masculine is analyzed, it will almost certainly give a lower overall score to that lesbian applicant. And, in turn, that software will likely have discriminated against the applicant due to sex stereotyping in ways similar to those seen in *Price Waterhouse v. Hopkins*.[103] This anti-LGBTQ discrimination becomes even more pronounced if, for example, lesbians across the board are found to display more masculine mannerisms according to the analysis of the facial recognition software. Yet, the algorithm programmers and employers relying on them can simply claim that they were relying on objective client preference data and did not intend for such bias against lesbians.

This potential justification of discrimination through reliance on superficially neutral statistical data illustrates why clear explanation of utilized algorithms' methods and inputs is crucial. Although facial recognition software companies could argue that their systems' algorithms constitute trade secrets, regulators should implement policies to root out legitimate trade secrets claims while ensuring that LGBTQ applicants are protected. Employers should be required to be as transparent as possible about their hiring decisions to avoid unintentional discrimination.

While some states have statutes prohibiting discrimination on the basis of sexual orientation, federal law under Title VII was only recently clarified to protect against discrimination on the basis of sexual orientation in *Bostock v. Clayton County*.[104] The Supreme Court clarified that language within Title VII's employment protections banning discrimination "because of sex" encompasses sexual orientation and gender identity discrimination.[105] As a result, LGBTQ individuals who feel they have been discriminated against in hiring as a result of the use of facial recognition technology during the hiring process now have a route for recourse in courts around the country. The LGBTQ community must begin to think about how to bring these types of suits and how to enact safeguards that affirmatively prevent discrimination in hiring through the use of facial-recognition technology.

F. *Government Hiring*

Public sector employees at the federal level benefit from a wide range of antidiscrimination statutes and other policies. Furthermore, the federal government and most state governments have constitutional protections that require adequate public review before making

[103] Price Waterhouse v. Hopkins, 490 U.S. 228, 234–36 (1989).

[104] Bostock v. Clayton Cty., 140 S. Ct. 1731, 1737–38 (2020).

[105] *See id.* at 1741–43.

firing decisions. These same protections would apply should governments begin to use facial recognition technology to aid in their hiring and firing decisions. To avoid both surreptitious and unintentional forms of LGBTQ discrimination in agency hiring processes, lawmakers should impose additional procedural safeguards on the use of facial recognition technology in government hiring decisions. As in the explainability concerns raised in the private-sector context, Algorithmic Impact Assessments (AIAs) are one possible policy lawmakers could adopt in line with existing administrative law procedures to meet the changing transparency needs associated with public sector hiring.[106]

Scholars have begun debating the procedures that the government should adopt to guard against discriminatory bias influencing hiring decisions. This procedure would amount to a public airing of the facial recognition methods before they go into effect.[107] AIAs would ensure that "both the agency and the public . . . [can] evaluate the adoption of an automated decision system before the agency has committed to its use."[108] AIAs would allow time to identify public concerns that may need to be negotiated or otherwise addressed before a contract is signed to use artificial intelligence tools in a governmental capacity. These concerns could then be translated into changes in the algorithm's metrics. Many of the artificial intelligence systems used by administrative agencies are already produced in-house.[109] Therefore, AIAs are also less likely to run afoul of trade secrets defenses brought by private facial recognition companies.

AIAs would resemble the notice and comment period required for administrative rulemaking regulations.[110] In the same way as federal agencies must provide a public notice and comment period before promulgating a rule, agencies should invite public participation before implementing decision-making procedures based on algorithms and AI.[111] Allowing for public comment on agencies' use of AI would provide

[106] Dillon Reisman et al., *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*, AI NOW INSTITUTE (April 2018), https://ainowinstitute.org/aiareport2018.pdf [https://perma.cc/TU8E-JY95].

[107] *Id.* at 9.

[108] *Id.* at 8.

[109] Emma Talley, *Researchers Discuss Use of Artificial Intelligence in Government Agencies: 45% of "Important" Government Agencies Use or Experiment with Artificial Intelligence, Researchers Say*, STAN. DAILY (Feb. 3, 2020), *https://www.stanforddaily.com/2020/02/03/researchers-discuss-use-of-artificial-intelligence-in-government-agencies* [https://perma.cc/E9U4-N5DQ] (quoting Professor David Engstrom of Stanford Law School as saying that in most cases the technologies used by government agencies "were developed in house by agency technologists, not by profit-oriented contractors.").

[110] 5 U.S.C. § 553(c) (2012) ("After notice required by this section, the agency shall give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation.").

[111] Reisman et al., *supra* note 103, at 15. ("In their self-assessments, agencies

legitimacy to the use of facial recognition technology. Moreover, *Heckler v. Campbell* has made clear that under the Administrative Procedure Act (APA), agencies can permissibly base the parameters of informal adjudications on frameworks laid out in prior rulemakings that resolve certain classes of issues.[112] AIAs could function as a prior rulemaking that lays out the parameters for how facial recognition technology will be involved in agencies' adjudicative decision-making. If AIAs function correctly, procedural bias against LGBTQ applicants and employees should be reduced.

State governments have also begun experimenting with AI technology. Some of their programs have spawned litigation that could lay relevant precedential groundwork for challenges to facial recognition systems that discriminate against LGBTQ individuals. In Wisconsin, for instance, the state courts piloted the use of Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), which is a statistical risk assessment AI program that assists in sentencing decisions.[113] Plaintiff Eric Loomis challenged the use of COMPAS on three grounds in *State v. Loomis*.[114] Loomis argued that: (1) COMPAS violated a defendant's right to be sentenced based upon accurate information, in part because the proprietary nature of COMPAS prevented him from assessing its accuracy; (2) it violated a defendant's right to an individualized sentence; and (3) it improperly used gendered assessments in sentencing.[115] The court addressed the concern that risk assessment tools "may disproportionately classify minority offenders as higher risk, often due to factors that may be out of their control such as familial background and education."[116] Although the court upheld the use of COMPAS, the court mandated that the Wisconsin judicial system adhere to certain procedural guardrails when considering a COMPAS risk assessment.

When using COMPAS, Wisconsin courts must explain the software's methods to defendants and acknowledge the potential inaccuracies of COMPAS.[117] They must also acknowledge that the data is not specific to Wisconsin populations and ensure that the risk assessment data are "constantly monitored and re-normed for accuracy due to changing populations."[118] Loomis's gender discrimination claim failed because both parties agreed that statistical evidence proved that men, on average, have

should identify potential impacts on the public and then proactively engage affected communities to ensure that a system meets a given community's goals.").

[112] Heckler v. Campbell, 461 U.S. 458, 467 (1983) (holding that agencies may rely on rulemakings to resolve certain classes of issues).

[113] State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

[114] *Id.*

[115] *Id.* at 757.

[116] *Id.* at 763.

[117] *See id.* at 769–70.

[118] *Id.* at 769.

a higher recidivism rate than women.[119] Furthermore, the COMPAS assessment can only be one of many factors that a court weighs when handing down sentences, and in doing so, it must explain its reasoning in full.[120] In other words, COMPAS could merely supplement a judge's decision-making, not supplant it altogether.

This holding could have persuasive implications for judicially-imposed constraints on the use of sexual orientation-detecting technology in public contexts more broadly. Important rules emerged from this case, including the requirement of constant monitoring of data accuracy, thorough explanation of how the algorithm is used, and consideration of facial recognition assessments alongside other metrics to reach decisions. If LGBTQ claimants are able to frame their complaint like Mr. Loomis' and plead adequate facts, they could then ask for similar relief, which could result in an improved process and limit the potential for discrimination in public employment and other governmental contexts.

Houston Federation of Teachers v. Houston Independent School District is another case that illustrates how a lack of explainability can violate procedural due process.[121] The Houston Independent School District had used an algorithm, licensed from a company which protected its software under trade secret law, to calculate teachers' impacts on student performance by examining students' standardized test scores.[122] Low impact scores then provided the basis for firing teachers.[123] These impact scores, however, could have been erroneously calculated for any number of reasons, "ranging from data-entry mistakes to glitches in the computer code itself."[124] Algorithms, like any human creation, are subject to error. The school district acknowledged that mistakes could occur in calculating a teacher's impact score, and even when a mistake was found in a teacher's score, it could not necessarily be promptly corrected.[125]

The district court allowed the suit against the school district to go forward since teachers' inability to challenge the accuracy of the algorithm potentially violated procedural due process. The court held that the teachers' inability to challenge the algorithm that threatened their employment presented a constitutional problem.[126] The court also emphasized that algorithmic methods must be explained to those whom they affect so that impacted parties can adequately understand them and

[119] *Id.* at 765.

[120] *Id.* at 769.

[121] Hous. Fed'n of Tchrs. v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168 (S.D. Tex. 2017).

[122] *Id.* at 1177.

[123] *Id.* at 1175.

[124] *Id.*

[125] *Id.*

[126] *Id.*

challenge them.[127] Opaque uses of sexual orientation-detecting facial recognition by the public sector could be challenged on similar grounds.

This case helps to strengthen the argument that the methods for assessing physical features or modes of expression by facial recognition technology must be thoroughly explained. Government agencies should be required to provide these sorts of explanations so that the burden of proof does not fall entirely on the LGBTQ community to show that members of the community are being systemically excluded from certain jobs and positions as a result of this technology. Similar to the school teachers in *Houston Federation of Teachers*, LGBTQ individuals could not do so without explanation of the methods.[128] Thankfully, the outcome of this case and others will reinforce the need for facial recognition software companies and governments that contract with them to disclose their methods. Although disclosure will not root out discrimination by itself, it will help to close a sizeable information asymmetry between parties, increasing the possibility for discrimination claims to succeed.

G. *Human Review of Facial Recognition Assessments*

Because facial recognition technology is still not perfectly accurate, scholars and policymakers are debating the contexts in which humans must legally be involved in the decision-making process. Some jurisdictions are moving toward articulating a right to a human decision, or at least human review of automated decision-making processes, as a method to remedy the discriminatory impacts of facial recognition and other AI technologies.[129] One reading of the holding in *Loomis* is that the court mandated some human participation in the decision-making and review of the AI analysis. Scholars such as Aziz Huq have examined how citizens in a world of AI technology might exercise a right to a human decision, as the court in *Loomis* implicitly granted.[130] Some argue that a right to a human decision in employment could safeguard the protections of the LGBTQ community in hiring. For example, if an LGBTQ applicant is denied employment, that applicant could demand a human decision-maker review the machine decision to avoid total reliance on an AI algorithm that might contain inherent biases in its programming.

The European Union's General Data Privacy Regulation (GDPR) is an example of a law that articulates a right to a human decisionmaker in certain instances.[131] Such laws aim to ensure that human decision-mak-

[127] *Id.* at 1178.

[128] *Id.* at 1177 ("HISD further concedes that any effort by teachers to replicate their own scores, with the limited information available to them, will necessarily fail. This has been confirmed by plaintiffs' expert, who was unable to replicate the scores despite being given far greater access to the underlying computer codes than is available to an individual teacher.").

[129] Aziz Huq, *A Right to a Human Decision*, 106 Va. L. Rev. 611, 621–24 (2020).

[130] *Id.* at 611.

[131] Regulation 2016/679, of the European Parliament and of the Council of 27

ing in society is never fully usurped by AI algorithms. The problem is that humans, although bound by laws, carry their own implicit biases as well.

Huq offers a more practical and promising solution. Huq acknowledges that AI algorithms, such as ones used in any sexual orientation-detecting technology, are still in their infancy.[132] Furthermore, they can be flawed in many ways. Regulators cannot assume that human decisions universally will be superior to machine decisions such that a right to a human-made decision should be enshrined in law.[133] In some cases, machine decisions might be more accurate, fair, or equitable than fallible human decision-makers. Huq therefore urges policymakers to consider articulating a right to a "well-calibrated machine decision" which would still address the transparency, fairness, and explainability concerns that facial recognition technology raises.[134] This right could be superior in many instances to the right to a human decision, where the unique biases of a human reviewer could cause even worse discrimination.[135]

III. Facial Recognition Technology Can Tangibly and Uniquely Violate the Privacy Rights of LGBTQ Individuals

This Part explores the importance of privacy rights to the LGBTQ community and how facial recognition technology threatens those rights. Privacy rights violations can be dignitary harms that impact everyone. But these violations can have particularly potent effects for LGBTQ individuals. Facial recognition technology can erode control over LGBTQ individuals' biometric data, which, although difficult to quantify in monetary terms, has been statutorily protected in certain jurisdictions. The implications of this erosion of privacy are described in the following Subparts.

A. *The Importance of Privacy for the LGBTQ Community*

There is a lingering assumption underlying this discussion of privacy rights for the LGBTQ community: that one's sexual orientation is something worth keeping secret. This assumption arguably perpetuates animosity and discrimination toward LGBTQ individuals. The LGBTQ community has attempted to counter these societal assumptions through

April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) (EU); *see* Huq, *supra* note 126 at 622–23 (explaining that Article 22(1) of the European Union's General Data Privacy Regulation vests natural persons with a "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.").

[132] Huq, *supra* note 126 at 687.

[133] *Id.* at 622.

[134] *Id.* at 619.

[135] *Id.*

pride parades and other visibility campaigns. Supervisor Harvey Milk, for example, famously pressured his LGBTQ brothers and sisters by telling them, "you must come out."[136] Yet, the above Part illustrates how harmful discrimination against the LGBTQ community persists, which is why privacy protections are still necessary.

Unfortunately, LGBTQ individuals still can face many grievous harms if they are outed against their will. If homophobic actors can deploy facial recognition technology in all social settings uninhibited, it could result in unwanted harassment, hate crimes, forced conversion therapy, and bullying both online and in person. School officials who out a student to their parents, for instance, could catalyze unintended consequences such as abuse, suicide attempts, or the student being thrown out of their home.[137] These scenarios highlight the value of privacy protections for LGBTQ individuals. They also illustrate how sexual orientation-detecting facial recognition software implicates both decisional privacy rights and restricted access privacy rights.

Of course, it would be preferable for society to accept fully the LGBTQ community. But that ideal is not yet reality. The "closet" has been central to LGBTQ experiences for centuries now. Privacy rights are thus incredibly valuable to the LGBTQ community. If, when, how, and under what circumstances an LGBTQ person comes out of the closet are choices over which the law should give such individuals full autonomy. Such a view would recognize the fact that, unfortunately, many corners of American society react with varying degrees of hostility toward openly LGBTQ individuals. The next two Subparts discuss the unique ways in which the public and private sectors' use of sexual orientation-detecting facial recognition technology could violate the privacy rights of LGBTQ individuals.

B. *Government Actors' Violation of LGBTQ Privacy Rights*

Government actors are already using facial recognition software in the criminal investigation context. Absent increased regulation and judicial oversight, government officers could continue to expand the technology's use. One could conceive that a police officer might attempt to use sexual orientation-detecting AI to identify a suspect about whom he knows very little except for the fact that she is a lesbian. If he had photos of five potential suspects, the officer could run a sexual orientation-detecting

[136] Bstewart23, *Harvey Implores*, YouTube at 0:30 (Nov 22, 2008), https://www.youtube.com/watch?v=UvZIoZNYTN8 [https://perma.cc/JWT5–5AM5] (featuring a compilation of snippets of newspaper articles and excerpts of Harvey Milk's speeches).

[137] *See, e.g.*, Sterling v. Borough of Minersville, 232 F.3d 190, 196 (3d. Cir. 2000); Letter from James D. Esseks, Director, ACLU LGBTQ & HIV Project, to Principal or Superintendent. (Aug. 26, 2020) (on file with the ACLU and available at: https://www.aclu.org/letter/open-letter-schools-about-LGBTQ-student-privacy) [https://perma.cc/ZP3Z-VCJS].

face scan on each photo to lead him in the right direction. Courts could rely on recent Fourth Amendment precedent, however, to classify this as an unreasonable search.[138] The Supreme Court in cases such as *Carpenter v. United States*[139] and *Riley v. California*[140] has extended Fourth Amendment protection to cover aggregated digital data. Those cases restricted the government's use of GPS and cell phone data tracking technology for law enforcement purposes. Sexual orientation-detecting facial recognition technology could similarly infringe this expectation of privacy.

While courts have declined to find a search for the purposes of the Fourth Amendment where a camera merely captures an image of a person in a public space, conducting facial recognition analysis on such an image is different. The technology involved in facial recognition scans are intrusive enough to rise to the level of a search.[141] The FBI's FACE technology discussed above, for instance, analyzes the biometric data of its subjects and compares it against the "peaks and ridges" of other individuals' facial images in its database.[142] In doing so, "the FBI is essentially searching the contours of a subject's face for criminality."[143] Without a proper warrant, this analysis violates the Constitution because it involves "searching for similarities between a vessel of known and unknown criminality."[144]

There are also dignitary harms involved in the government's violation of LGBTQ individual's privacy rights. The facial scan used by the technology would reveal sensitive information that the average human has no better chance of guessing correctly than a coin-flip.[145] Once the software outed an LGBTQ person as lesbian, gay, bisexual, or transgender, the technology unreasonably infringed upon the person's privacy

[138] *See* Elizabeth Snyder, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition Technology to Conduct Unlawful Searches*, 68 SYRACUSE L. REV. 255, 261–62. at 261–62. *See also* Kyllo v. United States, 533 U.S. 27 (2001) (holding that where a government uses a scanning device to explore the details of a private home that would previously have been unknowable without physical inspection, the scan constitutes a Fourth Amendment search, and is presumptively unreasonable without a warrant); United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring to assert that *Katz*'s reasonable expectation of privacy test must take into account technological developments and analyze whether "people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain" political viewpoint, religious practices, sexual habits, and so on).

[139] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[140] Riley v. Cal., 573 U.S. 373 (2014).

[141] Snyder, *supra* note 135.

[142] *Id.*

[143] *Id.* at 262.

[144] *Id.*

[145] *See* Wang & Kosinski, *supra* note 1, at 253 (finding that the average human can correctly detect sexual orientation with an accuracy rate of about 55–65 percent).

rights concerning when and how the person defines their identity.[146] This right was articulated in *Lawrence v. Texas*.[147] The Court there emphasized that "at the heart of liberty is the right to define one's own concept of existence."[148]

The Supreme Court in *Whalen v. Roe* has recognized the constitutional right of an individual to control the "nature and extent of highly personal information released about" that individual.[149] This right restricts government entities from disclosing information about deeply personal matters, such as sexual orientation. The Court also characterized the "accumulation of vast amounts of personal information in computerized data banks or other massive government files" as an explicit threat to privacy rights.[150] The Court emphasized that the rule of law requires that data "which is personal in character and potentially harmful if disclosed" be protected.[151] And as the Third Circuit has stated, "it is difficult to imagine a more private matter than one's sexuality and a less likely probability that the government would have a legitimate interest in disclosure of sexual identity."[152] Nonconsensual disclosure of an individual's sexual orientation could also run afoul of sex discrimination laws; for example, it could amount to harassment or creation of a hostile work environment for purposes of Title VII.[153] Thus, LGBTQ individuals have a particularized privacy interest in preventing nonconsensual disclosure of their sexual orientations and gender identities, and this interest extends to interactions with both the government and private parties.

It follows that sexual orientation-detecting facial recognition technology poses a heightened risk for LGBTQ individuals. For the government, use of this technology is effectively a search under the Fourth Amendment, and must be restricted.[154]

[146] This of course assumes that parties have the means to bring such a suit and the evidence to support a claim. One may not have knowledge that the government or another entity has conducted a facial recognition scan. Therefore, it would be preferable through regulation or legislation to impose affirmative duties on the government and private entities wishing to use facial recognition technology.

[147] Lawrence v. Tex., 539 U.S. 558 (2003).

[148] *Id.* at 574.

[149] Letter from James D. Esseks to Principal or Superintendent, *supra* note 134.

[150] Whalen v. Roe, 429 U.S. 589, 605 (1977).

[151] *Id.*

[152] Sterling v. Borough of Minersville, 232 F.3d 190, 196 (3d. Cir. 2000).

[153] *See* Letter from James D. Esseks to Principal or Superintendent, *supra* note 134; *cf.* Roberts v. Clark Cty. Sch. Dist., 215 F. Supp. 3d 1001, 1017 (D. Nev. 2016) (leaving to the jury to decide whether disclosure of plaintiff's transgender status in a department email established a prima facie case for harassment/hostile environment under Title VII's sex discrimination prohibition).

[154] *See* Snyder, *supra* note 135.

C. *Private Actors and Data Privacy Violations*

This Subpart discusses how data privacy laws impact sexual orientation-detection facial recognition technology. Data privacy violations tend to implicate private actors and their economic interests because many companies' business models today increasingly rely on analyzing large quantities of user data.[155] A relevant case of note is *Patel v. Facebook*, where the Ninth Circuit allowed a suit against Facebook to proceed on the grounds that Facebook's facial recognition software violated Illinois' 2008 biometric data protection law.[156] The outcome of this suit could have significant implications for how online entities such as Facebook deploy facial recognition technology.

In *Patel*, the Ninth Circuit affirmed the certification of a class of Facebook users who alleged that Facebook's facial recognition technology violated Illinois's Biometric Information Privacy Act (BIPA).[157] BIPA is one of the most protective laws of biometric data in the U.S., prohibiting private entities from collecting, capturing, purchasing, or receiving through trade a person's biometric information without the owner's informed consent.[158] The panel held that plaintiffs had alleged a concrete and particularized harm that was sufficient to confer standing because the statutory provisions of BIPA were intended to protect concrete interests in privacy.[159] In this case, the claim that Facebook's use of facial-recognition technology on its platform without explicit consent was initially found to invade an individual's private affairs and concrete interests.[160]

Patel could be the first in a line of precedent cases that assigns a tangible value to biometric data and subjects the exploitation of facial recognition technology to privacy tort lawsuits. The tort system could provide a viable method for regulating the use of facial recognition technology on LGBTQ individuals.

To further prove its point, the Ninth Circuit cited the recent expansion of the Supreme Court's application of traditional privacy protections to technological innovations. The Court cited *Carpenter v. U.S.*[161]

[155] Ken Dai & Jet Deng, *Big Data and Antitrust Risks in Close-Up: From the Perspective of Real Cases*, 30 No. 2 Competition: J. Anti., UCL & Privacy Sec. Cal. L. Assoc. 36 (2020).

[156] Patel v. Facebook, 932 F.3d 1264 (9th Cir. 2019).

[157] *Id.*

[158] *Litigation Breeding Ground: Illinois' Biometric Information Privacy Act*, National L. Rev. (Mar. 2021), https://www.natlawreview.com/article/litigation-breeding-ground-illinois-biometric-information-privacy-act [https://perma.cc/PUR3-SVYJ].

[159] *Patel*, 932 F.3d at 1275.

[160] *Id.* at 1273 (highlighting that Facebook violated sections 15(a) and 15(b) of BIPA by collecting, using, and storing biometric identifiers, a "scan" of "face geometry," from their photos without obtaining a written release and without establishing a compliant retention schedule).

[161] Carpenter v. United States, 138 S. Ct. 2206 (2018).

for the Supreme Court's recognition of the high likelihood of future development of AI technology.[162] The Ninth Circuit court speculated that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building.[163] Alternatively, a biometric face template could be used to unlock the facial recognition lock on that individual's mobile phone, resulting in a significant data privacy breach.[164] The court concluded that the use of facial recognition technology without consent invades an individual's concrete privacy interests.[165] The final outcome in this case could have significant implications on the reach of facial recognition technology and encourage other state lawmakers to enact similar privacy protection laws that would protect historically oppressed groups like those within the LGBTQ community.

D. *Native Advertising as a Deceptive Trade Practice and Violation of Privacy*

Native advertising at first glance might seem harmless and free from the possibility of discrimination. It is a type of paid advertising that matches the look and feel of the media format in which it appears. It is meant to provide more targeted ads in a format pleasing to the relevant audience. For example, native advertising appearing in Facebook or Instagram feeds are made to look like posts from friends, when in reality they are ads from companies. Facial recognition technology can aid advertisers by identifying particular traits of online users that help them determine which ads to broadcast to those users. A user that is identified as LGBTQ through facial recognition analysis of his social media posts, for instance, might receive targeted ads of rainbow pattern clothing during Pride Month.[166]

The general presumption is usually that this practice is consistent with free market principles. Yet, the Department of Housing and Urban Development, the ACLU, and employment law firm Outten & Golden LLP have filed suits against social media platforms for allowing advertisers to target customers with ads based on race, religion, national origin, and other protected traits.[167] While the settlement agreements reached

[162] *See* Patel, 932 F.3d at 1273.

[163] *Id.*

[164] *Id.*

[165] In granting standing, the court found that an invasion of an individual's biometric privacy rights "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549, (2016)). This proved sufficient to allow the suit against Facebook to go forward under the Illinois BIPA.

[166] *See* Chris Stokel-Walker, *Facebook's Ad Data May Put Millions of Gay People at Risk*, New Scientist (Aug. 24, 2019) https://www.newscientist.com/article/2214309-facebooks-ad-data-may-put-millions-of-gay-people-at-risk [https://perma.cc/56KU-9EHW].

[167] John D. McKinnon & Jeff Horwitz*, HUD Action Against Facebook Signals*

between Facebook and these entities did not specify the extent to which Facebook utilized facial recognition technology to target its ads, lawsuits like these illustrate the privacy and antidiscrimination concerns that arise from native advertising, and suggest some standards that tech companies should be held to if they wish to use facial recognition.

The FTC is also finding that some advertising practices go too far, especially when they constitute deceptive intrusions on users' privacy. Targeted native advertising could therefore be found to have the combined effect of infringing upon LGBTQ individuals' biometric data privacy while also subjecting them to unfair and deceptive advertising practices. The FTC can use its broad common law-like authority under the FTC Act to define unfair and deceptive trade practices.[168] Some states create similar state-level authorities through laws such as California's Unfair Competition Act.[169] This power has been extended into the digital realm. In *FTC v. Wyndham Worldwide Corp*, for example, the Third Circuit found that the FTC had authority to regulate data security of companies' online servers.[170] The FTC used this authority to extract a $5 billion settlement out of Facebook for its alleged violation of a 2012 FTC order.[171]

The 2019 fine relied in part on the fact that Facebook misrepresented users' ability to control the use of facial recognition technology with their accounts. According to the FTC complaint, Facebook's 2018 data policy deceived many millions of users who inadvertently allowed Facebook's facial recognition software to scan their photos because the "Tag Suggestions" setting was turned on by default.[172] The data policy,

Trouble for Other Platforms: Department Accuses Social Media Firm of Fostering Discrimination in Advertising Based on Race, National Origin, Religion, and More, WALL ST. J. (Mar. 28, 2019), https://www.wsj.com/articles/u-s-charges-facebook-with-violating-fair-housing-laws-11553775078 [https://perma.cc/K9SH-VRX3]; *Facebook Agrees to Sweeping Reforms to Curb Discriminatory Ad Targeting Practices*, ACLU (March 19, 2019), https://www.aclu.org/press-releases/facebook-agrees-sweeping-reforms-curb-discriminatory-ad-targeting-practices [https://perma.cc/84SK-L64R].

[168] 15 U.S.C. §§ 41–58 (2012); *see also* FED. TRADE COMM'N, ENFORCEMENT POLICY STATEMENT ON DECEPTIVELY FORMATTED ADVERTISEMENTS (2015), https://www.ftc.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf [https://perma.cc/C2YK-FQDK].

[169] *E.g.* California Unfair Competition Law, CAL. BUS. & PROF. CODE §§ 17200–17209 (West 2021).

[170] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 249 (3d Cir. 2015); *see also Administrative Law – Federal Trade Commission Act – Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability* – FTC v. Wyndham Worldwide Corp., *799 F.3d 236 (3d Cir. 2015)*, 129 Harv. L. Rev. 1120 (2016).

[171] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FTC PRESS RELEASES (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/65Q3-MFDT].

[172] *Id.*

however, implied that users would by contrast have the power to opt-in to having facial recognition software active on their accounts.[173] The resulting fine shows that U.S. courts and regulators are beginning to intervene to demand transparency from tech companies that use facial recognition technology on their users.

The FTC has been aware of facial recognition technology in the workplace since at least 2011 when it convened a working group on facial recognition technology.[174] The FTC issued a report following its working group that made three recommendations for best practices.[175] These included "privacy by design," "simplified consumer choice," and "transparency."[176] Notably, Commissioner J. Thomas Rosch dissented from the report's findings, arguing that they went "too far" and questioning whether the privacy invasions of the technology could ever rise to the level of substantial injury.[177] Coupled with that dissent, the fact that these findings were merely recommendations for best practices and not actually requirements could suggest that the FTC may be reluctant to take bold regulatory steps with this new technology. Yet, the FTC cases cited above provide countervailing evidence of an increasing willingness on the part of the FTC to protect consumer privacy. These regulatory actions demanding increased privacy protections, user choice, and transparency will have positive effects for the LGBTQ community and should be swiftly adopted.

IV. Proposed Legislative, Regulatory, and Judicial Approaches to Sexual Orientation-Detecting Facial Recognition Technology

Potential reforms of facial recognition technology fall into three main categories: legislative, regulatory, and judicial. This Part provides a summary of the main possible reforms for protecting LGBTQ people, and addresses counterarguments, based on our current understanding of this technology and its possible uses with respect to that population.

A. *Legislative Approaches*

Federal lawmakers should move to pass a U.S. version of Europe's GDPR. The law applies to facial recognition companies anywhere in the world that provide their services to European Union citizens. One

[173] *Id.*

[174] Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies i (Fed. Trade Comm'n ed. Oct. 2012) https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/9YB5-SW5U].

[175] *Id.* at 2.

[176] *Id.*

[177] *Id.* at A1.

notable provision of the GDPR articulates the right to be forgotten.[178] Under this provision, companies such as Facebook must create methods for scrubbing and permanently deleting data at an applicant's request. This provision is something lawmakers and regulators in the United States should consider as well.

Unfortunately, Congress' current polarization hinders swift passage of any legislation. Recent hearings on facial recognition technology in the House of Representatives, however, highlighted bipartisan interest in its negative impacts.[179] Individual representatives and Senators have introduced bills to study, restrict, or outright prohibit facial recognition technology.[180] For example, the George Floyd Justice in Policing Act, which has passed the House of Representatives, would limit uses of facial recognition technology if enacted.[181]

In spite of recent Congressional interest in studying facial recognition technology, a privacy bill has not yet been highlighted as a priority by the Biden Administration. But data privacy is a pressing issue, and federal lawmakers should implement strict limits on the use of facial recognition technology so as to prevent discrimination. While it is true that no private company has a "monopoly on math," Congress could legislate private rights of action to sue companies and government agencies that use facial recognition AI to infringe personal information such as one's sexual orientation. This kind of provision would provide a powerful disincentive for companies like Clearview AI to develop their technology without safeguards and sell it to any company willing to pay the right price.

San Francisco has banned its law enforcement from using facial recognition technology.[182] The federal government should do the same

[178] Regulation 2016/679, *supra* note 128, 43–44.

[179] Sabrina Eaton, *Facial Surveillance Draws Bipartisan Concern in Congress*, GOV'T TECH. (Jan. 16, 2020), https://www.govtech.com/policy/Facial-Surveillance-Draws-Bi-Partisan-Concern-in-Congress.html [https://perma.cc/MC8E-KN3H]; *see also Facial Recognition Technology*, *supra* note 15.

[180] Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. § 4 (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3284 [https://perma.cc/RAR6-CP9C]; Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. § 3(a) (2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084 [https://perma.cc/CJ6C-TE4F]; Facial Recognition and Biometric Technology Moratorium Act of 2020, H.R. 7356, 116th Cong. § 3(a) (2020), https://www.congress.gov/bill/116th-congress/house-bill/7356 [https://perma.cc/X493-V5WH]; George Floyd Justice in Policing Act of 2020, H.R. 7120, 116th Cong. § 372(g) (2020), https://www.congress.gov/bill/116th-congress/house-bill/7120 [https://perma.cc/V3GX-A2AV]; Advancing Facial Recognition Act, H.R. 6929, 116th Cong. § 2 (2020), https://www.congress.gov/bill/116th-congress/house-bill/6929 [https://perma.cc/42BT-7C6D].

[181] Tom Simonite, *A Bill in Congress Would Limit Uses of Facial Recognition*, WIRED (June 12, 2020), https://www.wired.com/story/bill-congress-limit-uses-facial-recognition [https://perma.cc/M6AQ-6EXV].

[182] Kate Conger, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES

or consider implementing warrant-like guardrails on the use of facial recognition technology.[183] We cannot merely rely on the good faith of democratically unaccountable corporations like Twitter, Facebook, and Google to privately regulate these matters. Their business models prevent them from being interested in doing so effectively. This is an issue that must be dealt with at the federal level. Because of the cross-border nature of the internet, a patchwork of differing state laws would only serve to create safe havens for nefarious actors and harmful technology.

Congress could mandate that employers ask for explicit consent before using facial recognition technology on job applications. Applicants should not be penalized if they decline to consent to facial recognition assessments and should be offered the chance to request in-person interviews instead. Applicants who do submit to facial recognition assessments should be able to request a full report detailing the analysis and scoring produced by the facial recognition technology. The Illinois legislature passed an act that requires employers to notify, inform, and obtain consent from employees before subjecting them to facial recognition scans.[184] This sort of practice would cut down on information asymmetry in hiring.

Although action at the federal level may seem distant, states and localities have been enacting productive legislation that could be used as blueprints for Congress. New York suspended the use of facial recognition technology in schools and commissioned a study of how it should be implemented, if at all.[185] California's Consumer Privacy Act of 2018 provides strong biometric data protections, the right to have personal data stored by entities deleted, and the right to consent before information is collected, which would apply to facial recognition scans.[186] These proactive actions should be replicated across the country by state legislatures in the absence of Congressional action to ensure the protection of all LGBTQ people across the country.

(May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/9PAW-NHGT].

[183] *See* Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084 [https://perma.cc/733H-4ZUG].

[184] Public Act 101–0260, HB2557, 101st General Assembly, (2019), https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=101–0260 [https://perma.cc/4AST-E4AS].

[185] Press Release, *Governor Cuomo Signs Legislation Suspending Use and Directing Study of Facial Recognition Technology in Schools*, New York State Governor (Dec. 22, 2020), https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-suspending-use-and-directing-study-facial-recognition [https://perma.cc/LP2R-SPMT].

[186] California Consumer Privacy Act of 2018, A.B. 25 (Oct. 14, 2019). *See* Justine Phillips, *Big Bang! California Expands Employee Privacy Rights & Insights from the Office of Attorney General*, Labor and Employment Law Blog, (Oct. 14, 2019), https://www.laboremploymentlawblog.com/2019/10/articles/privacy/ccpa-employee-rights [https://perma.cc/VUL2–86TS].

B. *Administrative and Regulatory Approaches*

The core reform needed for agencies using facial recognition is adopting the practice of AIAs for all their uses of facial recognition technology. This procedure would amount to a public airing of the facial recognition methods before they go into effect. AIAs would ensure that "both the agency and the public . . . [can] evaluate the adoption of an automated decision system before the agency has committed to its use."[187] AIAs would allow time to identify public concerns that may need to be negotiated or otherwise addressed before a contract is signed to use artificial intelligence tools in a governmental capacity, including those of LGBTQ people. These concerns could then be translated into changes in the algorithm's metrics. Many of the artificial intelligence systems used by administrative agencies are already produced in-house.[188] Therefore, AIAs are also less likely to run afoul of trade secrets defenses brought by private facial recognition companies.

As explained in the government hiring Part above,[189] AIAs would resemble the notice and comment period required for administrative rulemaking regulations.[190] In the same way that federal agencies must provide a public notice and comment period before promulgating a rule, agencies should do the same before implementing decision-making procedures based on algorithms and AI.[191] Analogizing AIAs to rulemaking would lend some legitimacy to adequately-assessed facial recognition technology. Moreover, *Heckler v. Campbell* has made clear that agencies can permissibly base the parameters of administrative decisions on frameworks laid out in prior rulemakings that resolve certain classes of issues.[192] The AIA could function as a prior rulemaking that lays out the parameters for how facial recognition technology will be involved in administrative decision-making. If the AIA framework functions correctly, procedural bias against LGBTQ applicants and employees could be significantly diminished.

[187] Reisman et al., *supra* note 103, at 8.

[188] Talley, *supra* note 106 (quoting Professor David Engstrom of Stanford Law as saying that in most cases the technologies used by government agencies "were developed in house by agency technologists, not by profit-oriented contractors") [https://perma.cc/E9U4-N5DQ].

[189] *See supra* Part II.D.2.

[190] 5 U.S.C. § 553c (2012) ("After notice required by this section, the agency shall give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation.").

[191] Reisman et al., *supra* note 103, at 16.

[192] Heckler v. Campbell, 461 U.S. 458, 467 (1983) (holding that agencies may rely on rulemakings to resolve certain classes of issues).

C. *Judicial Approaches*

Armed with a new line of precedents and executive orders, the LGBTQ community must begin to think about how to bring employment discrimination and privacy violation types of suits to enact safeguards that affirmatively prevent this type of discrimination. While some states have statutes prohibiting discrimination on the basis of sexual orientation and gender identity, federal law under Title VII was only recently clarified to protect against the same in *Bostock v. Clayton County*.[193] As a result, LGBTQ individuals who feel they have been discriminated against by facial recognition technology during the hiring process now have recourse in many states' court systems as well as within the federal system.

Judges can now rely on the *Bostock* decision and its interpretation of the widely used "because of sex" statutory language to extend protections to LGBTQ individuals who face discrimination or loss of privacy rights. With respect to LGBTQ-detecting facial recognition technology specifically, depending on what form of explainability prevails, the technology could be described as making determinations "because of sex" or due to sex stereotyping.[194] If the technology arrives at a biased determination, this framing of the complaint could allow the judge to grant discovery, forcing the parties to produce a deeper assessment of the technology's methods, uses, and applications.

It should also be noted that cisgender straight employees can also suffer from employment discrimination because they are perceived to be LGBTQ by their employer. Those employees may also file Title VII claims individually or with the EEOC. It is possible that facial recognition technology, for instance, could incorrectly identify a job applicant as gay and a biased employer could reject him as a result. That applicant would also have been discriminated against because of sexual orientation. Straight cisgender employment discrimination claimants have previously faced similar difficulties in challenging their dismissals or workplace conditions on these grounds,[195] but *Bostock* should make these claims easier to bring.

D. *A Jurisprudential Silver Lining?*

Facial recognition technology that accurately detects sexual orientation based on external physical analysis could change how society perceives the LGBTQ community because it challenges the notion that LGBTQ individuals have the liberty to decide their identity. Sexual orientation-detecting technology theoretically makes the LGBTQ identity independently and externally verifiable, and therefore more easily

[193] Bostock v. Clayton County, 140 S. Ct. 1731, 1754 (2020).

[194] *See* Price Waterhouse v. Hopkins, 490 U.S. 228, 240 (1989).

[195] *See* Guess v. Phila. Hous. Auth., 354 F. Supp. 3d 596, 599 (E.D. Pa. 2019).

perceptible by the general public. This erodes the privacy rights of the LGBTQ community. Yet, this change could strengthen the LGBTQ community's claim to intermediate or even strict scrutiny under the Fourteenth Amendment in cases involving government action.

Currently, constitutional claims of sexual orientation discrimination receive only rational basis review under the Fourteenth Amendment, although scholars argue over whether the actual level of scrutiny is slightly higher than ordinary rational basis review.[196] While the Court upholds almost any law or policy analyzed under rational basis review, government action reviewed by courts using strict scrutiny is usually found constitutionally defective.[197] Because all four opinions related to unconstitutional discrimination based on sexual orientation were written by Justice Kennedy and lacked clear doctrinal explanations, however, the precise contours of constitutional protections for the LGBTQ community are blurry. The usual elements used by courts to determine whether to elevate the applicable tier of scrutiny under an Equal Protection Clause analysis consist of a history of discrimination, the use of a trait unrelated to merit, the political powerlessness of the group in question, and the immutability of the trait.[198] In Justice Kennedy's opinions in *Romer v. Evans*, *U.S. v. Windsor*, *Lawrence v. Texas*, and *Obergefell v. Hodges*, there is no mention of the tiers of scrutiny. Justice Kennedy does make passing reference to the "immutable nature" of sexual orientation in *Obergefell*, but that is the only reference to the traditional criteria for elevating the applicable tier of scrutiny within his opinions.[199] He instead relies on notions of human dignity that are protected by a synergistic reading of the Equal Protection and Due Process Clauses of the Fourteenth Amendment.[200]

The tiers of scrutiny method was originally developed to allow for the analysis of claims of unconstitutional discrimination based on race. Legal advocates such as Justice Ginsburg relied on this framework to expand protections and develop what is known as intermediate scrutiny for use in claims of unconstitutional discrimination on the basis of sex, among other claims. Intermediate scrutiny applies in cases where the government action negatively affects a protected class, but that action can nonetheless be constitutional if it furthers an important government

[196] *See* Gayle Lynn Pettinga, *Rational Basis with Bite: Intermediate Scrutiny by Any Other Name*, 62 IND. L. REV. 779 (1987).

[197] *See, e.g.*, Gerald Gunther, *Foreword: In Search of Evolving Doctrine on A Changing Court: A Model for A Newer Equal Protection*, 86 HARV. L. REV. 1, 8 (1972); *see also* Fullilove v. Klutznick, 448 U.S. 448, 507 (1980) (Powell, J., concurring).

[198] *See e.g.*, Frontiero v. Richardson, 411 U.S. 677 (1973); United States v. Carolene Prod. Co., 304 U.S. 144, n.4 (1938).

[199] Obergefell v. Hodges, 135 S.Ct. 2584, 2594 (2015).

[200] *See* Pamela S. Karlan, *Equal Protection, Due Process, and the Stereoscopic Fourteenth Amendment*, 33 MCGEORGE L. REV. 473, 474 (2002).

interest in a way substantially related to that interest.[201] The cases related to LGBTQ discrimination started with an anti-animus justification in *Romer*.[202] In *Lawrence*, however, Justice Kennedy began to develop his synergistic reading of the Equal Protection and Due Process Clauses to strike down anti-sodomy laws as violations of the fundamental human dignity of LGBTQ individuals.[203] This synergistic reading of the two clauses and dignitary justification for constitutional protection led to *Windsor* and *Obergefell.*[204] Yet, *Windsor* and *Obergefell* were both 5–4 decisions that depended on Justice Kennedy's vote. Current justices on the Supreme Court are more likely to seek doctrinal clarity in this realm of the law than did Justice Kennedy, possibly jeopardizing the jurisprudential basis for many recent gains for the LGBTQ community.

Sexual orientation-detecting facial recognition technology could convince more conservative judges that sexual orientation is an immutable trait. If the technology assessed in Wang and Kosinski's study really is linking superficial physical features to sexual orientation, sexual orientation begins to look more like race, sex, and national origin. This realization would weaken any lingering conceptions that LGBTQ individuals can choose their sexual orientation and could simply abandon it at will if they wished; race, sex, and national origin do not usually require others to have mere faith in the word of the individual whose identity is in question. These protected characteristics are either superficially obvious or can be independently verified by an official document like a birth certificate. Individuals in the LGBTQ community, by contrast, have had an affirmative duty to come out. Anyone skeptical of those LGBTQ individuals' identity had little recourse but to take them at their word. Of course, facial recognition technology could externalize the decisional power to come out that is central to many LGBTQ people, thus depriving them of their autonomy. The LGBTQ community has not had to grapple with such a possibility before the advent of facial recognition software, so it remains to be seen whether the community would support such a loss. However, this technology could create an independently verifiable and therefore more superficially perceptible method for people to confirm someone's status as an LGBTQ person. This would seemingly strengthen the argument of the immutability of the LGBTQ identity under the Court's Fourteenth Amendment frameworks, and might therefore prove advantageous to some LGBTQ litigants.

The other factors in the jurisprudential analysis—history of discrimination, the trait being unrelated to merit, and the relative political powerlessness—would likely remain similar for the LGBTQ community as they have been prior to the development of this technology. It

[201] *See* Craig v. Boren, 429 U.S. 190 (1976).

[202] *See* Romer v. Evans, 517 U.S. 620 (1996).

[203] *See* Lawrence v. Texas, 539 U.S. 558 (2003).

[204] U.S. v. Windsor, 570 U.S. 744 (2013); *Obergefell*, 135 S.Ct. 2584.

would seem from these factors that the LGBTQ community could have an equally strong claim to intermediate scrutiny as women have under the Court's jurisprudence, and potentially even a claim for strict scrutiny. LGBTQ people are a relatively small percentage of the population, self-identifying at 4.5 percent of the adult U.S. population per recent research, whereas women form over 50 percent of people in America.[205] The small population makes it difficult to build political power through numbers, which perhaps justifies increased protection for the LGBTQ community. One also need look no further than the Supreme Court's own jurisprudence in cases such as *Bowers v. Hardwick* to illustrate a history of discrimination against LGBTQ individuals.[206] Lastly, the possibility that there are so-called "real differences" between men and women, which the Court relied on in granting sex discrimination constitutional claims only intermediate scrutiny, does not apply to sexual orientation.[207] To the extent they may exist, physical differences between LGBTQ and cisgender heterosexual people are likely imperceptible by humans and would be unrelated to the merit of any government program they might benefit from.

It is also worth noting that even if sexual orientation-detecting technology is not perfectly accurate, it still strengthens the LGBTQ claim to the immutability prong of Equal Protection Clause analysis. In other protected groups, there are also fringe cases. For example, a white woman who has dark hair and skin could be mistaken for a Latina woman. If she is denied a government job as a result of her perceived race, she is still discriminated against because of race in violation of the Equal Protection Clause. Similarly, if a heterosexual man is identified as a gay man by a facial recognition scan and loses his government job as a result, he should also be found to have been discriminated against because of sex in violation of the Equal Protection Clause. If the results of this sexual orientation-detecting technology are incorrect, but they still result in discrimination because of animus towards the LGBTQ community, the legal—and depending on the facts, constitutional—violation likely still exists. If this technology does develop unchecked by regulation, judges should ground their analysis of the technology's discriminatory effects in either the intermediate or strict scrutiny tiers for those employers and other actors bound by constitutional guarantees.

This analysis, however, brings with it a range of problematic assumptions about LGBTQ identities. Sexual orientation for many is seen as

[205] Kerith J. Conron & Shoshana K. Goldberg, *Adult LGBT Population in the United States*, WILLIAMS INSTITUTE (July 2020) https://williamsinstitute.law.ucla.edu/wp-content/uploads/LGBT-Adult-US-Pop-Jul-2020.pdf *[https://perma.cc/S66R-5EGF]; Quick Facts*, U.S. CENSUS https://www.census.gov/quickfacts/fact/table/US/LFE046219 [https://perma.cc/N3NC-NCRH].

[206] *See* Bowers v. Hardwick, 478 U.S. 186 (1986).

[207] *Cf.* Virginia Military Institute v. United States, 508 U.S. 946 (1993).

something that is fluid and subject to evolve over a lifetime. People should have the freedom to experiment with their sexualities, be that for periods of their lives or for their entire lifetimes. Understanding why one loves or feels sexually attracted to another is something humans have struggled to understand for millennia. This could be one explanation for why Justice Kennedy felt compelled to wax poetic about the "mystery of human life" in *Lawrence.*[208]

A facial recognition assessment of someone could work to rigidly solidify their legal fate in the eyes of society and courts, which is yet another reason to restrict the use of this technology. If an algorithm we create purports to define for individuals what their sexual orientation is, it could equip conservative jurists with logical ammunition to constrain and oversimply the LGBTQ identity. It could also be used to diminish the work of scholars such as Alfred Kinsey, who explained sexuality as a spectrum as opposed to a black and white reality.[209] If this technology were given too much weight in the legal world, it could erode the liberty rights of LGBTQ individuals that Justice Kennedy articulated in *Lawrence* and *Obergefell*. According to Justice Kennedy, liberty under the Constitution allows "persons, within a lawful realm, [] to define and express their identity."[210] Therefore, it is more important for lawmakers to focus on regulating and restricting the use of this technology and its development as discussed above.

Thoughtful jurists should take all these considerations into account when articulating new doctrinal boundaries for Fourteenth Amendment protections against sexual orientation discrimination. The ultimate takeaway from this analysis is that given current Fourteenth Amendment jurisprudential frameworks, discrimination grounded in animus of oppressed groups such as the LGBTQ community should not be constitutionally tolerated. If the facial recognition algorithm really is detecting sexual orientation based on physical traits, it could open the door to new, easier, and novel instances of discrimination against LGBTQ individuals forced out of the closet against their will. Constitutional law should protect them against such discrimination while also preserving the liberty of LGBTQ individuals to continuously define their identities.

Conclusion

As sexual orientation-detecting facial recognition technology becomes more widespread, our legal systems will have to adapt to protect the rights and dignity of LGBTQ individuals. There are jurisdictions in America that have taken the lead in this regulation. For example, California banned the use of facial recognition technology in police body

[208] *See Lawrence*, 539 U.S. at 574.

[209] *See* Alfred C. Kinsey, Sexual Behavior in the Human Male, 1948.

[210] *See* Obergefell v. Hodges, 135 S.Ct. 2584, 2593 (2015).

cams.[211] Similarly, the San Francisco Board of Supervisors has banned the use of facial recognition technology by county entities.[212] New York City was the first to commission an automated decision system task-force.[213] These peremptory regulations are smart policy as AI technology becomes more sophisticated and threatens the rights and dignity of the LGBTQ community.

This Note examined several areas of law where sexual orientation-detecting facial recognition technology will soon make an impact: employment discrimination, privacy rights, and equal protection jurisprudence. While there is more research to be done into other bodies of law that this technology will affect, this Note aims to start the discussion of some key issues. Race and sex can never be hidden in the way one could theoretically hide sexual orientation. Facial recognition technology could change that by forcing individuals in the LGBTQ community out of the closet in certain situations where their safety or dignity could be compromised. This Note raises the question of whether the right of privacy is something the LGBTQ community should continue organizing around. Women and people of color for the most part do not have decisional privacy rights over when and how to disclose their gender or race. Yet, so long as persistent homophobia, transphobia, and other forms of discrimination target the LGBTQ community, privacy will remain a valuable right for the LGBTQ community that the law must safeguard. Simultaneously, the law surrounding employment and public accommodations must push society in the direction toward equal treatment.

The LGBTQ community will have to organize to demand that lawmakers protect its members' equal access to employment opportunities and privacy rights. The community will have to continue litigating in court to invalidate instances of discrimination and privacy violations against LGBTQ individuals as unconstitutional forms of animus. Sexual orientation-detecting facial recognition technology has the potential to play a troublesome role in many legal areas. Therefore, the LGBTQ community and our lawmakers must continue to think strategically about how to limit its most deleterious effects.

[211] CAL. PENAL CODE § 832.19 (West 2020)..

[212] Conger, *supra* note 179.

[213] Rashida Richardson, ed., *Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force*, AI NOW INSTITUTE (Dec. 4, 2019) https://ainowinstitute.org/ads-shadowreport-2019 [https://perma.cc/PBQ8-HWLL].