UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 21 | Issue 4 Article 5

5-1-2020

# Facial Recognition Technology: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility

Sarah Chun

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 21, ISSUE 4: MAY 2020

# FACIAL RECOGNITION TECHNOLOGY: A CALL FOR THE CREATION OF A FRAMEWORK COMBINING GOVERNMENT REGULATION AND A COMMITMENT TO CORPORATE RESPONSIBILITY

***Sarah Chun****

*At a fundamental level, the misuse of facial recognition endangers privacy, human rights, and constitutional rights. However, merely banning facial recognition will not address or solve the issues and risks inherent in the use of facial recognition. Rather than an outright ban, developing specific limitations controlling how or when facial recognition can be used in public or private spaces can better serve public interests. This paper suggests creating a framework that combines government regulation and a commitment to social responsibility by developers. Creating this multi-prong framework can help distribute the burden of regulating facial recognition technology amongst parties such as the government, the companies developing the technology, and the end-users. Finally, assessing the risk levels of different uses of facial recognition technology will further allow proper allocation and distribution of this burden amongst the parties.*



* J.D. Candidate, University of North Carolina School of Law, 2021. I would like to thank Theodore F. Claypoole, Tara Cho, Professor Orla Maria O'Hannaidh, and Professor Joseph E. Kennedy. I could not have written this article without their feedback. I would also like to thank the entire NC JOLT board and staff. Finally, I would like to thank my parents for the numerous sacrifices that they have made for their children and for their unconditional support.

## I. INTRODUCTION

The use and development of facial recognition technology carries promises of remarkable applications such as the identification and return of missing children and enhancement of security and safety against crime or terrorism.[1] This emerging

[1] Bernard Marr, *Facial Recognition Technology: Here Are the Important Pros and Cons*, FORBES (Aug. 19, 2019), https://www.forbes.com/sites/bernardmarr/

technology, however, is predominantly unregulated in the United States, with no federal guidance and a sparse patchwork of laws in only a few states. There are an abundance of potentially harmful uses of facial recognition, from the use of facial recognition algorithms to identify human sexual orientation[2] to the prolific use of facial recognition in China to monitor and control its citizens' actions in everything from publicly shaming people wearing pajamas in public[3] to limiting the acceptable measurement of toilet paper used by an individual within a certain allotment of time.[4] While these examples are perhaps sensational compared to some of the more common use cases of facial recognition technology, the luridness of these examples helps highlight several important legal issues and fundamental rights at stake if the development and use of facial recognition remains unregulated in the United States.

While some groups in the United States have called for a moratorium[5] or even an outright ban on the use of facial recognition

---

2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#29820f0b14d1 [https://perma.cc/A5DB-JZBY].

[2] *See generally* Michal Kosinski & Yilun Wang, *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images*, 114 J. OF PERSONALITY & SOC. PSYCHOL. 246 (2018) (describing a study in which researchers created an algorithm to attempt to predict the sexual orientation of people by examining facial images compiled from online dating websites). *But see* John Leuner, *A Replication Study: Machine Learning Models Are Capable of Predicting Sexual Orientation From Facial Images*, 48–51 (Nov. 2018) (unpublished Master's dissertation, University of Pretoria) (on file with author) (discussing that the results of another study that was not able to successfully replicate results from the Kosinski & Wang study that claimed to be able to identify sexual orientation from facial features. Leuner's study proffers that factors such as hairstyle, makeup, and lighting may have been more indicative of sexual orientation rather than facial features).

[3] Amy Qin, *Chinese City Uses Facial Recognition to Shame Pajama Wearers*, N.Y. TIMES (Jan. 21, 2020), https://www.nytimes.com/2020/01/21/business/china-pajamas-facial-recognition.html?searchResultPosition=1 [https://perma.cc/Z59A-YEBJ].

[4] Rene Chun, *China's New Frontiers in Dystopian Tech*, ATLANTIC (Apr. 2018), https://www.theatlantic.com/magazine/archive/2018/04/big-in-china-machines-that-scan-your-face/554075/ [https://perma.cc/QJT5-6WJG].

[5] Angela Chen, *40 Groups Have Called for a US Moratorium on Facial Recognition Technology*, MIT TECH. REVIEW (Jan. 27, 2020),

technology, banning facial recognition is not the correct approach. In a surprising commentary, Pope Francis stated that while there are considerable challenges and dangers in creating ethical artificial technologies, these dangers "must not detract us from the immense potential that new technologies offer."[6] Nevertheless, while a ban may not solve many of the issues inherent in facial recognition technology, due to its potentially far-reaching and profound consequences, it is evident that some limitations must be placed on the development and use of facial recognition technologies.

Much of the controversy regarding the use of facial recognition technology stems from issues in accuracy of the technology, resulting in some arguing for a prohibition in use until the technology at least has less potential for bias.[7] However, rather than focusing regulation of the development of facial recognition technology, such as the creation of standardized benchmarks,[8] more meaningful regulation can perhaps focus on regulating and limiting uses of the technology to specific circumstances. Tightly regulating the specific uses of technology would mitigate many of these issues while still allowing for continued development of the technology and protection of human rights. This shift in focus will also allow for creation of regulation that will withstand future development of facial recognition.

---

https://www.technologyreview.com/f/615098/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance/ [https://perma.cc/B4FT-CHBJ].

[6] Robin Gomes, *Pope: Church's Social Teaching Can Help AI Serve the Common Good*, VATICAN NEWS (Feb. 28, 2020), https://www.vaticannews.va/en/pope/news/2020-02/pope-francis-artificial-intelligence-algor-ethics.html [https://perma.cc/6ZXS-UF3T].

[7] Daniel Castro, *Are Governments Right to Ban Facial Recognition Technology?*, GOV'T TECH. (Apr./May 2019), https://www.govtech.com/products/Are-Governments-Right-to-Ban-Facial-Recognition-Technology.html [https://perma.cc/V2QC-CL3K].

[8] *See* Katyanna Quach, *We Listened To More Than 3 Hours Of US Congress Testimony On Facial Recognition So You Didn't Have To Go Through It*, REGISTER (May 22, 2019), https://www.theregister.co.uk/2019/05/22/congress_facial_recognition/ [https://perma.cc/849U-B2FR] (explaining "benchmarks"); *see also* James Vincent, *The Tech Industry Doesn't Have A Plan For Dealing With Bias In Facial Recognition*, VERGE (July 26, 2018), https://www.theverge.com/2018/7/26/17616290/facial-recognition-ai-bias-benchmark-test [https://perma.cc/6243-VJFY].

Neither federal or state government bodies in the United States can successfully bear the entire burden of regulating facial recognition technology in an effective manner. While it is impossible to anticipate and address all current and future risks that may accompany the development of artificial intelligence (AI), it is important that the United States government and companies developing the technology working together to create a flexible "balanced and values-based regulatory framework"[9] that not only supports the growth of technology, but also protects human interests and individuals from discriminatory use or harm. Within this framework, it is imperative that the government identify, assess, categorize, and regulate higher risk uses of facial recognition, such as use by law enforcement, and provide guidance and opportunities for corporate self-regulation for lower risk uses of facial recognition. At the same time, companies should comply with such guidance and commit to developing facial recognition technologies ethically while remaining cognizant of potential negative impacts. In order to encourage ethical development of the technology, companies should adopt AI principles, similar to how public companies are required to adopt codes of business conduct, anti-corruption policies, or codes of ethics.[10]

This recent development will proceed in six parts. Part II will provide relevant background information about AI and facial recognition, review how facial recognition algorithms are trained, and explore datasets and how they are gathered. Furthermore, Part II will examine discrepancies in algorithmic performance across

---

[9] *Structure for the White Paper on Artificial Intelligence - A European Approach*, at 8–9, COM (Dec. 12, 2019) [hereinafter "EU White Paper"]; *see generally White Paper on Artificial Intelligence a European Approach to Excellence and Trust*, COM (Feb. 2020).

[10] *See* Lynn S. Paine et al., *Up to Code: Does Your Company's Conduct Meet World-Class Standards?*, HARV. BUS. REV. (Dec. 2005), https://hbr.org/2005/12/up-to-code-does-your-companys-conduct-meet-world-class-standards [https://perma.cc/Y6MN-458E] (describing that under the Sarbanes-Oxley Act, companies listed on the New York Stock Exchange and the Nasdaq adopted a code of conduct); *see also* Robert G. Hensley, *Can Business Conduct Be Legislated by a Code of Ethics?*, DORSEY & WHITNEY LLP (Apr. 2004), https://www.dorsey.com/newsresources/publications/2004/05/can-business-conduct-be-legislated-by-a-code-of-__ [https://perma.cc/64YT-H3HG].

different ethnicities. By examining the results of several studies, the disparity in the performance across different ethnicities will highlight the existence and danger of algorithmic bias. Part III will provide a brief overview of legal issues that arise in the use, development, and application of facial recognition technology, including privacy, human rights, and constitutional rights. Part IV will assess approaches taken by foreign and domestic governments, ultimately suggesting potential adoption of several of these measures in light of this review, as well as suggest additional approaches to regulation. Part V will propose a framework to guide government regulation and commitment by companies to responsibly develop facial recognition technologies. Finally, Part VI will look at uses of facial recognition technology by law enforcement and in the workplace, and analyze these "use" cases under the proposed framework.

## II. BACKGROUND INFORMATION REGARDING FACIAL RECOGNITION TECHNOLOGY, DATASETS, AND ALGORITHMIC BIAS

### *A. Basics of Facial Recognition Technology*

Before discussing the legal issues associated with the application and development of facial recognition technology, it is important to first understand a few basic concepts regarding facial recognition, including how the technology is trained and some issues that inherently exist as a result of this training. Facial recognition technology refers to software or an application that is trained with the specific task of identifying or verifying a person through an automated or semiautomated process which compares and analyzes unique facial vectors and contours.[11] Facial recognition software or applications are trained to identify and verify human faces via machine learning through exposure to large quantities of data that the algorithm analyzes which trains the program to learn how to

[11] *Facial Recognition*, TECHOPEDIA, https://www.techopedia.com/definition/32071/facial-recognition [https://perma.cc/Z4U9-YUZD] (last updated Feb. 25, 2019).

process certain types of information.[12] Training data used for facial recognition technologies consists of images or videos of human faces that are used to train an algorithm to either recognize a human face or identify a specific person.[13] Through repetitive exposure to thousands, if not millions,[14] of images, a computer algorithm can learn to make certain associations and connections within the data it is analyzing and eventually learn how to perform the specific task of recognizing and identifying a human face.[15] Finally, the collection of all the data and information used to train an algorithm is referred to as a dataset,[16] which, in the case of facial recognition technology, consists of photos, videos, and other images of human faces.

### *B. Algorithmic Bias*

While it is easy to assume that computers produce impartial or purely mathematical results, in the case of facial recognition technology, this assumption relies on a critical flaw. Datasets used to train facial recognition algorithms are curated by individuals who

---

[12] *Training Data*, TECHOPEDIA DICTIONARY, https://www.techopedia.com/definition/33181/training-data [https://perma.cc/PR8H-6DK5] (last visited Sept. 27, 2019).

[13] Divyansh Dwivedi, *Face Recognition for Beginners*, TOWARDS DATA SCI. (Apr. 28, 2018), https://towardsdatascience.com/face-recognition-for-beginners-a7a9bd5eb5c2 [https://perma.cc/MC76-8JXW]; *see generally Face Recognition Training Data: Helping to Train a Software*, CLICKWORKER, https://www.clickworker.com/case-studies/training-data-for-a-face-recognition-software/ [https://perma.cc/83DH-NU3V] (last visited Mar. 28, 2020).

[14] Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 [https://perma.cc/8YUM-7KZX] (explaining that Microsoft deleted one of the largest facial recognition databases available at that time named MS Celeb which contained 10 million photos).

[15] Oleksii Kharkovyna, *An Intro to Deep Learning for Face Recognition*, TOWARDS DATA SCI. (June 26, 2019), https://towardsdatascience.com/an-intro-to-deep-learning-for-face-recognition-aa8dfbbc51fb [https://perma.cc/68KH-BRPJ]; *see generally* Damilola Omoyiwola, *Machine Learning on Facial Recognition*, MEDIUM (Oct. 26, 2018), https://medium.com/datadriveninvestor/machine-learning-on-facial-recognition-b3dfba5625a7 [https://perma.cc/4LD4-AXNV].

[16] *Data Set*, TECHOPEDIA, https://www.techopedia.com/definition/3348/data-set-ibm-mainframe [https://perma.cc/V4D5-DPQF] (last visited Sept. 27, 2019).

have their own biases, whether these biases are implicit or explicit.[17] Because computer algorithms produce results that are only as good as the information used to train them, it is inevitable that when the datasets themselves contain hidden human biases, algorithms trained using these datasets may make associations and correlations between factors that either may compound on these human biases or even make unintended connections and correlations.[18] Thus, algorithms can develop associations that in some cases exacerbate preexisting human biases and may result in a deepening algorithmic bias.[19]

A study conducted in 2018 revealed that then existing facial recognition algorithms were prone to error in identification of people of color due to the non-diverse datasets used to train the algorithms.[20] According to the study, the facial recognition products

---

[17] *See generally Understanding Implicit Bias*, OHIO ST. UNIV. KIRWAN INST. FOR THE STUDY OF RACE AND ETHNICITY (2015), http://kirwaninstitute.osu.edu/research/understanding-implicit-bias/ [https://perma.cc/7YT3-V6JH] (describing that implicit biases are "attitudes or stereotypes that affect our understanding, actions, and decisions in an unconscious manner," and that these biases "are activated involuntarily and without an individual's awareness or intentional control."); *see also Project Implicit*, HARV. (2011), https://implicit.harvard.edu/implicit/takeatest.html [https://perma.cc/C4C2-Z4KP] (providing an online test allowing users to test their own implicit biases).

[18] Rachel Meade, *Bias in Machine Learning: How Facial Recognition Models Show Signs of Racism, Sexism and Ageism*, TOWARDS DATA SCI. (Dec. 13, 2019), https://towardsdatascience.com/bias-in-machine-learning-how-facial-recognition-models-show-signs-of-racism-sexism-and-ageism-32549e2c972d?gi=1af1673fc59c [https://perma.cc/HGD7-QPTT] (describing that facial recognition models show unintended occurrences of bias).

[19] *See* Nicol Turner Lee et al., *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS INSTITUTION (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ [https://perma.cc/ZTD6-YM55]; *see also* Stanford University, *New Algorithms Train AI to Avoid Specific Bad Behaviors*, EUREKALERT! (Nov. 21, 2019), https://www.eurekalert.org/pub_releases/2019-11/su-sct111819.php [https://perma.cc/AWF9-UJZN] (describing a study outlining a new technique in training algorithms to avoid "undesirable outcomes such as racial and gender bias.").

[20] *See generally* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACHINE LEARNING RES. 1 (2018) (examining facial recognition

of three leading technology companies had less than 1 percent error margins for white males, but dramatically increased, in the instance of one technology, to more than a 34 percent error margin in the identification of darker-skinned women.[21] The datasets used to train these facial recognition products were found to contain images that were 77 percent male and more than 80 percent white in some cases.[22] It is worth noting that following the illuminating results of the MIT study, several companies, including IBM,[23] made efforts to address and mitigate existing biases found in their algorithms by creating diverse datasets to train their algorithms.[24] Nevertheless, despite such attempts to address the inaccuracy in identifying ethnic faces, a subsequent study by the National Institute of Standards and Technology, which tested 189 algorithms from 99 different developers around the world, found that facial recognition products still were likely to falsely identify Asian and African-American faces between 10 to 100 times more often than Caucasian faces.[25]

While there is significant concern surrounding application of facial recognition with large error margins, the potential for bias or discrimination will not be eliminated even if facial recognition technology reaches 100 percent accuracy. In fact, having error free facial recognition technology would merely elicit different and potentially even more dangerous instances of bias or discrimination.[26] Modern uses of facial recognition have revived and

---

technology created by several leading technology companies to discover algorithmic bias in misidentification of darker-skinned and females).

[21] *Id*. at 11.

[22] *Id.* at 3.

[23] John R. Smith, *IBM Research Releases 'Diversity in Faces' Dataset to Advance Study of Fairness in Facial Recognition Systems*, IBM RES. BLOG (Jan. 29, 2019), https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/ [https://perma.cc/95ZS-ACKM].

[24] *Id.*

[25] *Facial Recognition Fails on Race, Government Study Says*, BBC (Dec. 20, 2019), https://www.bbc.com/news/technology-50865437 [https://perma.cc/BE34-KE9D]; *see also NIST Report On Facial Recognition: A Game Changer*, THE INT'L BIOMETRICS + IDENTIFICATION ASS'N 1, 4 (Feb. 14, 2020).

[26] Michelle Yan, *Facial Recognition Is Almost Perfectly Accurate — Here's Why That Could Be a Problem*, BUS. INSIDER (Apr. 17, 2019), https://www.businessinsider.com/facial-recognition-technology-regulation-

popularized the once debunked pseudoscience of physiognomy,[27] as evidenced by attempts to use facial recognition technology to discern everything from a person's character, mental health, political affiliations,[28] sexual orientation, and even whether a person may have any criminal tendencies[29] merely from the examination of facial features. Researchers note that the potential for bias or discrimination is particularly concerning given that a few studies have managed to produce successful results.[30] These few select results may lead to the validation and creation of discriminatory practices of using facial recognition technology to discern personal and private information like character traits or personality from facial features.

---

creepy-future-2019-4 [https://perma.cc/J4WA-KLSZ] (describing why perfectly accurate facial recognition is problematic).

[27] Oliver Bendel, *The Uncanny Return of Physiognomy*, ASS'N FOR THE ADVANCEMENT OF ARTIFICIAL INTELLIGENCE 10, 13–17 (2018); *see also* Matt Simon, *Fantastically Wrong: The Silly Theory That Almost Kept Darwin From Going on His Famous Voyage*, WIRED (Jan. 21, 2015), https://www.wired.com/2015/01/fantastically-wrong-physiognomy/ [https://perma.cc/C3XH-PPZ4] (providing historical background on the rise and fall of physiognomy and the belief that facial features could indicate personality and character traits); *see also Physiognomy*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/physiognomy [https://perma.cc/A7PE-HAHG] (last visited Mar. 15, 2020) (defining physiognomy as "the art of discovering temperament and character from outward appearance" or "facial features held to show qualities of mind or character by their configuration or expression").

[28] Alexander Todorov, *Can We Read a Person's Character from Facial Images?*, SCI. AM. (May 14, 2018), https://blogs.scientificamerican.com/observations/can-we-read-a-persons-character-from-facial-images/ [https://perma.cc/3MHT-DMYH] (describing that there has been a recent rise in studies claiming that facial images can be used to discern everything from mental health, politics, and sexual orientation).

[29] Xiaolin Wu & Xi Zhang, *Automated Inference on Criminality Using Face Images*, ARXIV (2016), https://arxiv.org/pdf/1611.04135.pdf [https://perma.cc/A23Q-V3LV].

[30] Bendel, *supra* note 27.

## III. INTRODUCTION TO PRIVACY, HUMAN RIGHTS, AND CONSTITUTIONAL RIGHTS

Legal issues with respect to facial recognition technology can largely be categorized under the umbrellas of privacy law, human rights issues, and constitutional law. At the developmental stage of creating facial recognition software, there are a multitude of privacy concerns regarding how personal facial data is collected, used, and stored. Subsequent to this developmental stage, the use and application of the technology also raises several additional concerns regarding discrimination and bias, which in turn implicate concerns over potential violations of both human rights and constitutional rights.

### *A. Privacy Issues in the Collection, Use, and Storage of Highly Sensitive Facial Data*

Chinese citizens currently live in a world in which their every action can be monitored via facial recognition technology. This technology is capable of identifying a person in the government's database in mere seconds.[31] Despite a sizable population of over 1.4 billion people, nearly every single Chinese citizen is included in the government's facial recognition database.[32] Chinese citizens truly have no escape from the reaches of this technology as their government monitors even micro actions including publicly shaming jaywalkers,[33] limiting the dispensing of toilet paper in public bathrooms to 23.6 inches,[34] monitoring sorting of trash,[35] and racially profiling, monitoring, and tracking ethnic minorities[36]

---

[31] Amanda Lentino, *This Chinese Facial Recognition Start-Up Can Identify A Person in Seconds*, CNBC (May 16, 2019), https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html [https://perma.cc/CCX9-LKWR].

[32] *Id.*

[33] Chun, *supra* note 4.

[34] *Id.*

[35] Karen Chiu, *Why is China Using Facial Recognition On Garbage Bins?*, ABACUS NEWS (Aug. 2, 2019), https://www.abacusnews.com/digital-life/why-china-using-facial-recognition-garbage-bins/article/3021110 [https://perma.cc/J6HY-8DUT].

[36] Zak Doffman, *China Is Using Facial Recognition to Track Ethnic Minorities, Even In Beijing*, FORBES (May 3, 2019), https://www.forbes.com/sites/

without concern of privacy. A company in China has even used other types of biometric data to monitor Chinese citizens, including tracking the brainwaves and activity levels of employees to increase productivity and efficiency in employee work.[37] Despite these significant differences in the current state and use of the facial recognition technologies between China and the rest of the world, the surveillance state in China should serve as a persuasive warning to other countries and governments that regulation and action are needed with respect to development and use of facial recognition technology. While the use of facial recognition technology admittedly may have beneficial uses, such as identifying a mass shooting suspect,[38] there is an undeniable concern that uncontrolled use may lead to an overly surveilled state as that which exists in China.[39]

The use of facial recognition raises privacy concerns at several stages of both development and application. Many companies have collected and used facial data to train the algorithms without seeking any consent from individuals or even notifying them.[40] What is further problematic is that even if people had knowledge that their

---

zakdoffman/2019/05/03/china-new-data-breach-exposes-facial-recognition-and-ethnicity-tracking-in-beijing/#1b6fe1aa34a7 [https://perma.cc/3DKG-NKG5].

[37] Tara Francis Chan, *China Is Monitoring Employees' Brain Waves and Emotions – And The Technology Boosted One Company's Profits By $315 Million*, BUS. INSIDER (May 1, 2018), https://www.businessinsider.com/china-emotional-surveillance-technology-2018-4 [https://perma.cc/WRZ2-Z82E] (describing how a Chinese company monitored their employees' brainwaves to track productivity, when breaks were needed, and when employees should be sent home, in an effort to track profitability and efficiency).

[38] Ian Bogost, *The Way Police Identified the Capital Gazette Shooter Was Totally Normal*, ATLANTIC (June 29, 2018), https://www.theatlantic.com/technology/archive/2018/06/capital-gazette-shooting-face-recognition/564185/ [https://perma.cc/W5FS-MPXC].

[39] Sam Shead, *Chinese Residents Worry About Rise of Facial Recognition*, BBC (Dec. 2, 2019), https://www.bbc.com/news/technology-50674909 [https://perma.cc/ZTS4-2KDX] (explaining that over 74 percent of Chinese citizens would like to use alternative technology rather than invasive facial recognition technology).

[40] Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, CNBC NEWS (Mar. 12, 2019), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [https://perma.cc/9PK4-BC4E].

facial data was used, in many cases, these individuals have no ability to opt out or stop the use of their data.[41] At the same time, there is an increasing demand for curation of more facial datasets in an effort to increase accuracy of facial recognition algorithms. This has resulted in an already thriving business of selling facial data that is procured without consent.[42] Demonstrably, the privacy and protection of facial data is an imminent cause for concern.[43]

Storage of sensitive facial data also gives rise to concerns over whether such data is adequately protected and secured. When sensitive facial data is stored without adequate security, the data can be very appealing to hackers.[44] This lax in security already resulted in data breaches which compromised individual facial data.[45] The United States Customs and Border Protection was a victim of a cyberattack in which photos were compromised.[46] Unlike other forms of data, stolen facial data poses the difficult challenge of having little to no recourse available. While people may change and create new numbers for identification[47] people cannot change their faces as easily.[48]

---

[41] *Id.*

[42] Jeff John Roberts, *The Business of Your Face*, FORTUNE (Mar. 27, 2019), https://fortune.com/longform/facial-recognition/.

[43] Solon, *supra* note 40.

[44] Alyssa Newcomb, *Border Patrol Hack Shows How New Technology Makes Law Enforcement a Target*, FORTUNE (June 11, 2019), https://fortune.com/2019/06/11/customs-border-patrol-hack/.

[45] Drew Harwell & Geoffrey A. Fowler, *U.S. Customs and Border Protection Says Photos of Travelers Were Taken In A Data Breach*, WASH. POST (June 10, 2019), https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/.

[46] *Id.*

[47] *Id.*

[48] Jonathan Stempel, *Facebook Loses Facial Recognition Appeal, Must Face Privacy Class Action*, REUTERS (Aug. 8, 2019), https://www.reuters.com/article/us-facebook-privacy-lawsuit/facebook-loses-facial-recognition-appeal-must-face-privacy-class-action-idUSKCN1UY2BZ [https://perma.cc/7XMB-VSYL] (explaining that facial data is particularly sensitive as it cannot be easily changed.); *see also* David Goldman, *Your Face Is Secretly Being Used Against You*, CNN (June 16, 2015), https://money.cnn.com/2015/06/16/technology/facial-recognition/index.html [https://perma.cc/KF75-QDBQ] (elaborating that

*B. Human Rights*

As discussed, facial recognition algorithms form correlations through mining facial data which can produce unintended correlations that may be biased or discriminatory.[49] This becomes particularly problematic when the interpretation of data is left solely to computers without any human review or understating of what correlations exist. In the absence of human review, "an assessment of human rights impacts" should be considered to reveal "bias [that] may be hidden in the data"[50] that may not be readily apparent but may manifest in application of the technology. To eliminate some existing biases, "disproportionate impacts on vulnerable communities" must be eliminated before there can be any acceptable "widespread adoption of facial recognition technology by government agencies."[51]

Companies have quietly developed and used facial recognition technologies commonly in hiring practices in the United States without any general public knowledge.[52] More than 100 employers in the United States have use facial recognition technology to review video interviews that consider candidates' "facial movements, word choice and speaking voice" and assign scores to candidates to rank their employability.[53] Many hopeful interviewees may participate in recorded video interviews without any awareness that their recording is reviewed by a computer rather than a person. The

---

people cannot easily change face, yet do not have meaningful opt-out processes out for companies using their facial data).

[49] *See generally* Buolamwini, *supra* note 20; *see also* COMMITTEE OF EXPERTS ON INTERNET INTERMEDIARIES, *Algorithms and Human Rights: Study on The Human Rights Dimension of Automated Data Processing Techniques and Possible Regulatory Implication* 6 (Mar. 2018).

[50] *Id.*

[51] *See, e.g.,* S.B. 5528, 66th Leg., Reg. Sess. (Wash. 2019) ("An Act Relating to the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology; and adding a new chapter to Title 10 RCW.").

[52] 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/8L5C-638B].

[53] *Id.*

videos are analyzed by AI that assigns scores to future, prospective employees in factors such as "personal stability" and "conscientiousness and responsibility."[54] While the scores assigned to interviewees may, in part, try to glean information about personality from facial expressions displayed in the recording, the review process fundamentally echoes "biological essentialism behind physiognomy."[55] By using facial features, structures, and measurements to determine unrelated factors such as employability or intelligence, the use of facial recognition in hiring opens the door for potentially highly bias and discriminatory recruiting practices.

The potential for workplace discrimination extends beyond facial recognition technology and is perpetuated through many other forms of AI. Amazon scrapped an ill-fated algorithm which reviewed job candidate resumes and was trained using data from their top performing employees.[56] The tool was removed from use because it formed an association between "male" or "man" and a successful candidate, and thereby penalized resumes including "women" or resumes that listed an education at an all-women's college.[57] While this resume reviewing tool was quickly scrapped once this bias was discovered,[58] not all technology is subject to review for bias. This demonstrates the need to remain cognizant of

---

[54] Sahil Chinoy, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019), https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html [https://perma.cc/WT45-YFAA].

[55] *Id.*

[56] *See* Isobel Asher Hamilton, *Why It's Totally Unsurprising That Amazon's Recruitment AI Was Biased against Women*, BUS. INSIDER (Oct. 13, 2018), https://www.businessinsider.com/amazon-ai-biased-against-women-no-surprise-sandra-wachter-2018-10 [https://perma.cc/EZ6B-EL82]; James Vincent, *Amazon Reportedly Scraps Internal AI Recruiting Tool That Was Biased Against Women*, VERGE (Oct. 10, 2018), https://www.theverge.com/2018/10/10/17958784/ai-recruiting-tool-bias-amazon-report [https://perma.cc/QP4F-UTG6]; Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 9, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/ES8A-G7DB].

[57] *See* Hamilton, *supra* note 56; Vincent, *supra* note 56.

[58] *Id.*

the potential for bias when developing facial recognition which is prone to comparable machine learning errors.

### *C. Implication of Constitutionally Protected Rights*

The use of facial recognition by law enforcement and government agencies implicate rights protected by the Fourth Amendment of the Constitution. While people may not have a general right to privacy in public spaces,[59] the way in which facial recognition technology is used raises heightened concerns over privacy[60] as our anonymity in public is entirely stripped.[61] Facial recognition technology not only can identify people in real-time, but it also can track retroactive movements of individuals[62] by mining through close-circuit television surveillance videos or other data to even track a specific person's movements "across time, location, and the environment."[63]

The Fourth Amendment of the Constitution prohibits unreasonable searches and seizures in areas that a person may reasonably expect to have privacy.[64] In *Katz v. United States*,[65] the United States Supreme Court developed a test to determine whether any individual has a reasonable expectation of privacy by assessing

---

[59] *What Is the "Reasonable Expectation of Privacy"?*, FINDLAW THOMSON REUTERS, https://injury.findlaw.com/torts-and-personal-injuries/what-is-the--reasonable-expectation-of-privacy--.html [https://perma.cc/9F48-XSFX] (last visited Apr. 5, 2020); *see also* David Kravets, *Feds: Privacy Does Not Exist in 'Public Places'*, WIRED (Sept. 21, 2010), https://www.wired.com/2010/09/public-privacy/ [https://perma.cc/T72Y-6XCE].

[60] *Data Privacy Week: Privacy in Public Spaces,* PRIVACY INT'L (Jan. 30, 2019), https://privacyinternational.org/long-read/2676/data-privacy-week-privacy-public-spaces [https://perma.cc/SH78-V9WQ].

[61] Jake Laperruque, *Preserving the Right to Obscurity in the Age of Facial Recognition*, CENTURY FOUND. (Oct. 20, 2017), https://production-tcf.imgix.net/app/uploads/2017/10/03111141/preserving-the-right-to-obscurity-in-the-age-of-facial-recognition.pdf [https://perma.cc/K7W3-ZHBC].

[62] Rebecca Heilweil, *New Surveillance AI Can Tell Schools Where Students Are and Where They've Been*, VOX (Jan. 25, 2020), https://www.vox.com/recode/2020/1/25/21080749/surveillance-school-artificial-intelligence-facial-recognition [https://perma.cc/298R-LGFS].

[63] *Id.*

[64] U.S. CONST. amend. IV.

[65] Katz v. United States, 389 U.S. 347, 361 (1967).

"(1) whether the person exhibited an actual, subjective expectation of privacy and (2) whether that expectation is one that society recognizes as reasonable."[66] In *Carpenter v. United States*,[67] the United States Supreme Court held that government use of historical data from cell phone companies without any warrant violated these Fourth Amendment rights.[68] The Court determined that police or government use of such technology "must be put to a higher standard and must obtain a judicial search warrant based on sworn facts that probable cause exists."[69] While facial recognition technology differs from cell phone data in many respects, *Carpenter* established the important idea that when newer available technologies allow the government to encroach on a person's expectation of privacy, an individual's privacy needs to be protected from intrusion by the government regardless of what tool is being used, especially if it occurs over a longer period of time.[70] The American Bar Association suggests that in light of *Katz* and *Carpenter*, use of facial recognition technology does not trigger Fourth Amendment rights for a "limited, short-term basis with strictly public systems" but may become problematic when used to track someone over an extended period of time.[71] This is due to the fact that this level of surveillance results in a higher invasion of a person's right to privacy regardless of whether the search occurred in a public space.[72]

## IV. CURRENT LEGAL LANDSCAPE IN THE EUROPEAN UNION AND THE UNITED STATES

Privacy laws with respect to facial recognition differ vastly between the European Union and the United States. The General

---

[66] *Id.*; Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us*?, AM. BAR ASS'N, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ [https://perma.cc/9VBK-W7WY] [hereinafter "ABA on Facial Recognition"] (last visited Apr. 6, 2020).

[67] Carpenter v. United States, 138 S. Ct. 2206, 2214–17 (2018).

[68] *Carpenter,* 138 S. Ct. at 2221; ABA on Facial Recognition, *supra* note 66.

[69] ABA on Facial Recognition, *supra* note 66.

[70] *Carpenter,* 138 S. Ct. at 2233; ABA on Facial Recognition, *supra* note 66.

[71] ABA on Facial Recognition, *supra* note 66.

[72] *Id.*

Data Protection Regulation (GDPR) unifies regulation of data protection and privacy throughout the entire European Union. By comparison, the legal landscape in the United States has no uniform federal regulation for data protection or privacy. In fact, while many states are considering creating regulations to for data protection or privacy only a few states have any existing or proposed regulation, including the California Consumer Privacy Act (CCPA), the Illinois Biometric Information Privacy Act (BIPA), and the Washington State Privacy Bill. It is important to note that the overview of each of the existing legal landscapes is limited to the very narrow scope only as related to facial recognition and that which could be potentially adopted into the proposed framework.

### *A. The European Union's General Data Protection Regulation*

Privacy concerns over the use of sensitive biometric data, such as facial data, is a central issue addressed in the GDPR.[73] The right to privacy is considered a fundamental right under the GDPR that affords European citizens autonomy, control over private individual information, and the right to be left alone.[74] Therefore, facial data which falls into the category of biometric data is considered sensitive data under the GDPR.[75] There are several regulations regarding how data must be treated under the GDPR, unless there is explicit consent.[76] The GDPR requires the minimization of data use as limited to the specific purpose, limits storage of data,[77] and mandates privacy impact assessments.[78] In fact, a Swedish school board was even fined for failure to comply with requirements under

---

[73] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 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) 1 [hereinafter "GDPR"].

[74] *Data Protection*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection_en [https://perma.cc/3EYX-N98S].

[75] GDPR, *supra* note 73, at Recital 51.

[76] *Id.* at art. 7, 9.

[77] *Id.* at art. 5.

[78] *Id.* at art. 35.

the GDPR when using sensitive facial data.[79] This enforceability stands in stark contrast to privacy laws in the United States, which remain far behind the European Union in protecting its citizens' data and privacy.[80] Despite the fact that the European Union already has significantly more robust regulation than that of the United States, they plan to even further tighten regulations in the GDPR to protect the privacy rights of European citizens when facial recognition is used.[81] The European Union, at one point, had briefly considered a five year ban on all facial recognition until privacy concerns are addressed.[82] While an outright ban may not be a good solution, the United States should consider adopting many aspects of the GDPR.

### *B. The Legal Landscape in the United States*

Unlike its European counterpart, the United States lacks regulation at the federal level and has only a few states laws regulating the use of facial recognition technology.[83] What is curious is that this difference in existing regulation of facial recognition technology has an inverse relationship with each country's appetite for development of the facial recognition systems. In 2016, the European Union invested €3.2 billion and Asia invested €6.5 billion

---

[79] *See generally* Sofia Edvardsen, *How to Interpret Sweden's First GDPR Fine on Facial Recognition in School*, INT'L ASS'N OF PRIVACY PROFS. (Aug. 27, 2019), https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/ [https://perma.cc/K3LX-H68G].

[80] The Editorial Board, *Why Is America So Far Behind Europe on Digital Privacy?*, N.Y. TIMES: THE PRIVACY PROJECT (June 9, 2019), https://www.nytimes.com/2019/06/08/opinion/sunday/privacy-congress-facebook-google.html [https://perma.cc/7CY3-BHRV].

[81] Mehreen Khan, *EU Plans Sweeping Regulation of Facial Recognition*, FIN. TIMES (Aug. 22, 2019), https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9.

[82] Foo Yun Chee, *EU Mulls Five-Year Ban On Facial Recognition Tech In Public Areas*, REUTERS (Jan. 16, 2020), https://www.reuters.com/article/us-eu-ai/eu-mulls-five-year-ban-on-facial-recognition-tech-in-public-areas-idUSKBN1ZF2QL [https://perma.cc/FND8-HAHV]; *see Facial Recognition: EU Considers Ban of Up To Five Years*, BBC (Jan. 17, 2020), https://www.bbc.com/news/technology-51148501 [https://perma.cc/52SR-5MQK].

[83] The Editorial Board, *supra* note 80 (describing that the US is far behind the EU in protecting the privacy of its citizens and that European laws, in fact, do a better job at protecting American privacy than American laws).

into developing AI while, in comparison, the United States invested a staggering €12.1 billion.[84] Yet, the United States is far behind in creating or enacting sufficient regulation or laws to guide the ethical development of facial recognition.

*1. The California Consumer Privacy Act in Relation to Facial Recognition*

The California Consumer Privacy Act (CCPA)[85] incorporates facial recognition data within the definition of biometric data and personal data.[86] The CCPA parallels many requirements set forth in the GDPR. The CCPA requires companies that have an annual gross revenue of over $25 million or receive personal data of more than 50,000 consumers in a year to, among many other things, inform consumers that the company is collecting personal data, provide consumers access to their data if requested by the customer, and allow them to delete such data if desired.[87] Companies that do not comply with the requirements set forth by the CCPA will face fines for non-compliance.

*2. The Washington State Privacy Laws in Relation to Facial Recognition*

Over several years, the state of Washington had proposed many iterations of laws to regulate the use of facial recognition which failed[88] before finally adopting its current laws. These new laws introduce substantial restrictions for the use of facial recognition by law enforcement, require warrants for use in an investigation if there is no emergency, and require a human review of results of facial recognition analysis that may have "legal effects" such as an effect

---

[84] EU White Paper, *supra* note 9, at 4.

[85] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (2018) (effective Jan. 1, 2020).

[86] *How the New California Privacy Law (CCPA) Handles Facial Recognition*, CLARITY IN PRIVACY!, https://www.clarip.com/data-privacy/california-privacy-law-facial-recognition/ [https://perma.cc/9RA6-5324] (last visited Feb. 1, 2020).

[87] *Id.*

[88] Khari Johnson, *Washington Privacy Act Fails Again, But State Legislature Passes Facial Recognition Regulation*, VENTUREBEAT (Mar. 12, 2020), https://venturebeat.com/2020/03/12/washington-privacy-act-fails-in-state-legislature-again/ [https://perma.cc/ZC52-GJUK].

on jobs, "financial services, housing, insurance, and education."[89] Unlike the GDPR and CCPA, Washington directly addresses facial recognition technology[90] rather than reading facial recognition into biometric data or personal data.

*3. The Illinois Biometric Information Privacy Act in Relation to Facial Recognition*

Unlike laws in either California or Washington, there have been a number of cases that address the requirements under the Illinois Biometric Information Privacy Act (BIPA) and several companies have already faced lawsuits and fines for violation of the BIPA. In *Patel v. Facebook*,[91] the Court found that the invasion of privacy by facial recognition technology is a concrete harm. The plaintiffs in *Patel* argued that collection of their biometric data, specifically photographs, without their consent or knowledge violated the BIPA.[92] While Facebook initially vehemently denied that there was any harm, the company subsequently chose to settle a separate class-action lawsuit that alleged that the company had violated the BIPA by collecting biometric data without the consent, knowledge, or providing any notice to its users.[93] Soon after settlement of the

---

[89] Paul Shukovsky, *Warrantless Facial Recognition Ban Bill Approved in Washington*, BLOOMBERG L. (Mar. 12, 2020), https://news.bloomberglaw.com/privacy-and-data-security/warrantless-facial-recognition-ban-bill-approved-in-washington [https://perma.cc/ZFR6-72GW]; Monica Nickelsburg, *Washington State Passes Landmark Facial Recognition Bill, Reining In Government Use Of AI*, GEEKWIRE (Mar. 13, 2020), https://www.geekwire.com/2020/washington-state-passes-landmark-facial-recognition-bill-reining-government-use-ai/ [https://perma.cc/TN3Y-GUBF]; Ryan Tracy, *Washington State OKs Facial Recognition Law Seen as National Model*, WALL ST. J. (Mar. 31, 2020), https://www.wsj.com/articles/washington-state-oks-facial-recognition-law-seen-as-national-model-11585686897 [https://perma.cc/SW6B-3RA2].

[90] Scott Ikeda, *With Enhanced Facial Recognition Technology Protections, the New Washington Privacy Act Would Be the Strongest U.S. Privacy Bill*, CPO MAG. (Feb. 27, 2020), https://www.cpomagazine.com/data-protection/with-enhanced-facial-recognition-technology-protections-the-new-washington-privacy-act-would-be-the-strongest-u-s-privacy-bill/ [https://perma.cc/R43A-FQ4W].

[91] Patel v. Facebook Inc., 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018).

[92] *Id.* at 950.

[93] Natasha Singer and Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020),

Facebook lawsuit, Google was also sued for violating the BIPA's requirement that a company must obtain written consent from users to collect, store, and use their personal data.[94]

*4. Cities Ban Use of Facial Recognition by Law Enforcement & Government*

Several cities in the United States, including San Francisco,[95] Oakland, Berkeley in California, and Somerville and Brookline in Massachusetts have all banned use of facial recognition by law enforcement or government agencies.[96] However, a blanket ban on facial recognition for law enforcement use misses the mark on eliminating the core issues with government use of the technology to monitor its citizens and invade their privacy.[97] While a blanket ban may alleviate these concerns on a short-term basis, the reality is that there are a multitude of technologies that can be used to track and monitor people beyond facial recognition.[98] Currently, technology can track individuals through identification of walking gait or through cell phone signals.[99] While this technology may not

---

https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html?action=click&module=Latest&pgtype=Homepage [https://perma.cc/6B9D-6E8G].

[94] Anthony Kimery, *Google Hit with New Biometric Data Privacy Class Action Under BIPA*, BIOMETRICUPDATE.COM (Feb. 10, 2020), https://www.biometricupdate.com/202002/google-hit-with-new-biometric-data-privacy-class-action-under-bipa [https://perma.cc/YKX5-SR3T].

[95] Kate Conger, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/Q5RP-N8NQ].

[96] Sarah Ravani, *Oakland Bans Use Of Facial Recognition Technology, Citing Bias Concerns*, S.F. CHRON. (July 17, 2019), https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php [https://perma.cc/C9NW-4U4H].

[97] Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html?searchResultPosition=2 [https://perma.cc/7NS2-FV4L].

[98] *Id.*

[99] *Id.*; *see generally* Aaron Holmes, *Facial Recognition Is on the Rise, but Artificial Intelligence Is Already Being Trained to Recognize Humans in New Ways — Including Gait Detection and Heartbeat Sensors*, BUS. INSIDER (Oct. 29,

be as invasive as facial recognition, a mere ban on facial recognition would not hinder the use or adoption of newer and perhaps equally invasive technologies. Newer technologies could merely take the place of facial recognition and leave opportunity for the same privacy and surveillance concerns.[100] Therefore, it is critical to consider how to create and design laws to regulate the specific uses of facial recognition in a manner that can protect our privacy rather than a blanket banning.[101] While the existing state laws in the United States form a patchwork of different approaches, they may still be effective if coupled with the proposed framework suggested in the following section.

## V. RECOMMENDATIONS FOR CREATION OF A FRAMEWORK

Despite many inherent issues, facial recognition technology has the potential to provide considerable and significant benefits, such as public safety, that warrant continued development and use of the technology. An outright ban on facial recognition would mean that law enforcement would be unable to use facial recognition when future tragedies occur. This potential benefit nevertheless must be balanced with protection of the right to privacy and freedom from discrimination. Thus, facial recognition must be developed in a manner that "prevents abuse and addresses the risk it poses."[102]

In the past, the United States has failed in attempting to create uniform federal regulation for tech related issues such as data breaches.[103] While facial recognition technology is unique in that there is unprecedented bipartisan support for regulation of the technology,[104] it is still unlikely that the country will establish a

---

2019), https://www.businessinsider.com/ai-training-beyond-facial-recognition-gait-detection-heartbeat-sensors-2019-10 [https://perma.cc/AJF5-HTUX].

[100] Schneier, *supra* note 97.

[101] *Id.*

[102] Laperruque*, supra* note 61.

[103] Rachel German, *What Are the Chances for a Federal Breach Notification Law?*, U. TEX. AT AUSTIN CTR. FOR IDENTITY, https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law [https://perma.cc/NE5W-U4FC] (last visited Feb. 1, 2020).

[104] Shirin Ghaffary, *How Facial Recognition Became the Most Feared Technology in the US: Two Lawmakers Are Drafting a New Bipartisan Bill That Could Seriously Limit the Use of the Technology Across the US*, VOX (Aug. 9,

uniform federal regulation of facial recognition technology in the near future.[105] However, government regulation is just one part to a whole system or framework that is necessary to provide a level of regulation, guidance, and best practices necessary to address the wide range of issues that facial recognition touches. A more comprehensive framework could include a three-prong approach for regulation of facial recognition including the government, companies or developers, and finally end-users or consumers. An initial risk assessment of each use case could help distribute responsibility across the three prongs. High risk uses could be allocated to state or federal government entities while other non-high or lower risk uses could be allocated for self-regulation by companies and developers of the technology. Finally, the presence of consumers or users could act as drivers of market forces to encourage ethical use and development of facial recognition technology.

### *A. Government*

Much like the GDPR,[106] determining the risk level of the use of facial recognition would allow categorization of requirements for how facial data and privacy should be protected and who should be charged with protecting the information. High risk cases would involve uses of facial recognition by the police or government, particularly for use in public spaces. This type of high risk uses involve a high chance of violation of privacy and constitutional

---

2019), https://www.vox.com/recode/2019/8/9/20799022/facial-recognition-law [https://perma.cc/G99N-AUSG].

[105] *See* Cat Zakrzeswki, *The Technology 202: Facial Recognition Gets Another Look on Capitol Hill Today From Skeptical Lawmakers*, WASH. POST (Jan. 15, 2020), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/01/15/the-technology-202-facial-recognition-gets-another-look-on-capitol-hill-today-from-skeptical-lawmakers/5e1dfc4588e0fa2262dcd2b5/ [https://perma.cc/6VGU-JG5F] (discussing skepticism on reaching agreement despite bipartisan support following three previous attempts at reaching federal regulation of facial recognition technology); *see also* Mason Kortz, *Facial Recognition Regulation – A Year in Review*, AM. CONST. SOC. (Dec. 17, 2019), https://www.acslaw.org/expertforum/facial-recognition-regulation-a-year-in-review/ [https://perma.cc/2QGN-PZAP].

[106] *See generally* GDPR, *supra* note 73.

rights and a high potential for discrimination if left unchecked. Therefore, uses that satisfy these considerations should be regulated by the state or federal government. Unless such rights are threatened, other cases would fall under the lower risk category. This could involve facial recognition technology for cases such as internal use in private companies that has limited use and is applied with user consent. Another means of differentiating when government regulation is needed is whether use of the technology occurred in a public space. Much like the GDPR, a public use requirement[107] could dictate conditions in which government regulation is needed for when the technology is applied in public spaces.

In addition, both the state or federal government could encourage participation in self-regulation by companies via offering a system of voluntary labeling[108] that would allow companies developing facial recognition technology who comply with certain conditions to be certified as an ethical or a trustworthy developer of the technology.[109] This would not only allow minimal oversight by the government, which could source certification to third parties once the conditions have been established, but would also allow for voluntary participation by companies that want to be recognized as ethical developers. In turn, this would allow for consumers and users to selectively seek out companies with such labeling or choose to discontinue their business with companies that do not have such labeling. The considerable strength of consumers and users in controlling market forces cannot be overlooked as a means to encourage ethical development of facial recognition. To illustrate this point, a few companies were forced to quickly retract and delete their datasets due to the severe, negative public outrage and exposure when it was discovered that these companies had used private facial data to curate their datasets without any the consent or knowledge of individuals.[110]

---

[107] EU White Paper, *supra* note 9, at 8.

[108] *Id.* at 14.

[109] *Id.*

[110] Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2.

*B. Adoption of Policies for Public Companies*

On the other hand, public companies should voluntarily adopt the policies in a show of good faith commitment to corporate responsibility. It cannot be said that a company is acting in good faith while developing facial recognition technology if an actor wholeheartedly ignores the principles of respect for human autonomy, privacy, and equal protection. One such method might be to require public companies developing facial recognition technology to adopt a policy similar to requirements for Code of Business Conduct Policies. Pursuant to the Sarbanes-Oxley Act[111] and as enforced by the United States Securities and Exchange Commission, a public company must disclose whether or not it has adopted a written Code of Business Conduct Policy.[112] In many ways, Code of Business Conduct Policies are similar to the proposed facial recognition principles. The Code of Business Conduct Policy require that certain parties in a company, such as senior financial officers and senior officers, act ethically, honestly, and in compliance with relevant laws.[113]

While companies may initially be hesitant to adopt policies with principles governing the development of AI and facial recognition technology, companies likely will need to adopt such policies at some point in the future whether imposed by an outside entity or self-generated. Therefore, it is in the best interest of companies developing facial recognition technology to preemptively create policies using their unique industry knowledge that suits their own needs, rather than waiting for a government body to enforce policies with which it may be harder to comply. In this situation, being proactive and partaking in developing these principles allows for companies to hold onto more control of the circumstances for compliance and perhaps create the norms that the government might adopt and impose on other companies. This would also allow companies to position themselves as leaders or trustworthy authorities in the public eye. Microsoft has already adopted this approach and positioned itself as a thought leader and user of ethical

---

[111] Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201 (2012).
[112] 17 C.F.R. § 229.406(a) (2014).
[113] *Id.*

practices by advocating for regulation and adoption of the GDPR requirements globally despite having no legal obligation to comply outside of the European Union.[114]

Companies could either choose to develop their own principles or policies for the development of AI and facial recognition technology or they could seek guidance from many existing policy examples. The Organisation for Economic Co-operation and Development (OECD) released a set of principles regarding development of AI.[115] The OECD principles state that AI should be developed keeping in mind human-centered values, fairness, transparency, robustness, security, safety, and finally, accountability.[116] The OECD's AI principles ultimately state that "AI actors should respect the rule of law, human rights and democratic values"[117] and that AI technology should not be developed without consideration of non-discrimination or equality and should respect human autonomy and privacy.[118] The OECD's principles further urge ethical and responsive disclosure by companies regarding their intentions and for the allowance of public discourse for any of their intentions which are objectionable.[119] Finally, the OECD's principles state that the companies and developers of AI technology should be accountable for the systems

---

[114] Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT BLOGS (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ [https://perma.cc/XJJ6-DBZF]; *General Data Protection Regulation Summary*, MICROSOFT DOCS (Feb. 27, 2020), https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr [https://perma.cc/3ZKL-Z39Q]; *GDPR Simplified: A Guide for Your Small Business*, MICROSOFT DOCS (Mar. 6, 2020), https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/gdpr-compliance?view=o365-worldwide (providing suggestions for small businesses and Microsoft services to for purchase).

[115] *Recommendation of the Council on Artificial Intelligence*, ORG. FOR ECON. CO-OPERATION AND DEV. (May 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [https://perma.cc/B8MT-GXH3].

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

that they create[120] and that these systems should be "robust, secure and safe through their entire lifecycle."[121]

Another policy that companies could look to for guidance is the Safe Face Pledge drafted by the Algorithmic Justice League and the Center on Technology and Privacy at Georgetown Law, which sets forth similar principles to the OECD with a specific focus on facial analysis technology.[122] The Pledge urges commitment to the following four principles: (1) show value for human life, dignity, and rights, (2) address harmful bias, (3) facilitate transparency, and (4) embed into business practices.[123] This highlights that embedding AI principles into business practices is critical because adopting a merely adopting a standalone policy or principles is will not affect real change. While it is easy to adopt a set of principles, these principles must be integrated and adopted into existing business practices to effectively uphold such principles while developing facial recognition technology. Furthermore, it is far more efficient to integrate privacy and human rights checks into existing procedures to keep parties involved cognizant of these issues rather than creating a cumbersome separate procedure.

The very companies that develop these highly sensitive technologies recognize the need for some government regulation and involvement with respect to certain technologies.[124] Mark Zuckerberg, founder of Facebook, stated that although regulation may hurt Facebook's bottom line, "I don't think private companies should make so many decisions alone when they touch on fundamental democratic values."[125] Similarly, Jeff Bezos, CEO of Amazon, stated that there was a clear need for regulation of facial recognition.[126] While some scholars argue that self-regulation by

---

[120] *Id.*

[121] *Id.*

[122] *Safe Face Pledge*, ALGORITHMIC JUST. LEAGUE AND THE CTR. ON TECH. & PRIVACY AT GEO. LAW (Dec. 11, 2019), https://www.safefacepledge.org/ [https://perma.cc/ED55-RC2W].

[123] *Id.*

[124] Mark Zuckerberg, *Big Tech Needs More Regulation*, FIN. TIMES (Feb. 16 2020), https://www.ft.com/content/602ec7ec-4f18-11ea-95a0-43d18ec715f5.

[125] *Id.*

[126] Todd Bishop & Monica Nickelsburg, *Bezos: Facial Recognition 'A Perfect Example' of the Need for Regulation, and Amazon Is Working on It*, GEEKWIRE

companies is impossible, as demonstrated by Facebook's own failure to regulate itself,[127] the proposed framework does not purport to argue that self-regulation alone will be enough to ensure that facial recognition is developed and applied in a manner that respects privacy, human rights, and constitutional rights. However, it is critical that the protection of these rights is given consideration at the developmental stage of creating facial recognition technology. Furthermore, the call for companies to engage in ethical development of facial recognition relies on an appeal to corporate social responsibility and ethics, which urges companies to act as good corporate citizens.[128] Self-regulation is merely a part of the framework that balances regulation by the government, self-regulation by companies, and market forces of users. While the individual prongs of this framework may be inadequate to solve the issues inherent in facial recognition, the combination of all prongs will ultimately better protect peoples' interests and rights.

## VI. ANALYSIS OF CASE STUDIES UNDER THE PROPOSED FRAMEWORK

Part VI of this paper assumes a legal framework in which these proposals have been adopted and examines two uses of facial recognition technology including: (A) use of facial recognition by the police or government and (B) in the workplace. The examination

---

(Sept. 25, 2019), https://www.geekwire.com/2019/jeff-bezos-facial-recognition-perfect-example-need-regulation-amazon-working/ [https://perma.cc/NGG6-TCFL] ("Good regulation in this arena would be very welcome I think by all the players. It makes a lot of sense for there to be some standards in how this all works, and that kind of stability would be probably healthy for the whole industry. It's a perfect example of where regulation is needed.").

[127] Rick Klein & Mary Alice Parks, *The Note: Facebook's Self-Regulation Failure*, ABC NEWS (Apr. 10, 2018), https://abcnews.go.com/Politics/note-facebooks-regulation-failure/story?id=54350427 [https://perma.cc/C2C5-HXBU]; *see also* Gary Machado, *Facebook and the EU, or the failure of self-regulation*, BLOGACTIV (EU) (May 22, 2018), https://guests.blogactiv.eu/2018/05/22/facebook-and-the-eu-or-the-failure-of-self-regulation/ [https://perma.cc/FX45-SBZ5].

[128] Godfrey Adda et. al, *Business Ethics and Corporate Social Responsibility For Business Success And Growth*, 4 EUR. J. OF BUS. & INNOVATION RES. 26, 26–42 (2016).

of each use case of facial recognition within the suggested framework and uncertainty of the current legal landscape will purport to show the achievable benefits of adopting a "balanced and values-based regulatory framework"[129] that involves participation by government, corporations, developers, and users.

### *A. Use by Law Enforcement and Government*

There is general public unrest surrounding the development of facial recognition technology for law enforcement or government use for the purpose of monitoring or surveilling its citizens.[130] Over eighty-five human rights, racial justice, faith, and civil groups have sent letters to companies like Microsoft, Amazon and Google demanding that these companies commit to not selling any face recognition or surveillance technology to any government entities.[131] Much of this unrest stems from eye-opening data accumulated through testing of existing facial recognition algorithms. The American Civil Liberties Union (ACLU) scrutinized Amazon's facial recognition soon after learning about the company's intention to develop facial recognition technology for use by law enforcement.[132] The results of the ACLU's study found that

---

[129] EU White Paper, *supra* note 9, at 8.

[130] Jon Schuppe, *Facial Recognition Gives Police A Powerful New Tracking Tool. It's Also Raising Alarms.*, NBC NEWS (July 30, 2018), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936 [https://perma.cc/G494-JSJ4]; *see also* Drew Harwell, *ACLU Sues FBI, DOJ Over Facial-Recognition Technology, Criticizing 'Unprecedented' Surveillance And Secrecy*, WASH. POST (Oct. 31, 2019), https://www.washingtonpost.com/technology/2019/10/31/aclu-sues-fbi-doj-over-facial-recognition-technology-criticizing-unprecedented-surveillance-secrecy/.

[131] *Pressure Mounts on Amazon, Microsoft, and Google Against Selling Facial Recognition to Government*, AM. CIV. LIBERTIES UNION (Jan. 15, 2019), https://www.aclunc.org/news/pressure-mounts-amazon-microsoft-and-google-against-selling-facial-recognition-government [https://perma.cc/3R8E-E6RN].

[132] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, AM. CIV. LIBERTIES UNION (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/W752-GVEC].

Amazon's facial recognition software mistakenly matched the faces of twenty-eight members of Congress with police mugshots.[133]

Despite these attempts to stop adoption of facial recognition technology by the police, a company named Clearview AI (Clearview) quietly sold facial recognition technology to more than 600 law enforcement departments in the country without any sort of public scrutiny, notification, or awareness at the time of adoption.[134] Public reaction to this news was highly negative with one Senator demanding answers from Clearview,[135] Twitter demanding that Clearview stop using its users' photos in development of its facial recognition technology,[136] and the filing of a class-action suit against Clearview.[137]

Even prior to the shocking knowledge of Clearview's extensive sales of facial recognition technology, four cities in the United States[138] had already banned the use of facial recognition technology and acknowledged the potential for abuse and propagation of bias

---

[133] *Id.*

[134] Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html?action=click&module=Top%20Stories&pgtype=Homepage [https://perma.cc/MY5P-UFFW]; *see also* Craig McCarthy, *NYPD Issues Policy on Facial Recognition Software After Nearly a Decade of Use*, N.Y. POST (Mar. 12, 2020), https://nypost.com/2020/03/12/nypd-issues-policy-on-facial-recognition-software-after-nearly-a-decade-of-use/ [https://perma.cc/7F8D-2K2H].

[135] Rae Hodge, *Clearview Facial Recognition App May Pose 'Chilling' Privacy Risk*, *Senator* Says, CNET (Jan. 23, 2020), https://www.cnet.com/news/senator-demands-answers-from-clearview-ai/ [https://perma.cc/4VAP-ZG2P].

[136] *Twitter Demands AI Company Stops 'Collecting Faces'*, BBC (Jan. 23, 2020), https://www.bbc.com/news/technology-51220654 [https://perma.cc/HRV8-3XMY].

[137] Corinne Reichert, *Clearview AI Sued Over Facial Recognition Privacy Concerns*, CNET (Jan. 24, 2020), https://www.cnet.com/news/clearview-ai-faces-lawsuit-following-facial-recognition-privacy-concerns/ [https://perma.cc/MHU4-6A59].

[138] Rachel Metz, *Beyond San Francisco, More Cities Are Saying No to Facial Recognition*, CNN (July 17, 2019), https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html [https://perma.cc/MQ59-2CBL].

and discrimination when used by the police and government.[139] Nevertheless, many companies around the world continue to develop and market facial recognition technology for police. Another company, Wolfcom, contracted with over 1,500 police departments, universities, and federal organizations in the United States for police body cameras equipped with facial recognition abilities.[140]

Under the proposed framework, use of facial recognition by law enforcement undoubtedly falls under the high-risk use category. However, while law enforcement entities procure the technology from private companies, there currently is no process or requirement for review of the technology, how it is created, and implications in application. Law enforcement entities should review how these companies collect data necessary to train the algorithms and analyze what sort of potential performance and discriminatory issues exist before adopting the technology. Alternatively, since law enforcement entities may not be able to realistically perform this sort of review themselves, they should choose to only purchase from companies who have performed this type of analysis on the technology and provide the results of the analysis. Many of these companies continue to develop facial recognition for police use without any mindfulness of protecting privacy or understanding of the performance of the technology.

Clearview's use of individual facial data to train its technology demonstrates another issue with use of facial data and how the data is stored. Alarmingly, although there are no regulations around storage of such sensitive data in the United States, it is estimated that over 117 million US citizens are in police facial recognition databases via some means of data collection.[141] Following the use of

---

[139] Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/3SPT-776Y].

[140] Dave Gershgorn, *Exclusive: Live Facial Recognition Is Coming to U.S. Police Body Cameras*, ONEZERO (Mar. 5, 2020), https://onezero.medium.com/exclusive-live-facial-recognition-is-coming-to-u-s-police-body-cameras-bc9036918ae0 [https://perma.cc/6QJW-UPC8].

[141] *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH., https://www.law.georgetown.edu/privacy-

billions of photos without user consent, Clearview's databases were hacked.[142] The federal Immigration and Customs Enforcement Agency also collected photographs from the Department of Motor Vehicles Drivers' License database without any prior knowledge or consent.[143] Storage of all sensitive facial data in the United States should be subject to the same data protection obligations as under the GDPR.[144]

A ban on facial recognition does not address the inherent issues in police use of facial recognition technology. Law enforcement cannot have an unchecked power to use facial recognition, as this would demonstrably lead to violations of constitutional rights afforded to United States citizens. Use of facial recognition by law enforcement should be subject to the same limitations that exist for other tools used by the police such as GPS tracking, searches, and seizures. Other tools used by law enforcement are limited under Fourth Amendment protections and subject law enforcement to the same limitations under the Constitution such as requirements for warrants or probable cause for searches or seizures.[145] This would alleviate some public concerns of creation of a surveillance state if government entities were not allowed to use facial recognition for general public surveillance and scan without probable cause or other comparable justification.

---

technology-center/publications/the-perpetual-line-up/ [https://perma.cc/ZR25-YULH] (last visited on Feb. 1, 2020); *see also Vermont: The Perpetual Line-Up: Unregulated Police Face Recognition in America,* GEO. L. CTR. ON PRIVACY & TECH., https://www.perpetuallineup.org/jurisdiction/vermont?mc_cid=ffed3e5d6e&mc_eid=1099afe0f2. [https://perma.cc/UX6W-PJES] (last visited Feb. 1, 2020).

[142] Jordan Valinsky, *Clearview AI Has Billions of Our Photos. Its Entire Client List Was Just Stolen*, CNN (Feb. 26, 2020), https://www.cnn.com/2020/02/26/tech/clearview-ai-hack/index.html [https://perma.cc/8EWJ-H2UA].

[143] Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html [https://perma.cc/69QU-8FSM].

[144] GDPR, *supra* note 73.

[145] *See generally* United States v. Knotts, 460 U.S. 276 (1983).

The practicalities of enforcing a requirement to get a warrant for use of facial recognition technology is a difficult problem to address. Although this seemingly may be a good method to limit the use of facial recognition, it is not practical to have to require a warrant for every single use of the technology. An alternate approach instead would be to separate use by law enforcement into two different categories. The first category would include use of facial recognition technology that would not require a warrant, such as reviewing facial data at a specific location or time in connection with active police investigations. This review could tie into a sliding scale probable cause analysis that would allow use of facial recognition technology without a warrant for criminal offenses such as murder, public safety, or immediate threat to human life. The second category would require a warrant or regulation in cases of tracking a specific suspect or identifying a specific individual.[146] For example, police would need a warrant to investigate the whereabouts of a specific individual over time or different locations. Certainly, facial recognition technology cannot exist in a vacuum and stand apart from current laws in the United States.

### *B. Use in the Workplace*

The use of facial recognition technology for internal workplace purposes would qualify as a low-risk use within the framework discussed. This type of low-risk use would warrant government guidance, but not necessarily specific regulation. Either state or eventually federal government bodies could require companies using facial recognition technology to take certain actions in some instances, while only providing guidance in others. For instance, companies could be required to implement a meaningful opt-in and opt-out process in facial recognition systems to allow employees to take control and protect their own privacy and choose whether or not to participate. Otherwise, companies are in a better position to regulate their internal workplace use of facial recognition rather than federal or state government body. Therefore, the decision by these companies on when and how they choose to internally use facial recognition could be deferred to the companies themselves.

---

[146] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

Artificial intelligence has long been used in the workplace. Many companies have turned to using biometric identification systems in lieu of badges which are easier to falsify.[147] These biometric identification systems range from facial scans, iris scans, walking gaits scans, and even scanning microchips implanted into the bodies of company employees.[148] In the past, companies have fired employees that refused to utilize the system such as fingerprint scanners.[149] This is not the example that companies using facial recognition should follow if they choose to implement any systems within their own organization or develop them for other companies. Although companies have legitimate interests to protect when implementing these systems, such as safety, security, or productivity, these interests must be balanced with protection of employee's privacy and liberties.

As briefly discussed in Part III, one way that facial recognition is used by companies in the workplace is to analyze videos and select candidates to hire.[150] AI algorithms will assess recorded video interviews of job candidates or review answers to questionnaires to rate and assign an employability score as to whether a candidate is likely to be a good culture fit in a company.[151] This use of facial recognition in the hiring process may be entirely unknown to the job candidates who likely think that a person is reviewing their interview videos. This is problematic because under these

---

[147] Catherine Stupp, *The Humble Office ID Badge Is About to Be Unrecognizable*, WALL ST. J. (Jan. 6, 2020), https://www.wsj.com/articles/the-humble-office-id-badge-is-about-to-be-unrecognizable-11578333651 [https://perma.cc/5DJR-5RFY].

[148] *Id.*

[149] Peter Holland & Tse Leng Tham, *Biometric Recognition Technology In The Workplace*, PHYS ORG (June 3, 2019), https://phys.org/news/2019-06-biometric-recognition-technology-workplace.html [https://perma.cc/Q3UK-FL2K]; *see also* Christopher Knaus, *Companies 'Can Sack Workers for Refusing to Use Fingerprint Scanners'*, GUARDIAN (Nov. 27, 2018), https://www.theguardian.com/world/2018/nov/27/companies-can-sack-workers-for-refusing-to-use-fingerprint-scanners [https://perma.cc/5ZGB-ANPN].

[150] Harwell, *supra* note 52.

[151] Chris Baraniuk, *Are You A 'Cultural Fit' For Your Job? Machines Can Now Tell*, BBC (Feb. 28, 2020), https://www.bbc.com/worklife/article/20200227-are-you-a-cultural-fit-for-your-job-machines-can-now-tell [https://perma.cc/YNG2-MQWV].

circumstances, companies likely did not notify or adequately notify candidates that facial recognition reviewed their video and likely did not receive express consent from the candidates. Therefore, if a company chooses to implement use of facial recognition in their workplace, the company must provide employees and prospective employees the opportunity to provide express, affirmative consent or chose to withdraw consent.[152] If employees or prospective employees decide to withdraw their consent, companies must also provide a meaningful opt-out process.[153]

## VII. CONCLUSION

While current use of facial recognition raises several concerns, an outright ban or moratorium of the technology is not the right answer. Banning the use or stopping the development of facial recognition is, in part, a result of fearing the unknown. A human fear of new technology is well documented throughout history when the technology is not well understood.[154] There was a time when radios, televisions, and computers were feared in their infancy and viewed as potentially harmful to people and society.[155] Now, each of these once feared technologies are ubiquitous and integral to daily life. The creation of a framework that balances the protection of human interests and the furtherance of facial recognition can soothe fears that exist about the technology by creating a system that assessed risk and distributes the burden of limiting use of facial recognition across the government, corporate developers of the technology, and

---

[152] *Privacy Principles for Facial Recognition Technology*, FUTURE OF PRIVACY F. (Dec. 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf [https://perma.cc/AYR6-LDFQ].

[153] Robert Hackett, *Why I Opt Out of Facial Recognition*, FORTUNE (Dec. 4, 2019), https://fortune.com/2019/12/04/facial-recognition-opt-out/.

[154] Melissa Dickson, *Fears About Technology Are Nothing New*, WORLD ECON. F. (June 26, 2016), https://www.weforum.org/agenda/2016/06/fears-about-technology-are-nothing-new [https://perma.cc/9ZWC-48N3].

[155] Vaughan Bell, *Don't Touch That Dial! A History of Media Technology Scares, From the Printing Press to Facebook.*, SLATE (Feb. 15, 2010), https://slate.com/technology/2010/02/a-history-of-media-technology-scares-from-the-printing-press-to-facebook.html [https://perma.cc/UL95-EXV4].

end-users. Perhaps by creating this framework, facial recognition may one day be viewed in the same light and no longer feared.