

Facial Recognition Technology and Privacy: Race and Gender – How to Ensure the Right to Privacy is Protected

LINDSEY JACQUES*

TABLE OF CONTENTS

I.	INTRODUCTION	112
II.	BACKGROUND.....	114
	A. <i>How Facial Recognition Technology Works</i>	114
	B. <i>Accuracy of the Technology</i>	116
	C. <i>The Expansion of its Use</i>	116
	D. <i>Beneficial Uses of the Technology</i>	118
III.	BIAS AND PRIVACY IMPLICATIONS – RACE AND GENDER	119
	A. <i>Bias in Facial Recognition Technology</i>	119
	1. <i>Racial Bias</i>	120
	2. <i>Gender Bias</i>	121
	B. <i>Privacy Implications</i>	122
	C. <i>Exacerbation of Privacy Concerns Caused by Bias</i>	125
IV.	LEGAL BACKGROUND AND IMPLICATIONS OF FRT USE	127
	A. <i>Constitutional Privacy Law in Each of the Five Nations</i>	128
	1. <i>China</i>	128
	2. <i>France</i>	128
	3. <i>Russian Federation</i>	128
	4. <i>United Kingdom</i>	129
	5. <i>United States</i>	129
	B. <i>United Nations International Covenant on Civil and Political Rights</i>	130
	C. <i>European Convention on Human Rights</i>	132

* © 2021 Lindsey Jacques. J.D. Candidate 2022, University of San Diego School of Law. The author would like to thank Professor Laurence Claus, Raquel Zilberman Rotman, Chandler Martin, and Joel Kaufmann for their input, guidance, and support.

	D. European Union General Data Protection Regulation.....	132
	E. UN Guiding Principles on Business and Human Rights	132
V.	FRT USE AND IMPLICATIONS IN EACH OF THE FIVE NATIONS	133
	A. FRT Use in Each of the Five Nations.....	133
	1. China	133
	2. France.....	136
	3. Russian Federation	137
	4. United Kingdom.....	138
	5. United States.....	139
	B. Implications of FRT Use as National Security Leaders	141
	C. Constitutional Provisions.....	142
	D. ICCPR and Privacy Implications of FRT.....	143
	E. European Convention on Human Rights.....	144
	F. European Union GDPR	144
	G. Company Self-Regulation Efforts and Third-Party Standards	145
VI.	PROPOSED AND POSSIBLE SOLUTIONS	146
	A. National FRT Regulation.....	147
	1. Moratorium, Not a Ban.....	148
	2. Regulatory Requirements.....	149
	B. International FRT Regulation.....	151
	C. The Role of Companies	153
VII.	CONCLUSION	154

I. INTRODUCTION

Technology has evolved to a point where science-fiction and dystopian movies are no longer far stretches of the imagination. A phone or apartment building can now be unlocked with just a scan of the face.¹ Police can use technology to monitor facial expressions within a crowd and determine whether someone seems likely to commit a crime.² Governments can track a person's movements using only images of the person's eyes.³ Although

1. Simon Denyer, *Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), <https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/> [https://perma.cc/T2UB-NSJU].

2. Jesse Damiani, *New Research Reveals Facial Recognition Software Misclassifies Transgender, Non-Binary People*, FORBES (Oct. 29, 2019, 3:21 PM), <https://www.forbes.com/sites/jessedamiani/2019/10/29/new-research-reveals-facial-recognition-software-misclassifies-transgender-non-binary-people/?sh=2925520606b5> [https://perma.cc/97HZ-RJQ8].

3. Rachel Metz, *Think Your Mask Makes You Invisible to Facial Recognition? Not so Fast, AI Companies Say*, CNN (Aug. 12, 2020, 8:14 AM), <https://www.cnn.com/2020/08/12/tech/face-recognition-masks/index.html> [https://perma.cc/Y2MF-G7YS] [hereinafter Metz, *Think Your Mask*].

this technology may still sound like it came from a science-fiction movie, the evolution of facial recognition technology makes all of this a reality across the globe.⁴

Facial recognition technology (“FRT”) may sound scary, but it has the potential to be very beneficial for national security, identifying criminals, and mitigating threats of terrorism.⁵ However, the technology does not come without issue, as the technology is often thought to violate privacy and is biased against people of color, women, transgender individuals, and people who do not present gender⁶ on the typical male-female gender-binary.⁷ The technology is largely unregulated and has highly irregular accuracy due to this racial and gender bias. The beneficial uses and issues of FRT creates an ethical dilemma between the technology’s security protections and privacy violations.

This Article specifically focuses on the use of FRT by the five permanent members of the United Nations (“UN”) Security Council which are China, France, the Russian Federation, the United Kingdom, and the United States (the five nations).⁸ As permanent members of the Security Council, these five nations are tasked with maintaining international security under the UN Charter.⁹

National leaders in these countries are forced to face the question of whether the national security mitigating benefits of FRT outweigh the privacy and equity concerns the technology imposes for populations often considered the most vulnerable. This Article proposes solutions to this ethical dilemma at a national and international level.

Section II walks through how FRT works, the accuracy of the technology, how the technology has expanded and evolved, and the beneficial uses of the technology. Section III discusses the bias of the technology and the

4. *Facial Recognition Market*, MKTS. & MKTS., <https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html> [<https://perma.cc/U4D9-MT67>].

5. *See infra* Section II.D.

6. Sex refers to the biological differences in anatomy between individuals. Gender refers to socially constructed appearances, behaviors, and expressions of sex, typically based on social norms and stereotypes. *Sex and Gender*, PLANNED PARENTHOOD, <https://www.plannedparenthood.org/learn/gender-identity/sex-gender-identity> [<https://perma.cc/9LB9-JF4N>].

7. Much of society operates on a gender binary, which classifies individuals as one of two genders: male or female. This binary aligns with the social construct that people with certain anatomy should present as “male,” and people with other anatomy should present as “female.” Damiani, *supra* note 2.

8. U.N. Charter, art. 23, ¶ 1.

9. *Id.* at art. 24, ¶ 1.

privacy implications of its use. Section IV then walks through the governing law including the constitutional privacy rights, the International Convention on Civil and Political Rights (“ICCPR”), the European Convention on Human Rights, the EU General Data Protection Regulation (“GDPR”), and the Guiding Principles on Business and Human Rights. Section V lays out the use of FRT by each of the five nations, and the legal implications of this FRT use. Section VI proposes solutions both at a national and international level, and Section VII concludes the Article.

II. BACKGROUND

A. How Facial Recognition Technology Works

FRT is a form of biometric which is “a way to identify someone based on physical characteristics: fingerprints, DNA, retinas, voice, [or] face.”¹⁰ The collected facial data is then considered biometric data.¹¹ Facial recognition technology works by detecting a face, analyzing or mapping out that face, and finally recognizing the identity of the person behind the face.¹² The technology relies on machine learning and algorithms to detect, map, and recognize faces.¹³

To train the technology, data consisting of large volumes of images of faces is fed to artificial intelligence (“AI”) systems which trains the algorithms to recognize patterns or physical traits of faces.¹⁴ To identify a face, FRT analyzes distinctive features of a person’s face.¹⁵ Some FRT

10. *Biometrics*, ACLU, <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics> [<https://perma.cc/8WCV-TD4H>].

11. *Amnesty International Calls for Ban on the Facial Recognition Technology for Mass Surveillance*, AMNESTY INT’L (June 11, 2020, 6:00 PM), <https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/> [<https://perma.cc/8WCV-TD4H>] [hereinafter *Amnesty International Calls for Ban*].

12. Thorin Klosowski, *Facial Recognition is Everywhere. Here’s What We Can Do About It*, N.Y. TIMES (July 15, 2020), <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/> [<https://perma.cc/N429-STZ5>].

13. *Id.*

14. Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> [<https://perma.cc/2HAY-55JL>].

15. *Street-Level Surveillance*, ELEC. FRONTIER FOUND., <https://www EFF.org/pages/face-recognition#:~:text=Face%20recognition%20systems%20use%20computer,in%20a%20face%20recognition%20database> [<https://perma.cc/KBJ3-ZXEM>].

analyzes physical features outside of just the face such as the clothing an individual is wearing¹⁶ or the length of an individual's hair.¹⁷

FRT allows a specific individual to be identified from a photo, video, or live surveillance.¹⁸ FRT can be used for one-to-one identification in which the technology identifies one individual against an image of one individual.¹⁹ In one-to-one FRT use, the technology is ensuring a person is who they say they are, often to gain entry or access. There is also one-to-many identification²⁰ in which one individual is attempted to be matched and identified amongst a database of many (sometimes billions)²¹ facial images.

When FRT is involved in one-to-many use, there must be a database of facial images to compare the image to. In practice, this form of FRT use entails “widespread bulk monitoring, collection, storage, [and] analysis or other use of material and collection of sensitive personal data . . . which amounts to indiscriminate mass surveillance.”²² When FRT is deployed in real time, a face can be spotted in a live crowd of people.²³ When FRT is implemented by governments or agencies, it is sometimes deployed using hidden cameras and closed-circuit television (“CCTV”).²⁴ It functions as a form of surveillance because it does not require the consent or participation of the individual being monitored.²⁵

16. Morgan Klaus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, 3 Proc. ACM Hum.-Comput. Interact., Vol. 3, No. CSCW, Art. 144 (Nov. 2019).

17. Short Wave, *Why Tech Companies are Limiting Police Use of Facial Recognition*, NPR, at 9:55 (Feb. 18, 2021), <https://www.npr.org/2021/02/17/968710172/why-tech-companies-are-limiting-police-use-of-facial-recognition> [<https://perma.cc/5PV2-S29N>].

18. Klosowski, *supra* note 12.

19. An example of this is unlocking a phone or apartment with your facial image. In one-to-one identification, the technology is essentially ensuring it is you. Short Wave, *supra* note 17, at 0:50.

20. *Id.* at 1:43.

21. 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> [<https://perma.cc/F73C-NXYG>] [hereinafter Hill, *The Secretive Company*].

22. *Amnesty International Calls for Ban*, *supra* note 11.

23. Mozur, *supra* note 14.

24. Damiani, *supra* note 2.

25. *Face Recognition Technology*, ACLU, <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology> [<https://perma.cc/SHA8-NPBN>] [hereinafter *ACLU Facial Recognition Technology*].

B. Accuracy of the Technology

Many companies selling the technology rely on a different algorithm with a distinct level of accuracy.²⁶ The accuracy of the technology is impacted by many factors including the specific algorithm used, the diversity of images used to train the algorithm,²⁷ and the physical conditions in which the FRT is deployed.²⁸ There is no international accuracy standard for FRT, and no nation has national accuracy standards for FRT.²⁹

Third-party independent organizations have conducted studies of global accuracy on FRT to try to determine how accurate the technology really is.³⁰ The inaccuracies across the various algorithms ranged from insubstantial to high levels inaccuracy.³¹ These studies also found that most algorithms have some level of demographic differential, with false positives more frequent than false negatives.³² A false positive means the FRT incorrectly considered two different individuals the same person.³³ Conversely, a false negative means the FRT did not match a person even though there was a match to be made.³⁴ A false negative may result in incorrect exclusion, but a false positive can lead to an incorrect inclusion of an individual.³⁵

C. The Expansion of its Use

The use of FRT has become mainstream in recent years.³⁶ Some individuals were first introduced to FRT through Apple's Face ID which

26. Tom Simonite, *Why Chinese Companies Plug a US Test for Facial Recognition*, WIRED (Mar. 6, 2020, 7:00 AM), <https://www.wired.com/story/china-earns-high-marks-us-test-facial-recognition/> [<https://perma.cc/PLQ5-GS9V>].

27. Klosowski, *supra* note 12.

28. William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, CSIS (Apr. 14, 2020), <https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter> [<https://perma.cc/PSD4-JTB3>].

29. *See infra* Section II.A.

30. U.S. DEP'T OF COM., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS (2019).

31. *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2019), <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software> [<https://perma.cc/38LJ-QGWM>] [*hereinafter NIST Study*].

32. U.S. DEP'T OF COM., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *supra* note 30.

33. *NIST Study*, *supra* note 31.

34. *NIST Study*, *supra* note 31.

35. *NIST Study*, *supra* note 31.

36. Klosowski, *supra* note 12.

allows iPhone users to unlock their device with a scan of the face.³⁷ The same technology has since found uses ranging from replacing keys for home access to protecting Taylor Swift from stalkers.³⁸ The prevalence of FRT is increasing as the technology improves and becomes normalized.³⁹

FRT is growing worldwide both in governmental and commercial use.⁴⁰ The technology continues to quickly evolve, pushing the boundaries of its capabilities and the possible uses of the tech. Recently, the technology has been used to predict emotional states⁴¹ such as fear on an individual's face.⁴² With this development, agencies can use the technology to determine if someone seems mad or angry enough to commit a crime and can preemptively stop the potential crime.⁴³ During the Coronavirus pandemic, companies quickly developed their FRT to ensure their technology could still recognize faces even with masks on, an item long used to avoid FRT.⁴⁴ To do so, some FRT companies developed their technology to identify individuals using only an image of the eyes.⁴⁵

The way in which FRT has been used and implemented across the globe differs.⁴⁶ In a few nations the technology is restricted, but in the majority of nations across the globe it is freely used or its use is at least being

37. This technology utilizes one-to-one use of FRT in which the FRT compares the face of the person attempting to unlock the phone, and the image of the face stored in the phone. Klosowski, *supra* note 12.

38. Klosowski, *supra* note 12.

39. See Klosowski, *supra* note 12.

40. Sintia Radu, *The Technology That's Turning Heads*, US NEWS (July 26, 2019, 4:38 PM), <https://www.usnews.com/news/best-countries/articles/2019-07-26/growing-number-of-countries-employing-facial-recognition-technology>.

41. Damiani, *supra* note 2.

42. Ryan Browne, *Tech Giants Want Rules on Facial Recognition, but Critics Warn that Won't be Enough*, CNBC (Aug. 30, 1:26 AM), <https://www.cnbc.com/2019/08/30/facial-recognition-tech-firms-want-regulation-but-critics-want-a-ban.html> [<https://perma.cc/5793-SBHF>].

43. Oscar Schwartz, *Don't Look Now: Why You Should be Worried About Machines Reading Your Emotions*, THE GUARDIAN (Mar. 6, 2019), <https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science> [<https://perma.cc/JNF4-9M6M>].

44. Alfred Ng, *Facial Recognition Firms are Scrambling to See Around Face Masks*, CNET (May 15, 2020, 5:00 AM), <https://www.cnet.com/health/facial-recognition-firms-are-scrambling-to-see-around-face-masks/> [<https://perma.cc/56QR-RTWG>].

45. Metz, *Think Your Mask*, *supra* note 3.

46. See 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/L9K6-ZZMU>].

considered by governments, industry, or both.⁴⁷ Some FRT is sold within the borders of the nation it was developed in, but some FRT is sold internationally.⁴⁸ One example of international FRT sales is the American company Clearview AI which has sold its FRT technology to national law enforcement agencies, government bodies, and police forces in twenty-six countries.⁴⁹

D. Beneficial Uses of the Technology

There are several beneficial uses of facial recognition technology. In one-to-one use, FRT can increase convenience and security.⁵⁰ For example, the technology has been implemented at apartment buildings which allows an individual to enter their⁵¹ apartment building without a key just by scanning their face at the entrance.⁵² The technology can also be fun for individuals to use and provides a positive user experience by allowing iPhone users to forgo a passcode, for example.⁵³ However, the real benefit of this technology is the security it can provide.

In one-to-one use, FRT likely provides minimal actual security protection, but in one-to-many use, the technology can be very beneficial in protecting national security.⁵⁴ The technology can be used to solve cases, identify victims,⁵⁵ identify perpetrators,⁵⁶ monitor known criminals, find suspects at large events, increase national security at borders or airports,⁵⁷ and find

47. Klosowski, *supra* note 12.

48. Sam Shead, *Facial Recognition Tech Developed by Clearview AI Could be Illegal in Europe, Privacy Group Says*, CNBC (June 11, 2020, 11:42 AM), <https://www.cnbc.com/2020/06/11/clearview-ai-facial-recognition-europe.html> [<https://perma.cc/W3UK-CUBQ>] [hereinafter Shead, *Facial Recognition Tech*].

49. The 17 nations Clearview AI is selling its FRT to include Belgium, Denmark, Finland, France, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Portugal, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom. *Id.*

50. Klosowski, *supra* note 12.

51. To ensure representation and inclusivity, this discussion will use the terms “their,” “themselves,” and “they” instead of “his or her” as grammar fails to include genders outside of the male-female binary just like facial recognition technology.

52. Denyer, *supra* note 1.

53. Klosowski, *supra* note 12.

54. Klosowski, *supra* note 12.

55. Short Wave, *supra* note 17, at 2:01.

56. Hill, *The Secretive Company*, *supra* note 21; see, e.g., Kashmir Hill, *The Facial-Recognition App Clearview Sees a Spike in Use After Capitol Attack*, N.Y. TIMES (Jan. 9, 2021), <https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html> [<https://perma.cc/F6HQ-M2RU>] [hereinafter Hill, *The Facial-Recognition App*] (FRT was used to identify perpetrators of the January 6, 2021 Trump supporting white nationalist attack on the U.S. capitol).

57. Klosowski, *supra* note 12.

people who have gone missing.⁵⁸ The technology has been used to reunite lost individuals who have Alzheimer's disease with their family, locate child rapists on the run, and help identify potential witnesses.⁵⁹ It has also proven to be useful when an individual is attempting to evade police detection, such as the case of a man who bit off his finger prints to avoid being identified by police.⁶⁰

Although the technology is rarely used alone in this capacity and typically has a human overseer,⁶¹ the technology does what a police agency cannot—it provides an ever-present eagle eye watching for wrongdoers. The wrongs the technology prevents differs broadly, ranging from ensuring individuals with COVID-19 are following quarantine orders,⁶² to identifying individuals who attacked the U.S. capitol on January 6th, 2021.⁶³

The technology is only growing in its use and capabilities, so the security and protection measures the technology provides will likely continue to grow as well. The beneficial uses of the technology will also likely increase if and when the technology becomes less biased and more accurate.

III. BIAS AND PRIVACY IMPLICATIONS – RACE AND GENDER

While FRT may be the cutting edge of policing and national security, the benefits of the technology do not come without flaw resulting in intrusive and potentially life-threatening bias and privacy violations.

A. Bias in Facial Recognition Technology

Facial recognition technology has major problems with bias, specifically regarding race and gender.⁶⁴ Because of these biases, the technology fails

58. *Delhi: Facial Recognition System Helps Trace 3,000 Missing Children in 4 Days*, TIMES OF INDIA (Apr. 22, 2018, 7:23), <https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/article-show/63870129.cms> [<https://perma.cc/LMM4-6T6E>].

59. 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/TU46-LKRB>].

60. *Id.*

61. Short Wave, *supra* note 17, at 11:42.

62. See, e.g., Mary Ilyushina, *How Russia is Using Authoritarian Tech to Curb Coronavirus*, CNN (Mar. 29, 2020, 12:01 AM), <https://www.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html> [<https://perma.cc/S2QN-QJ54>].

63. Hill, *The Facial-Recognition App*, *supra* note 56.

64. Short Wave, *supra* note 17, at 2:15.

to accurately identify people of color, women,⁶⁵ and people who don't present gender on the stereotypical male-female gender binary.⁶⁶

Bias creeps into FRT algorithms beginning with the data fed into the technology.⁶⁷ The technology creates a statistical model of what a face should look like based on the images that were fed to it during training; "the machine is only as smart as its training data."⁶⁸ Research has found that common data sets used by FRT companies are "overwhelmingly pale and male," with data being comprised of up to eighty-six percent white individuals.⁶⁹ When the technology does not learn what a black or brown face looks like, it will have a bias or preference towards white faces because it views the white face as "correct." While the exact level of bias depends on the specific algorithm used,⁷⁰ the evidence of bias raises the ethical quandary of any FRT use.

1. Racial Bias

Overall, FRT is not good at identifying people of color.⁷¹ Research has shown that the technology is more effective on lighter skinned faces than darker skinned faces.⁷² The issue of racial bias is one of a failure to identify individuals accurately more often when they have a greater pigmentation to their skin.

This racial bias could possibly be improved with greater racial diversity in the algorithmic data. FRT tends to be able to identify Asian and Caucasian people with a higher accuracy when the technology is developed in an Asian country.⁷³ It appears that racial inaccuracy of the technology decreases when the algorithm is trained using more images of that particular race.

65. *Id.* at 5:58.

66. Damiani, *supra* note 2.

67. Short Wave, *supra* note 17, at 6:33.

68. Short Wave, *supra* note 17, at 7:37.

69. Short Wave, *supra* note 17, at 7:37.

70. *Facial Recognition Technology (FRT)*, NIST (Feb. 6, 2020), <https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0> [<https://perma.cc/A9SM-PVZN>] [hereinafter NIST on FRT].

71. Jeffery N. Rosenthal & Huaou Yan, *Coming Face-to-Face With Facial Recognition Technology*, THE LEGAL INTELLIGENCER (July 29, 2019), https://plus.lexis.com/document/?pdmfid=1530671&crid=f853a061-d3e7-4e7a-98d9-1354def8d3d6&pddocfullpath=%2Fshared%2Fdocument%2Flegalnews%2Furn%3AcontentItem%3A5WP7-W6F1-JBM3-R1J4-00000-00&pdcontentcomponentid=12324&pdworkfolderlocatorid=NOT_SAVED_IN_WORKFOLDER&prid=59e5ef7c-0330-429d-8c79-58f272997ec1&ecompt4k&earg=sr1&cbc=0 [<https://perma.cc/NR6D-942L>].

72. Short Wave, *supra* note 17, at 2:15.

73. *NIST Study*, *supra* note 31.

2. Gender Bias

FRT also has a gender bias.⁷⁴ There are two kinds of gender bias in FRT. First, gender bias exists because the technology typically functions on a gender binary,⁷⁵ so it is inherently prejudicial against gender presentations outside the binary. Self-identified gender labels, such as non-binary,⁷⁶ agender,⁷⁷ or genderqueer⁷⁸ are universally not able to be classified by FRT.⁷⁹ Although these individuals may not be misidentified at higher rates than male or female identified genders, the technology cannot identify their identified gender whatsoever.⁸⁰ By only classifying gender as male or female,⁸¹ the technology perpetuates the idea that gender is binary. Gender is a social construct of the presentation of anatomical sex,⁸² so the notion that one must be either “male” or “female” presenting is clearly erroneous and antiquated.

The second form of gender bias, like the racial bias of FRT, exists when the technology fails to identify female gender presenting individuals with the same accuracy as male presenting individuals.⁸³ Similarly, the technology misidentifies transgender people and individuals not presenting gender on the male-female binary at higher rates than those who are not transgender and those who present gender based on the male-female binary.⁸⁴

74. Short Wave, *supra* note 17, at 2:15.

75. Scheuerman et al., *supra* note 16.

76. Non-binary is the term used by individuals to refer to gender when they do not fit within the male-female gender binary. *Nonbinary*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/nonbinary> [<https://perma.cc/7DUC-JZJD>].

77. Agender refers to the gender of an individual who does not identify as any particular gender. *Agender*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/agender> [<https://perma.cc/EN3J-T4DW>].

78. Genderqueer is a term used to refer to gender when an individual does not fit within the male-female binary. *Genderqueer*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/genderqueer> [<https://perma.cc/L2LG-RET4>].

79. This study showed that the technology correctly identified cisgender women 98.3 percent of the time and cisgender men 97.6 percent of the time, but only identified include genders outside of the male-female binary as well. transgender women correctly 87.3 percent of the time and transgender men only 70.5 percent of the time. Scheuerman et al., *supra* note 16.

80. Scheuerman et al., *supra* note 16.

81. Scheuerman et al., *supra* note 16.

82. *Gender and Health*, WORLD HEALTH ORGANIZATION [WHO], https://www.who.int/health-topics/gender#tab=tab_1 [<https://perma.cc/4MVN-95P4>].

83. NIST on FRT, *supra* note 70.

84. Scheuerman et al., *supra* note 16.

FRT is limited by the premise that gender can be classified by outward appearance.⁸⁵ For example, researchers have found correlations between short hair and how FRT classifies an individual's gender.⁸⁶ This has led Black women with afros to be misgendered⁸⁷ and thus misidentified at higher rates than white women.⁸⁸ Some algorithms even include traditionally gendered features like beards or mustaches or traditionally gendered clothing in gender identification.⁸⁹ The technology's gender bias impacts transgender and non-binary individuals, and anyone who does not present gender in a stereotypical gender normative⁹⁰ way.

Gender classification has been found to be inconsistent across FRT companies due to variances in algorithms.⁹¹ Some technology relies more heavily on gender stereotypes than others, as individuals who wear makeup and dress as a stereotypically presenting female have been classified as both male and female depending on the algorithm.⁹²

B. Privacy Implications

The widespread response to FRT implementation and use across the globe has been that the technology is invasive and goes too far.⁹³ This reaction shows that individuals, regardless of where they reside, hold an expectation of privacy that seems to be violated by the use of FRT.

Privacy is a basic expectation most individuals hold to some degree; it allows individuals to create boundaries for protection from arbitrary intrusion into the intimacies of life.⁹⁴ The ACLU defines privacy as, “a concept central to our identities, our ability to control information and our senses of self, and our interactions with other individuals and communities.”⁹⁵

85. Scheuerman et al., *supra* note 16.

86. Short Wave, *supra* note 17, at 9:48.

87. Short Wave, *supra* note 17, at 9:48.

88. *NIST Study*, *supra* note 31.

89. Scheuerman et al., *supra* note 16.

90. Gender normative means adhering to ideal or typical standards of femininity or masculinity. *Gender Normative*, MERRIAM WEBSTER, <https://www.merriamwebster.com/dictionary/gender%20normative> [<https://perma.cc/JNX7-R9D2>].

91. Scheuerman et al., *supra* note 16.

92. Scheuerman et al., *supra* note 16.

93. *See infra* Section V.A.

94. *The Right to Privacy and Why it Matters*, EACH OTHER (July 23, 2015), <https://eachother.org.uk/the-right-to-privacy-and-why-it-matters/> [<https://perma.cc/FJW6-RPZS>].

95. *Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights*, ACLU (Mar. 2014), <https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf> [hereinafter *Privacy Rights in the Digital Age*].

Privacy is a basic human right and is recognized as such by the United Nations in international human rights law such as the ICCPR.⁹⁶ Despite being a basic human right, there is no clear definition of the term “privacy” in international law.⁹⁷ The Secretary-General of the UN has observed:

[T]he very existence of an internationally recognized right to privacy presupposes agreement that there are certain areas of the individual's life that are outside the concern of either governmental authorities or the general public, areas which may vary in size from country to country, but which do possess a common central core.⁹⁸

The general reaction to FRT shows that its use may pry into the part of an individual's life that should exist outside of governmental concern.

The technology is evolving faster than privacy law can keep pace with, and “recent [technological] developments have called into question the extent to which traditional understandings of privacy remain[s] viable in modern times.”⁹⁹ When fundamental human rights laws, such as the ICCPR, were enacted, the technological capabilities of the twenty-first century were unimaginable and were thus not considered when writing the law.¹⁰⁰

FRT creates a “quantum shift” in the way individuals think about privacy.¹⁰¹ The technology invites a question of whether the idea of anonymity¹⁰² plays a role in the modern version of privacy, and if it does, whether FRT violates this right. While it is not expected that a face will be private while in a public setting, one does not expect greater scrutiny and analysis of the facial image for unknown and potentially unethical reasons. It is expected that in a public space, others see us as much as we see them, not more than we see them. It is not expected that someone in public can identify the name and details of an individual they do not know personally. The thought of someone not immediately in the vicinity watching and analyzing faces through FRT creates the same uncomfortable feeling of someone watching public actions through binoculars. This greater scrutiny and complete lack of anonymity feels to many like a total invasion of privacy.

96. International Covenant on Civil and Political Rights, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

97. See Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 B.U.L. REV. 2179, 2220 (2020).

98. Myres Smith McDougal, et al., HUMAN RIGHTS AND WORLD PUBLIC ORDER: THE BASIC POLICIES OF AN INTERNATIONAL LAW OF HUMAN DIGNITY 842 (2nd ed. 2019).

99. *Privacy Rights in the Digital Age*, *supra* note 95.

100. *Privacy Rights in the Digital Age*, *supra* note 95.

101. Turley, *supra* note 97.

102. Turley, *supra* note 97.

When one is aware others are watching, they make act differently. Accordingly, the technology “implicates the loss of freedom to move and interact in public spaces without fear of being recognized or tracked. [FRT] impacts the ability of individuals to freely form new experiences, associations, and viewpoints.”¹⁰³ If the use of FRT is known, people may not protest, speak freely, or pray in public for fear of being identified and punished for their actions.

However, non-disclosure of FRT use creates an issue of consent. The use of FRT does not require the knowledge or consent of the person subject to the technology.¹⁰⁴ The technology analyzes the face so if the FRT is not disclosed when used, it is nearly impossible to evade if an individual enters into a space where FRT has been implemented.¹⁰⁵

To train the algorithms, companies rely on large databases of facial images¹⁰⁶ which are taken—often without consent of the subject of the image—from various locations including websites, social media, dating services, and cameras in restaurants or college campuses.¹⁰⁷ Many FRT algorithms are proprietary and are thus not publicly disclosed,¹⁰⁸ so it is not always clear for each FRT company how many photos are in the database or where the photos came from. The number of photos in each database is likely very large—potentially in the billions; it has been found that Clearview AI has a database of three billion images taken from various websites including Facebook, YouTube, and Venmo.¹⁰⁹ While some of these facial datasets are kept private, others are shared both nationally and internationally with governments and companies.¹¹⁰

When one does not know their biometric data is being used, there is no way of knowing if one’s biometric data has been stolen. Biometric data can and has been stolen,¹¹¹ but unlike the way passwords and usernames can be reset after a breach, the face cannot be reset. Once the breach happens,

103. Turley, *supra* note 97.

104. ACLU *Facial Recognition Technology*, *supra* note 25.

105. One cannot avoid surveillance cameras if they do not know if and where it has been implemented.

106. Browne, *supra* note 42.

107. Cade Metz, *Facial Recognition Tech is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), <https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html> [<https://perma.cc/MYS3-DW2B>] [hereinafter Metz, *Growing Stronger*].

108. U.S. GOV’T ACCOUNTABILITY OFF., GAO-20-522, FACIAL RECOGNITION TECHNOLOGY: PRIVACY AND ACCURACY ISSUES RELATED TO COMMERCIAL USES (2020).

109. Hill, *The Secretive Company*, *supra* note 21.

110. Metz, *Growing Stronger*, *supra* note 107.

111. Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, THE GUARDIAN (Aug. 14, 2019), <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms> [<https://perma.cc/G38H-QYGF>].

the individual in the image is vulnerable to have their image used for sinister purposes; for example, for purposes that may send them to jail, to an encampment, or to a war-stricken country. The individual in the image may not have even known they were being subjected to FRT in the first place, but improper security of their facial data could cause them to suffer life-altering consequences.

The issue of privacy in FRT use has been exacerbated and accelerated by the global Coronavirus pandemic beginning in 2020.¹¹² As the Coronavirus spread across the globe, countries raced to track the spread of the virus.¹¹³ Some countries used FRT to track contagious individuals and monitor the spread of disease,¹¹⁴ but this opened the door to a new pandemic—intrusive and problematic surveillance through FRT.

C. Exacerbation of Privacy Concerns Caused by Bias

People of all races, genders, and national origins are subject to privacy concerns surrounding FRT, but these privacy issues are exacerbated for people of color and individuals not presenting gender on the binary. As the UN Committee on the Elimination of Racial Discrimination's Verene Shepherd stated, "[b]ig data and AI tools may reproduce and reinforce already existing biases and lead to even more discriminatory practices."¹¹⁵ The committee also pointed out that FRT use by policing agencies "risks deepening racism, racial discrimination, . . . and consequently the violation of many human rights" due to the technology's bias.¹¹⁶ It should be noted that although the committee did not mention the technology's gender discrimination, LGBT+¹¹⁷ individuals have historically faced discrimination across the globe and are similarly impacted by the technology.¹¹⁸

112. Ng, *supra* note 44.

113. Ilyushina, *supra* note 62.

114. Ilyushina, *supra* note 62.

115. *UN Committee Issues Recommendations to Combat Racial Profiling*, OHCHR (Nov. 26, 2020), <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26548&LangID=E> [<https://perma.cc/RV5N-NAEZ>].

116. *Id.*

117. LGBT+ stands for Lesbian, Gay, Bi-sexual, Transgender. The plus typically includes individuals who do not represent gender on the male-female gender binary. See Kendra Cherry, *What Does LGBTQ+ Mean*, VERYWELLMIND (Nov. 30, 2020), <https://www.verywellmind.com/what-does-lgbtq-mean-5069804> [<https://perma.cc/9AQH-85W>].

118. See *Police Violence Around the World*, AMNESTY INT'L, <https://www.amnestyusa.org/issues/deadly-force-police-accountability-police-violence/> [<https://perma.cc/A4SS-52YY>] [hereinafter *Police Violence*]; see also Margaret Goff, *Five Reasons Mass*

In an age of increasing gender diversity, identification technology that functions on a gender binary is not accurate and has the potential to reinforce gender stereotypes and may cause exclusion, unequal access, and discrimination.¹¹⁹ The ramifications of this technology's use of gender normative characteristics for identifying sex can reinforce harmful gender stereotypes.¹²⁰ For example, one of China's FRT uses includes monitoring restroom entrances.¹²¹ Individuals are granted entry if the FRT identifies the individual as the gender the restroom is designated to serve—male or female.¹²² For those not presenting gender on the typical binary, this sort of gender classification required for entry has the potential to obstruct access completely. Gender classification based on physical appearance is inherently discriminatory.

The technology discriminates in large part because of the false positives the bias causes. The algorithmic bias is less accurate and thus results in more false positives for people of color and non-binary gender presenting individuals.¹²³ The United States' National Institute of Technology and Standards ("NIST") conducted research relating to bias in FRT, and found that in one-to-one matching, some algorithms produced 100 times more false positives with African and Asian faces compared to Eastern European faces.¹²⁴ While existing research largely focuses on one-to-one FRT matching, NIST has found that similar demographic disparities also exist in some one-to-many FRT—but it all depends on the algorithm.¹²⁵ This disproportionate impact of FRT use can lead to detrimental effects for already marginalized communities.¹²⁶

When FRT is used for security purposes, an increased number of false positives for a certain demographic will likely result in more government interventions and interactions for individuals of that particular demographic. When used for policing, more false positives can lead to more interactions

Incarceration is a Queer Issue, URB. WIRE: CRIME & JUST. (Oct. 24, 2017), <https://www.urban.org/urban-wire/five-reasons-mass-incarceration-queer-issue> [<https://perma.cc/25CF-YGNX>].

119. Damiani, *supra* note 2.

120. Scheuerman et al., *supra* note 16.

121. Denyer, *supra* note 1.

122. Denyer, *supra* note 1.

123. NIST Study, *supra* note 31.

124. NIST on FRT, *supra* note 70.

125. NIST on FRT, *supra* note 70.

126. Short Wave, *supra* note 17, at 6:27.

between racially, ethnically,¹²⁷ and gender identity prejudiced¹²⁸ police agencies and people of color, transgender individuals, and non-binary individuals. When minor infractions lead to arrest and prosecution, inaccuracies in FRT could result in increased rates of arrest and prosecution for these groups of people.¹²⁹ These results will perpetuate already existing oppression of people of color, non-binary, and transgender individuals.

Even if the FRT algorithm bias in a specific algorithm is minimal, FRT can create additional problems depending on who is using the technology and for what purpose. If the technology is in the hands of an individual or agency that engages in discriminatory or prejudicial profiling, the technology can be used to promote oppression. For example, in China government officials sorted people by religious affiliation—solely relying on stereotypical facial characteristics of people in that religion—and placed certain individuals in camps based on this categorization.¹³⁰ Similarly, in the U.S. the technology has been used by police agencies which recently drew global backlash due to the systematic racial prejudice in the American policing system.¹³¹

IV. LEGAL BACKGROUND AND IMPLICATIONS OF FRT USE

There are several laws and guiding principles related to privacy that govern each of the permanent National Security Council members including national

127. Racial and ethnic bias in policing and/or government authority has been seen in China, France, Russia, the United Kingdom, and the United States. Sarah Cahlan & Joyce Sohyun Lee, *Video Evidence of Anti-Black Discrimination in China Over Coronavirus Fears*, WASH. POST (June 18, 2020), <https://www.washingtonpost.com/politics/2020/06/18/video-evidence-anti-black-discrimination-china-over-coronavirus-fears/?arc404=true> [https://perma.cc/4HZU-YHQ7]; Bénédicte Jeannerod & Judith Sunderland, *Time to Stop Ethnic Profiling in France*, HUM. RTS. WATCH (Jan. 28, 2021, 12:00 AM), <https://www.hrw.org/news/2021/01/28/time-stop-ethnic-profiling-france> [https://perma.cc/RG3E-293V]; MIRNA ADJAMI, *ETHNIC PROFILING IN THE MOSCOW METRO 9* (David Berry, James A. Goldston & Anita Soboleva eds. 2006); Anthony Cuthbertson, *Eleven Charts that Show Extent of Racial Inequality in the UK*, THE INDEP. (June 18, 2020, 3:28 PM), <https://www.independent.co.uk/news/uk/home-news/racism-uk-inequality-black-lives-matter-wealth-economic-health-a9567461.html> [https://perma.cc/9PQZ-HXME]; *Police Violence*, *supra* note 118.

128. *Police Violence*, *supra* note 118.

129. Nina Larson, *UN Urges 'Moratorium' on Facial Recognition Tech Use in Protests*, BARRON'S (June 25, 2020), <https://www.barrons.com/news/un-urges-moratorium-on-facial-recognition-tech-use-in-protests-01593091505> [https://perma.cc/8S2J-4KCG].

130. Mozur, *supra* note 14.

131. Kade Crockford, *How is Face Recognition Surveillance Technology Racist*, ACLU (June 16, 2020), <https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/> [https://perma.cc/HA6B-B7RU].

constitutions, the International Convention on Civil and Political Rights, the EU General Data Protection Regulation, the European Convention on Human Rights, and the Guiding Principles on Business and Human Rights.

A. Constitutional Privacy Rights in Each of the Five Nations

The permanent members of the UN's Security Council have varying levels of constitutional privacy protections. Additionally, the constitutions that do provide some form of privacy protections do not clearly define "privacy," related terms, or the expanse of the protection.

It should be noted that although China and Russia technically have independent court systems, they do not operate as such.¹³² This lack of functional independence renders the constitutional privacy provisions of each nation less binding because the judiciary is not required to abide by the constitution, but rather the outside forces controlling it.

1. China

The Chinese Constitution lists as a fundamental right, "[f]reedom and privacy of correspondence of citizens."¹³³ Infringing on this right by an organization or individual is not allowed, except where it is needed "to meet the needs of State security or of criminal investigation, [or] public security."¹³⁴

2. France

France has no constitutional provisions specifically granting a right to privacy.¹³⁵

3. Russian Federation

Russia's Constitution provides that, "[e]veryone shall have the right to the inviolability of his (her) private life, personal and family privacy, and protection of his (her) honour and good name."¹³⁶ Additionally, the

132. *Russian Federation: Independence and Impartiality; Judicial Integrity and Accountability*, INT'L COMM'N OF JURISTS (June 16, 2014), <https://www.icj.org/cijlcountryprofiles/russian-federation/russian-federation-judges/russian-federation-independence-and-impartiality-judicial-integrity-and-accountability-2/> [<https://perma.cc/KW4U-8ADN>] [hereinafter *Russian Federation*]; HE WEIFANG, ET AL., IN THE NAME OF JUSTICE: STRIVING FOR THE RULE OF LAW IN CHINA 35 (2012) [hereinafter *IN THE NAME OF JUSTICE*].

133. XIANFA, art. 40, (1982).

134. *Id.*

135. 1958 CONST. (Fr.).

136. KONSTITUTSIJA ROSSIJSKOJ FEDERATSII [KONST. RF] [CONSTITUTION] art. 23 (Russ.).

Constitution includes specific rights as to digital privacy stating “[e]veryone shall have the right to privacy of correspondence, of telephone conversations and of postal, telegraph and other communications. This right may be limited only on the basis of a court order.”¹³⁷

The Russian Federation’s Constitution must again be qualified. Russia has a history of disregarding its constitutional protections, as the 1936 Constitution offered Russian citizens similar protections that were blatantly disregarded by the Stalin regime.¹³⁸

4. *United Kingdom*

The United Kingdom differs from the other countries in this analysis as it does not have one codified constitution like the others. However, the Human Rights Act of 1988 and the European Convention on Human Rights, two constitutional documents of the nation, have been relied upon to establish a general right to privacy for citizens.¹³⁹

5. *United States*

The United States Constitution does not explicitly grant the American people privacy rights, but the Supreme Court of the United States found the right to privacy implicit in the Bill of Rights, specifically through the First, Third, Fourth, Fifth, and Ninth Amendments of the United States Constitution.¹⁴⁰

The Supreme court has also warned of the chilling effect government action may have on individual freedoms, such as “the freedom of expression, by making the individual more reluctant to exercise [that right].”¹⁴¹

137. *Id.*

138. J. Arch Getty, *State and Society Under Stalin: Constitutions and Elections in the 1930s*, 50 *SLAVIC REV.* 18, 18 (1991).

139. Robert Walker, *The English Law of Privacy – An Evolving Human Right*, THE SUP. CT. https://www.supremecourt.uk/docs/speech_100825.pdf [<https://perma.cc/RH8L-JTTP>].

140. The First Amendment provides for the freedom of speech, religion, assembly, press and petition, the Third Amendments guarantees against the quartering of soldiers without consent, the Fourth Amendment protects from unreasonable searches and seizures, the Fifth amendment protects against self-incrimination, and the Ninth Amendment provides the enumeration clause stating the listing of rights in the constitution does not mean other rights do not exist. U.S. Const. amends. I, III, IV, V, IX; *Griswold v. Connecticut*, 381 U.S. 479, 485 (1965).

141. *See, e.g., Smith v. California*, 361 U.S. 147, 151 (1959).

Although privacy as to a picture or image of one's face is generally not protected by the U.S. Constitution,¹⁴² FRT creeps into the territory of mass surveillance which leads to the above-mentioned chilling of individual expression.¹⁴³

B. United Nations International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights is a United Nations international human rights treaty.¹⁴⁴ It provides a range of protections for civil and political rights including provisions regarding a right to privacy.¹⁴⁵ The ICCPR is considered to be part of the International Bill of Human Rights.¹⁴⁶

Article 17 of the ICCPR states that “[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”¹⁴⁷ Comment 16 provides more, but not binding, clarification regarding privacy in Article 17 from the UN Human Rights Committee:

The gathering and holding of personal information on computers . . . whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for

142. Katz v. United States, 389 U.S. 347, 351 (1967).

143. It has long been held that individuals act differently when they know they are being watched. See, e.g., Spencer EA & Mahtani K, *Hawthorne Effect. When Individuals Modify an Aspect of their Behaviour in Response to their Awareness of Being Observed*, SACKETT CATALOGUE OF BIAS (2017), <https://catalogofbias.org/biases/hawthorne-effect/> [<https://perma.cc/B2R8-PLYG>].

144. ICCPR, *supra* note 96.

145. ICCPR, *supra* note 96.

146. The International Bill of Human Rights consists of three documents: (1) the Universal Declaration of Human Rights, (2) the International Covenant on Economic, Social and Cultural Rights, and (3) the ICCPR. Together, they address various issues including “racial discrimination, torture, enforced disappearances, disabilities, and the rights of women, children, migrants, minorities, and indigenous peoples. *The Foundation of Human Rights Law*, UNITED NATIONS, <https://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html> [<https://perma.cc/BN29-8UQQ>]; ICCPR FAQ, ACLU, https://www.aclu.org/sites/default/files/assets/faq_iccpr_updated_april_2014.pdf [<https://perma.cc/TV3T-L7PH>].

147. ICCPR, *supra* note 96, at art. 17.

what purposes. Every individual should also be able to ascertain which public [authorities] or private individuals or bodies control or may control their files.¹⁴⁸

This Comment requires nations to regulate FRT nationally with adequate storage measures for biometric data and disclosure of FRT use.

The ICCPR also provides that each nation must “respect and . . . ensure to all individuals within its territory . . . the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, . . . religion, . . . [or] national or social origin”¹⁴⁹

Article 9 of the treaty states “[n]o one shall be subjected to arbitrary arrest or detention.”¹⁵⁰

However, Article 12 of the ICCPR, provides that all of the rights stated in the treaty can be restricted in ways “necessary to protect national security, public order . . . public health or morals or the rights and freedoms of others, and are consistent with the other rights recognized in the [ICCPR].”¹⁵¹

Ratification of a treaty signifies intent to be bound by the treaty, whereas solely signing it does not establish consent to be bound, just a willingness to continue in the treaty making process.¹⁵² The five countries, China, France, the United Kingdom, the United States, and the Russian Federation, have all signed the ICCPR.¹⁵³ Thus, all nations have an obligation to “refrain, in good faith, from acts that would defeat the object and purpose of the treaty.”¹⁵⁴ All but China have ratified the ICCPR, committing to ensure that their citizens are not subjected to “arbitrary or unlawful interference with [their] privacy.”¹⁵⁵

148. U.N. Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Apr. 8, 1988).

149. ICCPR, *supra* note 96, at art. 12.

150. *Id.* at art. 9.

151. *Id.* at art. 12.

152. *What is the Difference Between Signing, Ratification and Accession of UN Treaties*, UNITED NATIONS (Dec. 17, 2020, 11:05 AM), <https://ask.un.org/faq/14594> [<https://perma.cc/DWG7-CTWJ>] [hereinafter *What is the Difference*].

153. Status of International Covenant on Civil and Political Rights (Sept. 11, 2021, 10:50 AM), <https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20IV/IV-4.en.pdf> [perma.cc/9CEC-8B57].

154. *What is the Difference*, *supra* note 152.

155. ICCPR, *supra* note 96, at art. 17.

C. European Convention on Human Rights

The European Convention on Human Rights is an international treaty aimed at protecting human rights.¹⁵⁶ It has been ratified by France, Russia, and the United Kingdom.¹⁵⁷ The treaty provides that “[e]veryone has the right to respect for his private and family life, his home and his correspondence.”¹⁵⁸ Additionally it states that:

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.¹⁵⁹

D. European Union General Data Protection Regulation

The European Union’s General Data Protection Regulation sets out standards for the processing and collection of biometric data in countries in the European Union (“EU”), which includes France.¹⁶⁰ Under the GDPR guidelines, biometric data includes data relating to the “physical, physiological or behavioral characteristics of a natural person, . . . such as facial images. . . .”¹⁶¹ The GDPR generally does not allow the use of biometric data collection unless an exception applies under the regulation.

The GDPR also sets express limitations on the transfer of data to other countries, which, because FRT utilizes biometric data, limits the transfer of FRT information between countries outside of the EU.¹⁶²

E. UN Guiding Principles on Business and Human Rights

The issue of company regulation has been addressed on a global scale, but no legally binding regulation has been set. The UN has endorsed the Guiding Principles on Business and Human Rights which set the first global standard for preventing and addressing adverse human rights impacts

156. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

157. Chart of Signatures and Ratifications of Treaty 005, Council of Europe (Mar. 7, 2021, 3:26 PM), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=DJRV0ml0 [<https://perma.cc/8DTZ-SKQS>].

158. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

159. *Id.*

160. Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

161. *Id.* at art. 4.

162. *Id.* at art. 2.

associated with business activity.¹⁶³ The principles apply to nations and businesses and instruct them to abide by international law in business so to maintain “socially sustainable globalization.”¹⁶⁴ The framework of principles is not legally binding.¹⁶⁵

V. FRT USE AND IMPLICATIONS IN EACH OF THE FIVE NATIONS

A. *FRT Use in Each of the Five Nations*

The use of FRT is prevalent in each of the five nations that hold permanent seats at the UN Security Council. The FRT implementation has not come without challenge; there is widespread public backlash against the use of FRT in each of these nations. Despite the growing public uncertainty as FRT continues to expand in use, none of these nations have legislation specific to FRT nor do they have biometric data legislation with strong enough teeth to prevent its use. All five nations claim to be implementing and/or using the technology for national security and/or public health purposes.

1. *China*

In China, FRT is technically regulated by the Cybersecurity Law of the People's Republic of China, and although it specifically discusses biometric data,¹⁶⁶ it has not been strong enough to limit the use of FRT in the country. In the spring of 2020, Chinese legislatures drafted new legislation with a stronger focus on biometrics to create teeth and address the very clear need for greater protection, but the legislation has not yet come to fruition.¹⁶⁷ Currently, there is ongoing litigation regarding private use of

163. U.N. Hum. Rts. Council, Guiding Principles on Business and Human Rights, A/HRC/17/31 (2011), https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf [perma.cc/34XS-M2UT].

164. *Id.*

165. *Id.*

166. Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. of the Nat'l People's Cong., Nov. 7, 2015, effective June 1, 2017), art. 53, LEXIS 1603.

167. Seungha Lee, *Coming into Focus: China's Facial Recognition Regulations*, CTR. FOR STRATEGIC & INT'L STUD. (May 4, 2020), <https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations#:~:text=Facial%20recognition%20in%20China%20is,the%20People's%20Republic%20of%20China.&text=It%20specifies%20guidelines%20on%20data,collection%2C%20abuse%2C%20and%20access> [https://perma.cc/9B8C-UDLL].

FRT by a park, which is the first time FRT has been legally challenged in the nation.¹⁶⁸

China has a vast network of cameras across the country to enable the widespread use of facial recognition technology.¹⁶⁹ The country has at least 626 million FRT cameras in place.¹⁷⁰ The cameras have been placed in a myriad of locations including railways, airports, gyms, offices, dormitories, exhibition halls,¹⁷¹ hotels, public toilets, and the entrance of apartment buildings.¹⁷²

The technology is also used by police to track suspects and monitor suspicious behavior, to spot suspects, and to predict and prevent crime.¹⁷³ FRT databases catalogue for those with “criminal records, mental illnesses, records of drug use, and those who petitioned the government over grievances.”¹⁷⁴ Many companies are producing the technology in China, these include Yitu, Megvii, SenseTime, and Cloudwalk.¹⁷⁵

In the past, the Chinese government used FRT for legitimate and beneficial purposes, but there is a growing concern among the Chinese population that the practice has become overly intrusive.¹⁷⁶ Currently, the Chinese government uses FRT for intimidation and mass surveillance of the Chinese people.¹⁷⁷ For example, all Chinese phone users that use a SIM card must submit mandatory facial scans to the government through FRT.¹⁷⁸

168. *Id.*

169. Emily Feng, *How China is Using Facial Recognition Technology*, NPR (Dec. 16, 2020, 4:24 PM), <https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology> [https://perma.cc/684P-U2M8].

170. Lauren Dudley, *China's Ubiquitous Facial Recognition Privacy Backlash*, THE DIPLOMAT (Mar. 7, 2020), <https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/> [https://perma.cc/596E-U8KG].

171. Ma Zhenhuan, *Park Alters Entry Rules Following Facial Recognition Tech Lawsuit*, CHINA DAILY (Updated Nov. 7, 2019), <http://global.chinadaily.com.cn/a/201911/07/WS5dc38381a310cf3e35575f3a.html> [https://perma.cc/EQ28-YU2A].

172. Denyer, *supra* note 1.

173. Denyer, *supra* note 1.

174. Mozur, *supra* note 14.

175. Mozur, *supra* note 14.

176. Sam Shead, *Chinese Residents Worry About Rise of Facial Recognition*, BBC (Dec. 5, 2019), <https://www.bbc.com/news/technology-50674909> [https://perma.cc/X2TC-3PJX].

177. *See* Mozur, *supra* note 14.

178. Lily Kuo, *China Brings in Mandatory Facial Recognition for Mobile Phone Users*, THE GUARDIAN (Dec. 2, 2019), <https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users> [https://perma.cc/FQ9N-Y58K].

One major use of FRT in China,¹⁷⁹ which has raised a global outcry, has been the tracking and detainment of the Uighur Muslim population.¹⁸⁰ Uighurs are a Muslim minority group in China.¹⁸¹ The Chinese government uses FRT to track the movements of Chinese Uighurs and looks for members of the Uighur population based on their facial characteristics using FRT.¹⁸²

International data has been used to train FRT used in China, including the FRT used by China to detain members of the Uighur population.¹⁸³ A database, aptly called “Brainwash,” which included 10,000 facial images of potentially unaware¹⁸⁴ United States café goers was made public and subsequently used in China by a company which provided surveillance technology used to monitor the Uighurs.¹⁸⁵

China keeps watch on the eleven million members of the Uighur population in China,¹⁸⁶ and over one million Uighurs have been put in one of the eighty-five identified detainment camps set aside for the Uighurs since 2017.¹⁸⁷ China has defended its detainment of the Uighurs in the name of anti-terrorism, yet Uighurs have been singled out and detained using FRT based only on their apparent presentation of race, ethnicity, and religion.¹⁸⁸

179. See *Data Leak Reveals how China ‘Brainwashes’ Uighurs in Prison Camps*, BBC (Nov. 24, 2019), <https://www.bbc.com/news/world-asia-china-26414014> [<https://perma.cc/P72E-UUBB>] [hereinafter *Data Leak*].

180. Humeyra Pamuk & David Brunnstrom, *U.S. Leads Condemnation of China for ‘Horiffic’ Repression of Muslims*, REUTERS (Sept. 24, 2019, 3:19 PM), <https://www.reuters.com/article/us-usa-china-un-xinjiang/u-s-leads-condemnation-of-china-for-horiffic-repression-of-muslims-idUSKBN1W92PX> [<https://perma.cc/M4P7-KR69>].

181. See *Data Leak*, *supra* note 179.

182. Mozur, *supra* note 14.

183. Metz, *Growing Stronger*, *supra* note 107.

184. A research study conducted by Stanford University collected facial data from café goers in San Francisco, California, United States. The research done by Stanford to collect facial recognition data did not acknowledge whether or not the café patrons knew they were being photographed for research. See Metz, *Growing Stronger*, *supra* note 107.

185. Metz, *Growing Stronger*, *supra* note 107.

186. Mozur, *supra* note 14.

187. Bryan Wood, *What is Happening with the Uighurs in China*, PBS NEWS HOUR, <https://www.pbs.org/newshour/features/uighurs/> [<https://perma.cc/DD4U-JFRB>].

188. Mozur, *supra* note 14.

China has publicly claimed the camps are for reformation and re-education, but those who have left the camps have reported abuse.¹⁸⁹ Uighurs who had been in the camps said they were “detained, interrogated and beaten because of their religion.”¹⁹⁰ Those detained have reportedly been subject to “brainwashing,” and human rights advocates say the camps are a “gross human rights violation.”¹⁹¹

Recently, it was reported that Uighurs in the camps were subjected to forced labor, including mask production due to the Coronavirus outbreak.¹⁹² Some fear the Chinese government will use Coronavirus as an excuse for increased detention and policing of the Uighurs.¹⁹³

In September 2019, the U.S. and twenty-nine other countries condemned the Chinese camps.¹⁹⁴ China has recently stated the camps are closed, but there is significant reason to doubt this claim by the Chinese government.¹⁹⁵ The Chinese use of FRT to detain and potentially abuse Uighurs illustrates one of the key issues of FRT use: profiling based upon stereotypical identifying features.

2. France

France recently began using facial recognition technology.¹⁹⁶ The French government first used the city of Nice as a testing ground for mass surveillance through FRT in 2019.¹⁹⁷ This newfound use of FRT was met with public outcry largely due to the lack of regulatory framework for the technology.¹⁹⁸ Since its implementation, several groups called on the government to institute a moratorium to ensure the nation’s use of FRT

189. Chris Buckley, *China Is Detaining Muslims in Vast Numbers. The Goal: ‘Transformation’*, N.Y. TIMES (Sept. 8, 2018), <https://www.nytimes.com/2018/09/08/world/asia/china-uighur-muslim-detention-camp.html> [https://perma.cc/UCB9-NEW8].

190. Wood, *supra* note 187.

191. *Data Leak*, *supra* note 179.

192. Muyi Xiao et al., *China is Using Uighur Labor to Produce Face Masks*, N.Y. TIMES (July 19, 2020, updated Aug. 13, 2020), <https://www.nytimes.com/2020/07/19/world/asia/china-mask-forced-labor.html?action=click&module=RelatedLinks&pgtype=Article> [https://perma.cc/J9JE-H5LS].

193. Javier C. Hernández, *China Locks Down Xinjiang to Fight Covid-19 Angering Residents*, N.Y. TIMES (Sept. 24, 2020), <https://www.nytimes.com/2020/08/25/world/asia/china-xinjiang-covid.html> [https://perma.cc/FNB4-6K7C].

194. Pamuk & Brunnstrom, *supra* note 180.

195. Buckley, *supra* note 189.

196. The specific date and year are not certain due to inadequate transparency, although it became known around 2019. See Martin Untersinger, *Facial Recognition: The CNIL Ticks on the Results of the Nice Experience*, LE MONDE (Aug. 28, 2019), https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html [https://perma.cc/3AB4-Q4CJ].

197. *Id.*

198. *Id.*

does not result in the level of surveillance seen in China.¹⁹⁹ The nation's security watchdog, the Commission Nationale de l'informatique et des Libertés (CNIL), has called for legislation regarding FRT, but no legislation has been passed.²⁰⁰

In 2019, France announced its plan for national FRT surveillance through an initiative called "Alicem" which will create facial IDs for residents using FRT.²⁰¹ Clearview, an American company, supplied at least part of this FRT.²⁰² Although the country's independent privacy regulator pointed to issues of security regarding Alicem²⁰³ and other opponents say the plan may break EU General Data Protection Regulation, the nation appears to be moving forward with the plan.²⁰⁴ The EU briefly considered a ban on FRT for public surveillance but has since dropped that idea.²⁰⁵

3. Russian Federation

Russia began rolling out mass surveillance facial recognition cameras in early 2020, which prompted backlash and a suit against the government.²⁰⁶ There is concern from the Russian people regarding the lack of regulation, oversight, and data protection regarding the nation's use of FRT.²⁰⁷ Although Russian law requires explicit consent from an individual for the government to collect biometric data via FRT, the law allows for FRT use

199. *Facial Recognition: The Urgency of a Moratorium*, LIBÉRATION (Dec. 17, 2019), https://www.liberation.fr/debats/2019/12/17/reconnaissance-faciale-l-urgence-d-un-moratoire_1769794/ [<https://perma.cc/C7PV-U75S>] [hereinafter Libération].

200. Untersinger, *supra* note 196.

201. Helene Fouquet, *France Set to Roll out Nationwide Facial Recognition ID Program*, BLOOMBERG (Oct. 2, 2019, 9:00 PM), <https://www.bloomberg.com/news/articles/2019-10-03/french-liberte-tested-by-nationwide-facial-recognition-id-plan> [<https://perma.cc/S872-4P6Y>].

202. Shead, *Facial Recognition Tech*, *supra* note 48.

203. *Délibération 2018-342 du 18 Octobre 2018*, LÉGIFRANCE, <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038477075/> [<https://perma.cc/ZUS3-TWD9>] [hereinafter Délibération].

204. Fouquet, *supra* note 201.

205. Foo Yun Chee, *EU Drops Idea of Facial Recognition Ban in Public Areas: Paper*, REUTERS (Jan. 29, 2020, 3:09 PM), <https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q> [<https://perma.cc/8ZDM-7RM2>].

206. Ilyushina, *supra* note 62.

207. *Russia Expands Facial Recognition Despite Privacy Concerns*, HUM. RTS. WATCH (Oct. 2, 2020, 8:00 AM), <https://www.hrw.org/news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns> [<https://perma.cc/6L8P-3VHJ>].

without consent for justice or national security purposes.²⁰⁸ A recent ruling from a suit challenging the nation's use of FRT was dismissed, solidifying the legality of its implementation, and showing legal objections in Russian courts to the use of FRT will very likely be dismissed.²⁰⁹

Moscow has at least 105,000 FRT surveillance cameras, all of which are developed by the firm NTechLabs.²¹⁰ The country began using FRT to track individuals infected with Coronavirus using public health as a justification for rolling out large numbers of FRT cameras.²¹¹ In June of 2020, Russia announced a plan to install FRT in every school in the country.²¹²

The Moscow Department of Technology claims that FRT is being used to ensure safety.²¹³ Police officers are allowed to make requests to view the FRT surveillance video.²¹⁴ However, even when police in Russia were not yet using the FRT, police officers allegedly paid people with access to the technology to run searches via internet transactions.²¹⁵

4. United Kingdom

The UK implemented FRT as early as 2015, despite public backlash and reports showing the technology being deployed was extremely inaccurate.²¹⁶ The United Kingdom has no legislation specifically regarding the use of facial recognition technology.²¹⁷ Despite the tech's growing use in the

208. Federal'nyi Zakon No. 152-FZ RF o Personal'nyh Danyih [Federal Law No. 152-FZ of the Russian Federation on Personal Data], ROSSIIŖSKAIA GAZETA [ROS. GAZ] July 8, 2006.

209. Alexander Marrow, *Russian Court Rules in Favor of Facial Recognition Over Privacy Claims*, REUTERS (Mar. 3, 2020, 8:22 AM), <https://www.reuters.com/article/us-russia-technology-facialrecognition/russian-court-rules-in-favor-of-facial-recognition-over-privacy-claims-idUSKBN20Q29U> [<https://perma.cc/DY37-UY3U>].

210. Alina Polyakova & Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, BROOKINGS (Aug. 2019), https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

211. Ilyushina, *supra* note 62.

212. *Russia to Install 'Orwell' Facial Recognition Tech in Every School – Vedomosti*, THE MOSCOW TIMES (June 16, 2020), <https://www.themoscowtimes.com/2020/06/16/russia-to-install-orwell-facial-recognition-tech-in-every-school-vedomosti-a70585> [<https://perma.cc/GU73-X2PK>].

213. Marrow, *supra* note 209.

214. Marrow, *supra* note 209.

215. Patrick Reeve, *How Russia is Using Facial Recognition to Police its Coronavirus Lockdown*, ABC (Apr. 30, 2020, 2:06 AM), <https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736> [<https://perma.cc/H8PW-TMVD>].

216. *Stop Facial Recognition*, BIG BROTHER WATCH, <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>.

217. Davey Winder, *Police Facial Recognition Use Unlawful – U.K. Court of Appeal Makes Landmark Ruling*, FORBES (Aug. 12, 2020, 6:53 AM), <https://www.forbes.com/>

country, in August of 2020, a South Wales court ruled that the use of FRT was illegal.²¹⁸ The court cited the technology as being a violation of the European Convention on Human Rights because the South Wales Police's implementation of the technology left "too broad a discretion" to individual police officers.²¹⁹ While this ruling was specifically about Wales, this ruling has the potential to be far-reaching and render the technology illegal in the country until the government approves its use through statute.²²⁰

The London Metropolitan Police has been using FRT since January 2020, with the stated purpose of identifying serious and violent criminals.²²¹ The UK has a history of video surveillance, but the addition of FRT increases the scrutiny of the surveillance and adds to the amount of surveillance policing in the nation.²²² The United Kingdom also uses FRT developed outside of the EU; for example, the American company Clearview sells its technology to the UK.²²³

5. United States

There is currently no national FRT regulation in the United States.²²⁴ Despite the lack of federal regulation, three states, California, New Hampshire, and Oregon, have placed restrictions on the technology's use by police

sites/daveywinder/2020/08/12/police-facial-recognition-use-unlawful-uk-court-of-appeal-makes-landmark-ruling/?sh=3e1c18b775e0 [https://perma.cc/BNN4-78P2].

218. Bridges, R v. South Wales Police [2020] EWCA (Civ) 1058, [201] (appeal taken from Eng.) (UK).

219. *Id.* at 124.

220. Sam Shead, *UK Court Finds Facial Recognition Technology Used by Police was Unlawful*, CNBC (Aug. 11, 2020, 9:55 AM), <https://www.cnbc.com/2020/08/11/swp-facial-recognition-unlawful.html> [https://perma.cc/XG32-GE3L]; Winder, *supra* note 217.

221. Danny Shaw, *Met Police to Deploy Facial Recognition Cameras*, BBC (Jan. 30, 2020), <https://www.bbc.com/news/uk-51237665> [https://perma.cc/6KSX-ECVG].

222. Adam Satariano, *London Police are Taking Surveillance to a Whole New Level*, N.Y. TIMES (Jan. 24, 2020), <https://www.nytimes.com/2020/01/24/business/london-police-facial-recognition.html> [https://perma.cc/J5PX-CKS3].

223. Shead, *Facial Recognition Tech*, *supra* note 48.

224. Facial Recognition and Biometric Tech. Moratorium Act of 2020, S. 4084, 116th Cong. (2019-2020); Pam Greenberg, *Facial Recognition Gaining Measured Acceptance*, NCSL (Sept. 18, 2020), <https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx> [https://perma.cc/E4AF-PQWR]; James Andrew Lewis, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*, CSIS (Sept. 29, 2021), <https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape> [https://perma.cc/8GBB-6ET5].

officers.²²⁵ Several cities have taken the issue of lack of federal regulation into their own hands and have banned or put a moratorium on the use of FRT; typically only banning its use by city agencies including police.²²⁶ The city of Portland, Oregon took a more drastic approach and banned the use of FRT in both private and government use.²²⁷ In 2020, the United States Congress attempted to pass legislation that would impose limits on the use of biometric surveillance systems by federal and state government entities, but the legislation failed to get past Senate introduction.²²⁸

The U.S. publicly acknowledged its widespread use of facial recognition technology in 2017.²²⁹ That year, President Trump signed an executive order to deploy FRT at U.S. airports²³⁰ and take data from both citizens and non-citizens.²³¹ The original order allowed citizens to opt out, but the United States Customs and Border Protections removed the opt-out possibility in 2019.²³² This change was said to be implemented for anti-terrorism purposes; by 2021, FRT will scan all people passing through the top twenty U.S. airports.²³³

Additionally, Clearview has also been used in the United States by at least fifty educational institutions.²³⁴

Beginning in 2019, the United States' Immigration and Customs Enforcement ("ICE") agency has used Clearview, a U.S.-based facial recognition company, for Homeland Security investigations, and enforcement and removal operations.²³⁵ Although it is unclear what exactly the agency is using the technology for, it is possible the technology was used in connection

225. Facial Recognition and Biometric Tech. Moratorium Act of 2020, S. 4084, 116th Cong. (2019-2020); Greenberg, *supra* note 224.

226. Shannon Flynn, *13 Cities Where Police are Banned from Using Facial Recognition Tech*, INNOVATION & TECH TODAY, <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/> [<https://perma.cc/W6Z6-NCMH>].

227. *Id.*

228. Facial Recognition and Biometric Tech. Moratorium Act of 2020, S. 4084, 116th Cong. (2019-2020); Greenberg, *supra* note 224.

229. Malkia Devich-Cyril, *Defund Facial Recognition*, THE ATLANTIC (July 5, 2020), <https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/> [<https://perma.cc/4PKT-RMXL>].

230. *Id.*

231. *Id.*

232. *Id.*

233. Exec. Order No. 13780 82 FR 13209 (Mar. 6, 2017); Davey Alba, *The US Government Will be Scanning Your Face At 20 Top Airports, Documents Show*, BUZZFEED NEWS (Mar. 11, 2019, 9:27 AM), <https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for> [<https://perma.cc/W6TL-EWRE>].

234. Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BUZZFEED NEWS (Feb. 27, 2020), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement> [<https://perma.cc/2MZ4-Z2BB>].

235. *Id.*

with the over 50,000 people detained and kept in poor conditions in immigration camps at the U.S. Mexico border.²³⁶ The agency has also used the technology to analyze drivers licenses of the drivers in at least three U.S. states without their permission.²³⁷

The United States Federal Bureau of Investigation (“FBI”) has long been using the technology, running over 390,000 searches to date.²³⁸ The FBI says the technology is used to “preserve [the] nation’s freedoms, ensure . . . liberties are protected, and preserve . . . security.”²³⁹ However, little is known about when the agency conducts searches, who is targeted by the searches, or the frequency of false positives.²⁴⁰

Since 2019, at least 600 law enforcement agencies in the U.S. have started using Clearview FRT, which is implemented through hidden cameras in uniforms.²⁴¹ This technology identifies individuals and “predict[s] emotional states and the likeliness a given individual might commit a crime.”²⁴² The United States first used emotion-reading surveillance technology in airports in 2006 in an attempt to find terrorists, but the technology was allegedly used for racial profiling as well.²⁴³

B. Implications of FRT Use as National Security Leaders

As leaders of the UN Security Council, these nations must “maintain international peace and security in accordance with the principles and purposes of the United Nations.”²⁴⁴ One of the four main purposes of the United Nations is to “promot[e] respect for human rights.” China, France, Russia, and the United Kingdom are all also members of the UN Human

236. Madeleine Joung, *What is Happening at Migrant Detention Centers? Here's What to Know*, TIME (July 12, 2019, 2:01 PM), <https://time.com/5623148/migrant-detention-centers-conditions/> [https://perma.cc/3RM7-ZS5W].

237. 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/6STV-EXJ8].

238. Rosenthal & Yan, *supra* note 71.

239. *Id.*

240. Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 12:54 PM), <https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/> [https://perma.cc/BK4X-94S9].

241. Hill, *The Secretive Company*, *supra* note 21.

242. Damiani, *supra* note 2.

243. Schwartz, *supra* note 43.

244. U.N. Security Council, Functions and Powers, <https://www.un.org/securitycouncil/content/functions-and-powers> [https://perma.cc/KA5B-86Z8].

Rights Council.²⁴⁵ Yet each nation has implemented FRT in ways that may violate an individual's basic assumption of privacy, which again, is a basic human right under international law. With the nations that hold leadership positions in the UN clearly using FRT, and likely using it in a way that violates a basic assumption of privacy, international law has been rendered meaningless.

C. Constitutional Provisions

The impact of constitutional privacy protections seems to depend on the courts working independence, as well as whether or not the nation has a privacy provision at all.

Both Russia and China characterize privacy as a fundamental constitutional right.²⁴⁶ However, due to the lack of judicial independence,²⁴⁷ FRT has largely remained unchecked, and the privacy of the nation's people is being violated.²⁴⁸ Russia's lack of adherence to its constitution could also be linked to its history of not adhering to its constitutional human rights promises.²⁴⁹

The United Kingdom and the United States both have tangential constitutional privacy rights. The UK provision, which has been implicated by courts, is the European Convention on Human Rights and was sufficient to render FRT use illegal in *Whales*.²⁵⁰ No known U.S. cases have challenged FRT specifically citing constitutional protections.²⁵¹

France is the only one of the five nations to have no constitutional right to privacy.²⁵² It seems that the nation has taken the quickest approach to implementation, going from no use of FRT to using FRT to establish facial IDs for residents in a matter of a few years.²⁵³ With no constitutional right to privacy, the nation has quickly been able to grow its FRT use to a

245. U.N. Human Rights Council, Current Membership of the Human Rights Council for the 15th Cycle (Jan. 1, 2021), <https://www.ohchr.org/EN/HRBodies/HRC/Pages/CurrentMembers.aspx> [<https://perma.cc/58CG-D34S>].

246. *See infra* Sections IV.A.1, IV.A.3.

247. *Russian Federation*, *supra* note 132; *IN THE NAME OF JUSTICE*, *supra* note 132.

248. *See infra* Sections II.A.1., II.A.3.

249. Arch Getty, *supra* note 138.

250. Iman Barr, *Police use of facial recognition technology infringes European Convention on Human Rights*, HUM. RTS. L. CTR. (Aug. 8, 2020), <https://www.hrlc.org.au/human-rights-case-summaries/2020/8/28/police-use-of-facial-recognition-technology-infringes-european-convention-on-human-rights> [<https://perma.cc/L9NM-GSZ8>].

251. Nathan Freed Wessler, *A Federal Court Sounds the Alarm on the Privacy Harms of Face Recognition Technology*, ACLU (Aug. 9, 2019), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/federal-court-sounds-alarm-privacy-harms-face> [<https://perma.cc/4U5Y-S9FS>].

252. *See infra* Section IV.A.

253. Fouquet, *supra* note 201.

level that rivals China. France is, however, bound to the European Convention on Human Rights, so this may be limiting to France's FRT growth in the future.

Comparing the constitutional right to privacy in these nations, it seems that having a constitutional right to privacy does not mean privacy rights will be protected, especially if an independent judiciary does not operationally function as an independent judiciary. Conversely, if a nation has no privacy rights listed, or weak rights, privacy violations can grow quickly when the opportunity arises and remain relatively unchecked due to the lack of constitutional teeth to prevent its use. Without required disclosure there is no way to know with certainty that this observation is accurate.

D. ICCPR and Privacy Implications of FRT

First turning to Article 17 of the ICCPR which grants freedom from "arbitrary or unlawful interference [of] . . . privacy,"²⁵⁴ the four ratifying nations have seemingly unlawfully interfered with privacy of their citizens by implementing FRT. As the only country that did not ratify the ICCPR, China is still obliged to "refrain, in good faith, from acts that would defeat the object and purpose of the treaty,"²⁵⁵ which seems incompatible with its extremely widespread use of FRT across the country in direct violation of its Constitution. If the definition provided in Comment 16²⁵⁶ is considered the definition of privacy in this analysis, it seems likely that all of the nations abused their power and violated Article 17. With no clear definition of the term "privacy," the issue becomes much more complex and more difficult to determine whether privacy is technically being violated.

In China, FRT is clearly being used arbitrarily to detain Uighurs and keep them in camps, in apparent contravention of Article 9.²⁵⁷ The excuse,

254. ICCPR, *supra* note 96, at art. 17.

255. *What is the Difference*, *supra* note 152; *China: Ratify Key International Human Rights Treaty*, HUM. RTS. WATCH (Oct. 28, 2020), <https://www.hrw.org/news/2013/10/08/china-ratify-key-international-human-rights-treaty> [<https://perma.cc/H6V9-WCEZ>].

256. See U.N. Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Apr. 8, 1988).

257. Lindsay Maizland, *China's Repression of Uyghurs in Xinjiang*, COUNCIL ON FOREIGN RELS. (Mar. 1, 2021 7:00 AM), <https://www.cfr.org/backgrounder/chinas-repression-uyghurs-xinjiang> [<https://perma.cc/H4G8-WPZ9>]; ICCPR, *supra* note 96, at art. 9.

again, is national security. The United States has also potentially violated Article 9 if ICE used FRT to detain and cage non-citizens.²⁵⁸

Finally, Article 12 is especially relevant to the ICCPR discussion as it restricts the rights in Article 17 and Article 9 if national security is claimed to be the justification for the action. Each of the Security Council members has excused their FRT use by citing national security. Although the Article 12 exceptions are extremely important considerations, the provisions of this Convention are weak in that almost any use of facial recognition technology can be justified through Article 12. Additionally, without the requirement to disclose the use of facial recognition technology, it is unclear if these countries are actually using the technology for a purpose justified under Article 12.

Article 2 of the ICCPR does not allow for the rights instilled by the ICCPR to be different based on gender, religion, and national origin, but by allowing nations' use of FRT to be justified under Article 12, the ICCPR aides in the disproportionate impact of FRT use on people of different religions, genders, and races.

Despite the many potential violations under the ICCPR, none of the five nations are likely to face any legal consequences because of Article 12's excuses for FRT use when claimed to be used for national security. Article 12 of the ICCPR provides a loophole for nations and is insufficient in protecting the fundamental right to privacy the ICCPR grants. The ICCPR does not protect the citizens of signatories, especially people of color, transgender, and non-binary individuals, but rather provides powerful nations with an excuse to intrude on the privacy of its people.

E. European Convention on Human Rights

As signatories, France, the UK, and Russia are all bound by the European Convention on Human Rights, but the treaty has only been enough to render FRT use illegal in part of one of the nations. With the UK ruling, however, there is the potential for this convention to render more FRT use illegal in the future.

F. European Union GDPR

France, as a member of the European Union,²⁵⁹ is bound by the GDPR, which provides protections against the collection of biometric data. The

258. Joung, *supra* note 236; ICCPR, *supra* note 96.

259. *Countries in the EU and EEA*, Gov.UK, <https://www.gov.uk/eu-eea#:~:text=The%20EU%20countries%20are%3A,%2C%20Slovenia%2C%20Spain%20and%20Sweden>.

nation's security watchdog entity, the CNIL, has reported that the nation's Alicem facial ID program potentially does not fall within the guidelines of the GDPR.²⁶⁰ Despite this and backlash from citizens, the nation has continued to roll out the program.²⁶¹ Like the ICCPR, this international regulation does not appear to be strong enough to prevent France's use of FRT for applications with negative privacy implications.

G. Company Self-Regulation Efforts and Third-Party Standards

With so little regulation and ethical guidance regarding FRT use, several FRT companies have turned to self-regulation.²⁶² In China, the company Megvii created a six-part guideline for FRT implementation including provisions highlighting the need for data security and privacy risk aversion.²⁶³ There is also an initiative from twenty-seven tech companies including SenseTime, Tencent, and Xiaomi to draft industry standards for FRT.²⁶⁴ While this is not binding, it does put pressure on lawmakers to create legally binding standards.

In the U.S., in June of 2020, Microsoft, Amazon, and IBM all put out statements regarding their use of FRT.²⁶⁵ The company IBM stated it would stop selling the technology altogether, but as for the other companies, these statements did not come without limitations.²⁶⁶ Amazon implemented a one-year moratorium on the use of their FRT by U.S. law enforcement to give Congress time to pass regulation.²⁶⁷ Microsoft instituted a moratorium on its FRT use until the issue was brought up in Congress.²⁶⁸ Despite Congressional efforts to pass legislation that would impose limits on the use of biometric surveillance systems by federal and state government entities, the legislation did not get past Senate introduction.²⁶⁹ Tech giant Google has in the past

260. See Fouquet, *supra* note 201.

261. Fouquet, *supra* note 201.

262. Browne, *supra* note 42.

263. Lee, *supra* note 167.

264. Lee, *supra* note 167.

265. Short Wave, *supra* note 17, at 0:09.

266. Short Wave, *supra* note 17, at 4:18.

267. Short Wave, *supra* note 17, at 4:25.

268. Brian Fung, *Tech Companies Push for Nationwide Facial Recognition Law. Now Comes the Hard Part*, CNN (June 13, 2020, 1:06 PM), <https://www.cnn.com/2020/06/13/tech/facial-recognition-policy/index.html> [https://perma.cc/GDK5-3NVS].

269. Facial Recognition and Biometric Tech. Moratorium Act of 2020, S. 4084, 116th Cong. (2019-2020); Greenberg, *supra* note 224; Lauren Feiner & Annie Palmer, *Rules Around Facial Recognition and Policing Remain Blurry*, CNBC (June 12, 2021),

stated their FRT would not be implemented for general purpose before the company “work[s] through important technology and policy questions.”²⁷⁰

Microsoft has also made a direct appeal specifically for international regulation of FRT in 2018.²⁷¹ The company called for corporate responsibility in maintaining ethics in FRT, specifically citing the UN’s Guiding Principles on Business and Human Rights as proposed guidelines.²⁷²

Some third-party organizations have created global non-binding standards, guidelines, and best practice manuals for FRT use.²⁷³ These groups include the International Biometrics and Identification Association, and the Institute of Electrical and Electronics Engineers.²⁷⁴

VI. PROPOSED AND POSSIBLE SOLUTIONS

In an ever evolving and technology reliant world, there is a fine line between new forms of technology like FRT being useful, and the technology leading to a new and intrusive reality. Improper use of FRT is, at the very least, problematic and ethically questionable. The technology has developed and evolved faster than it can be regulated both nationally and internationally.²⁷⁵ This would not be nearly as problematic if the technology operated as intended, but most FRT falls short due to algorithmic bias and lack of accuracy.²⁷⁶

The group of countries permanently tasked by the UN to maintain international security have all implemented, to some degree, facial recognition technology,²⁷⁷ each justifying their use of the tech with national security.²⁷⁸ By using the technology in troubling ways, these nations are adding a new category of activity that is justified because of national security. These five nations

<https://www.cnn.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html> [https://perma.cc/ZH72-EW7T].

270. Kent Walker, *AI for Social Good in Asia Pacific*, GOOGLE (Dec. 13, 2018), <https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/amp/> [https://perma.cc/WAA8-2AZX].

271. Brad Smith, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, MICROSOFT: MICROSOFT ON THE ISSUES (July 13, 2018), <https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/> [https://perma.cc/XU88-UK2A].

272. *Id.*; OHCHR and Business and Human Rights, OHCHR, <https://www.ohchr.org/EN/Issues/Business/Pages/BusinessIndex.aspx> [https://perma.cc/VCK9-GM34].

273. Facial Recognition and Biometric Tech. Moratorium Act of 2020, S. 4084, 116th Cong. (2019-2020); Greenberg, *supra* note 224.

274. Greenberg, *supra* note 224.

275. Greenberg, *supra* note 224.

276. Greenberg, *supra* note 224.

277. *See supra* Section V.A.

278. *Supra* Section V.A.

are tasked with maintaining international security under the UN Charter, but at what cost?

The current national and international laws are not enough to deter any of the nations from using facial recognition technology in ways that infringe upon privacy rights. These issues are exacerbated for people of color, women, transgender individuals, and those who do not present gender according to binary norms.²⁷⁹ To ensure the privacy rights of all individuals are adequately protected, more must be done to correct this growing invasion of human rights.

The benefits of this technology are important to consider in the search for solutions. There is a delicate balance to be found between the positive uses of the technology and its harmful privacy violations. However, it is important not to drastically chill technological innovation in this field due to its likely growing list of beneficial uses, but restrictions and standards must be in place for the benefits to outweigh the harms.

A. National FRT Regulation

One solution is for all nations to regulate FRT, to some degree, on a national level. Technology has outgrown constitutional protections and law in all five nations discussed above and must be met with strict requirements to ensure privacy protections and to uphold human rights for all individuals. The national regulation recommendations discussed below are for the United States specifically but are generally applicable to all five nations considered here, as well as many other nations. As the United States Constitution does not explicitly protect privacy, passing legislation specifically regarding FRT would allow suits against unjust FRT uses to prevail.

It would be very symbolic for the United States to pass strict FRT regulation in the beginning of Joe Biden's Presidency. It would show the world that his administration is serious about re-entering the world stage and protecting human rights after Trump withdrew from international relationships and the UN Human Rights Council and conducted several human rights atrocities during his term in office.²⁸⁰

279. See Libération, *supra* note 199; see also Damiani, *supra* note 2.

280. See, e.g., *United States of America 2019*, AMNESTY INT'L, <https://www.amnesty.org/en/countries/americas/united-states-of-america/report-united-states-of-america/> [<https://perma.cc/38D8-7XR6>].

1. *Moratorium, Not a Ban*

The first step in regulating FRT is to create a national moratorium on FRT use by government agencies, or police agencies at a minimum. The widespread and potentially large bias in the technology has too high of a potential to create discrimination and disparate impacts to allow its use to continue unregulated. The technology has continued to evolve,²⁸¹ and will continue to do so in ways that may create further problems for equity in the technology, so the passing of a moratorium must be swift. A moratorium should be put in place until strict regulation is passed which takes extra precaution to ensure that all individuals are equitably protected from the technology.

Several organizations have called for a ban on the use of FRT,²⁸² but this is likely not a feasible solution, nor is it the best solution for ensuring marginalized communities are adequately protected. If a moratorium and development of regulations are done correctly and quickly, the benefits of the technology make the moratorium worthwhile.

It is difficult if not impossible to completely walk back on the current FRT reliance and go “from an increasingly nymous to an anonymous society.”²⁸³ The technology has already been implemented and, while shown to be beneficial, has invaded the privacy rights of millions of individuals. At this point both nations and companies have invested money, and the market for the technology is there. If a ban were imposed, there is the potential for a black-market demand for FRT which would mean less oversight and regulation than before. A black-market for FRT has already been exposed in Russia even without a ban on FRT use.²⁸⁴

A ban is also not the best solution to protect marginalized communities in the U.S. because of the recent rise in violence from white supremacist extremists, which the Department of Homeland Security has labeled as

281. See, e.g., Damiani, *supra* note 2.

282. See e.g., *Stop Facial Recognition*, BIG BROTHER WATCH, <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/> [https://perma.cc/733E-YXYS]; see e.g., Foo Yun Chee, *EU Privacy Watchdogs Call for Ban on Facial Recognition in Public Spaces*, REUTERS (June 21, 2021), <https://www.reuters.com/technology/eu-privacy-watchdogs-call-ban-facial-recognition-public-spaces-2021-06-21/> [https://perma.cc/4XSC-5SMJ]; see e.g., Press Release, Amnesty International, *Ban Dangerous Facial Recognition Technology that Amplifies Racist Policing* (Jan. 26, 2021, 8:22 AM), <https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/>.

283. See Turley, *supra* note 97, at 2245.

284. See *For Sale: Access to Moscow's CCTV Network on Black Market*, THE MOSCOW TIMES (Dec. 6, 2019), <https://www.themoscowtimes.com/2019/12/06/access-moscows-cctv-network-facial-recognition-black-market-a68506> [https://perma.cc/PM6D-8R5V].

“the most persistent and lethal threat in the Homeland.”²⁸⁵ White supremacists “have demonstrated longstanding intent to target racial . . . minorities, [and] members of the LGBTQ+ community.”²⁸⁶ The technology is essential in identifying culprits of these heinous crimes and reversing the rise of white supremacy and extremism. The large and growing threat to these communities highlights the need for FRT regulation to happen as quickly as possible.

While a moratorium is necessary, there may be some circumstances where exceptions to the moratorium should be upheld, as in the case of protecting against terrorism. This terrorism exception is necessary with the enhanced risk of domestic terrorism the U.S. faces. The technology was used to identify the white supremacists who attacked the U.S. capital on January 6th, 2021,²⁸⁷ and this type of FRT use would not be possible without a terrorism exception to the moratorium.

The technology should not, however, be used for immigration purposes or by police forces for standard crimes. This exception would not be a general national security exception. There would need to be a requirement of researched and justified risk from the threat; the harm to the public must be balanced with the harm to human rights.

2. Regulatory Requirements

To ensure the regulation adequately addresses the privacy and equity concerns arising from FRT, the regulation must be strict and specific. One of the most crucial aspects of the regulation is the need for accuracy standards. These accuracy standards must be extraordinarily high and must be specifically tested against all races, ethnicities, and gender presentations to ensure equality in FRT use.

Regulation must ensure that algorithm data is significantly diversified by race, ethnicity, and gender to allow for the accuracy to increase and so the chance of false matches and misidentifications would further be decreased. These protections are essential to maintaining human rights and protecting all individuals under the law.

285. U.S. DEP'T HOMELAND SEC., HOMELAND THREAT ASSESSMENT, 18 (Oct. 2020), https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf [<https://perma.cc/URC2-RRNB>].

286. *Id.*

287. Hill, *The Facial-Recognition App*, *supra* note 56.

Regulation must also ensure the biometric data captured by FRT use is adequately secured. Data breach has been an issue for the United States in recent years,²⁸⁸ so the government must take greater action to ensure biometric data is protected.

Once the regulation ensures that the technology itself is accurate, unbiased, and secure, the regulation must provide that the technology is equitably distributed into cities so as not to add to the over policing of communities.²⁸⁹

While a very high accuracy standard is necessary, there is still a risk of false matches, so regulation would need to include a requirement of human analysis before government agencies can contact an individual based on FRT matching. This would further decrease the chance of agency interaction with falsely identified individuals.

FRT regulation must include additional requirements for commercial one-to-one matching including consent and alternatives for those who do not consent to the technology's use. A consent requirement is not feasible in one-to-many identification because the technology would not be able to serve its basic function of surveilling, but in one-to-one matching, consent is essential in ensuring equity. To ensure people are not disproportionately impacted by FRT because of their race, gender, or gender presentation, alternative options must be in place when FRT is used for access such as entrance into gendered restrooms.

To ensure that FRT implemented after regulation is passed meets the stringent requirements of the regulation, an independent third-party organization must be established. This group would be tasked with rigorously testing FRT being used and how the FRT has been implemented. Agencies using FRT must be required to disclose their use of FRT to the third-party group to ensure the technology is accurate, secure, and unbiased. Without disclosure of FRT use, concerns related to human rights violations that the tech may cause cannot be adequately addressed.

If the U.S. implemented strict regulation with the specificities discussed above, companies would need to produce accurate, unbiased, and secure FRT to sell in the U.S. Many companies, including Clearview which is selling

288. See, e.g., David E. Sanger, *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES (Dec. 13, 2020), <https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html> [https://perma.cc/WL6Q-C4YB].

289. See, e.g., West Baltimore Commission on Police Misconduct and the No Boundaries Coalition, *Over-Policed, Yet Underserved: The People's Findings Regarding Police Misconduct in West Baltimore*, NO BOUNDARIES COALITION, <http://www.noboundariescoalition.com/wp-content/uploads/2016/03/No-Boundaries-Layout-Web-1.pdf> [https://perma.cc/XWH8-Y8JS].

to many countries,²⁹⁰ would be likely to improve the technology they are selling to all nations after improving the technology they are selling to the U.S. so as to improve their competitive advantage amongst FRT competitors. If multiple nations imposed strict regulation and standards for FRT, companies would have no choice but to up their technology so to remain competitive in these markets.

B. International FRT Regulation

National regulation is a necessary step in protecting against harm from FRT, but the international scale of this technology renders regulation by one nation alone insufficient; the international expansion of FRT necessitates an international solution. While FRT would be bettered by several nations instituting accuracy standards, to effectively prevent privacy violations caused by FRT use for all individuals across all nations there must be global and uniform regulation. While global regulation might be difficult to achieve, it is clear that more must be done on an international scale.

Current international law is not sufficient to protect all people from facial recognition technology. EU protections in the European Convention on Human rights have been effective to some extent in the UK,²⁹¹ but the extent of its reach is questionable, and it has not rendered FRT use illegal in either France or Russia. The ICCPR and GDPR have proven to not have sufficient teeth to prevent misuse of FRT and provide protection on the basis of race and gender presentation.

It has been suggested that a new comment for Article 17 of the ICCPR with definitions of terms including more specificity for biometric data is all that is necessary to protect against FRT,²⁹² but this is not so. A new comment and new definitions could help guide nations on what privacy should be protected, but there are two fatal flaws with this suggestion: (1) a comment is not binding,²⁹³ and (2) Article 12 still allows for the use of FRT for national security.

The best solution may be for the United States to initiate an international treaty or Security Council Resolution with a moratorium and similar regulation as recommended above for individual nations. In doing so, the

290. Shead, *Facial Recognition Tech*, *supra* note 48.

291. Bridges, *R v. South Wales Police* [2020] EWCA (Civ) 1058, [201] (appeal taken from Eng.) (UK).

292. *Privacy Rights in the Digital Age*, *supra* note 95, at 16, 31.

293. *Id.* at 7.

United States should call to action the other four permanent members of the Security Council in an effort to garner support as national security leaders.

If regulation of FRT usage is instituted, the regulation would need to be extremely strict, much like the national regulation suggested above. An effective international agreement would need to be very specific and contain no provisions justifying the technology's use for any purpose outside of the outlined scope, including national security. Additionally, the agreement would need to take extra precaution in ensuring equity and protecting individuals on the basis of race and gender.

Like state regulation, international regulation would need to include accuracy standards; these must be globally uniform to protect against its potential for human rights violations. Without a global accuracy standard there is no accountability for the level of bias in the technology being used, which could lead to even greater privacy violations and concerns. The bias in the technology must be minimized to the greatest extent possible so as not to further exclusion and oppression of marginalized populations. Global accuracy standards would increase competition among FRT companies, driving up need for accuracy and bias free technology even further.

With global accuracy standards comes global biometric data sharing. Global data sharing is essential for increasing FRT accuracy. Diversity in facial images used to train FRT algorithms is how the technology becomes less biased.²⁹⁴ This data sharing could be problematic though if the regulation is not sufficient to ensure the biometric data is obtained humanely. However, the harm from unethical data gathering may be less than the harm from inaccurate and biased FRT in use.

There would also need to be a third-party independent body in charge of enforcement and acting as an umpire. This body would be needed to test the accuracy of FRT, ensure it is being used according to the regulation, and that any exception to the regulation is interpreted in the favor of human rights. Disclosure of FRT usage and implementation to the third-party group would also need to be required by the agreement to ensure enforcement is possible and any violations would be observable and thus subject to sanction. If disclosure of use was not required, privacy violations could continue and go unpunished.

By proposing a short moratorium and regulation instead of a complete ban on use, the international support may be increased. It would still be very difficult to gain the support of the other members of the Security Council though, as they are all using the technology. A moratorium may also be difficult to enforce with the use of the technology shrouded in secrecy and

294. See Schwartz, *supra* note 43.

used to gain a competitive advantage on bad actors from different nations. The strictness of the regulation may also prevent nations from being willing to sign on or ratify regulation.

Additionally, international agreements may not hold the same weight as they used to with shifting political climates in some of the major global political players. The U.S.²⁹⁵ and UK²⁹⁶ have both pulled out of international treaties and agreements in recent years, with the UK leaving the EU and the U.S. leaving various international treaties under the Trump administration.²⁹⁷ Although United States' President Joe Biden has stated he will rejoin international agreements during his presidency and has already begun doing so,²⁹⁸ the previous Trump administration has cast a spotlight on the fragility of international agreements when a powerful country leaves or does not comply.

While an international moratorium and subsequent regulation is the ideal solution, it does not seem likely this solution is feasible. There is still, however, one potential solution to achieve the goal of equitable FRT use.

C. The Role of Companies

In recent years, private companies, specifically technology companies, have been gaining autonomy in the sociopolitical sphere. Companies are no longer just businesses, but rather social entities closely tied to national politics.²⁹⁹ When large and divisive events occur, companies are now expected to take a stand, and failure to do so may put a company in bad

295. Zachary B. Wolf, *Here are All the Treaties and Agreements Trump has Abandoned*, CNN (Feb. 1, 2019, 11:50 AM), <https://www.cnn.com/2019/02/01/politics/nuclear-treaty-trump/index.html> [<https://perma.cc/UT9G-FB8D>].

296. *Guidance Living in Europe*, GOV.UK (last visited Sept. 9, 2021), <https://www.gov.uk/guidance/living-in-europe>.

297. See Wolf, *supra* note 295.

298. Lindsay Maizland, *Biden's First Foreign Policy Move: Reentering International Agreements*, COUNCIL ON FOREIGN RELATIONS (Jan. 21, 2021), <https://www.cfr.org/in-brief/bidens-first-foreign-policy-move-reentering-international-agreements> [<https://perma.cc/E3W6-8TN7>].

299. See Tiffany Hsu, *Corporate Voices Get Behind 'Black Lives Matter' Cause*, N.Y. TIMES, <https://www.nytimes.com/2020/05/31/business/media/companies-marketing-black-lives-matter-george-floyd.html> [<https://perma.cc/56MA-4ULK>]; see also Tiffany Hsu & Davey Alba, *Meta Makes Changes to Marketing Strategy Amid Scandals*, N.Y. TIMES (Nov. 2, 2021), <https://www.nytimes.com/2021/11/02/business/media/meta-ad-strategy-facebook-scandal.html> [<https://perma.cc/R5C2-DS7L>].

light.³⁰⁰ Companies have been called on to take action and advocate for human rights when the government cannot or will not.³⁰¹

Although international law is not binding to companies specifically, FRT companies across the globe must work together to create ethical guidelines for FRT and promote human rights when nations cannot or will not. Companies must take responsibility for their impact on human rights violations.

Some FRT companies have already called for regulation and actively want more regulation.³⁰² Businesses have begun self-regulating the uses of their technology and who or what agencies can use the technology,³⁰³ but global cohesive action is necessary. Business morality should not place companies at a competitive disadvantage. If FRT continues on unregulated, it may develop to a point where it is far too dangerous to be implemented and a ban may be necessary.

If public outcry grows regarding FRT use, businesses who have not already suggested regulation will have no choice but to change course in their implementation and increase awareness of where and how the tech is used. While government and international regulation is necessary, consumers and concerned citizens can also drive change. The motive for a company to change course need not be internal. If enough public pressure is mounted, companies may voluntarily impose self-regulation and increase transparency.

VII. CONCLUSION

Facial recognition technology has been developed for the betterment of society, but without proper regulation of the technology, there has been and will continue to be grave consequences for the privacy of all individuals. The populations most vulnerable to oppression are subject to greater risk of this privacy intrusion and thus must have greater protections. A moratorium

300. This became evident during the 2020 Black Lives Matter protests. Companies and businesses who did not voice support for the social justice and civil rights movement were looked down upon. *Id.*

301. CEOs of social media companies were called on to block Donald Trump from Twitter and other platforms after continuing to incite violence on the platforms after the January 6, 2021 attack on the United States Capitol. *See e.g.*, Kate Conger et. al., *Twitter and Facebook Lock Trump's Accounts After Violence on Capitol Hill*, N.Y. TIMES (Jan. 6, 2021), <https://www.nytimes.com/2021/01/06/technology/capitol-twitter-facebook-trump.html> [<https://perma.cc/GQC3-NM28>].

302. *See e.g.*, Jeffrey Dastin, *Amazon Extends Moratorium on Police use of Facial Recognition Software*, REUTERS (May 18, 2021), <https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/> [<https://perma.cc/MD9K-TGUX>].

303. *See infra* Section V.G.

and regulation are necessary to ensure this technology does not completely eliminate any existing right to privacy.

The rights of all individuals, regardless of race or gender, must be protected from unlawful and unreasonable intrusion into individual privacy. More must be done to protect all individuals against facial recognition technology.

