PULLING BACK THE VEIL: EXPOSING PERNICIOUS USES OF FACIAL RECOGNITION TECHNOLOGY

INTRODUCTION

Facial recognition is nothing new. Technology giants have been developing and implementing facial recognition for years; our iPhone lock mechanisms are proof of that. The potential uses for facial recognition are limitless and many companies already wield the capability to create powerful tools. Several countries, enticed by the promise of such tools, have jumped at the opportunity to use facial recognition to bolster policing and security forces. The Chinese government serves as a primary example.[1] However, even in the United States, private companies have sold novel artificial intelligence ("AI") technologies to law enforcement agencies who have leveraged them to surveil a largely unsuspecting American public.[2]

The primary blockade for such companies in implementing their technology is privacy. Several facial recognition-based software companies are currently under legal fire for privacy violations.[3] In many of these cases, courts have legitimized privacy concerns by

1 Yaron Steinbuch, *Chinese city rolls out facial-recognition thermometers on buses to combat coronavirus*, NEW YORK POST (Feb.19, 2020), https://blog.homeip.net/2020/02/19/chinese-city-rolls-out-facial-recognition-thermometers-on-buses-to-combat-coronavirus/.

2 Jon Schuppe, *How facial recognition became a routine policing tool in America: The technology is proliferating amid concerns that it is prone to errors and allows the government to expand surveillance without much oversight*, NBC NEWS (May 11, 2019), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251.

3 Rachel Metz, *Clearview AI sued in California by immigrant rights groups, activists,* CNN BUS. (Mar. 9, 2021), https://www.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html; J.Jon Fingas, *Google settles Photos facial recognition lawsuit for $100 million,* ENGADGET (June 6, 2022) https://www.engadget.com/google-photos-bipa-lawsuit-settlement-161237789.html.

refusing to grant dismissal actions.[4] This year, Apple announced that it will begin scanning personal photo libraries on Apple devices to crack down on child abuse and pornography.[5] Both domestic and international digital rights groups have raised concerns about shrinking privacy rights and the general public's lack of control on the matter. For a company like Apple that has distinguished itself with a platform tailored to keep personal information private, a decision to roll-out an invasive security feature without an opt-out option is bold.[6] This move comes with a tradeoff. Customers must now choose between the peace of mind that their data is for their eyes only (and whoever they choose to share it with) and the very different peace of mind that minors and other vulnerable technology users are protected against bad actors. This note attempts to answer some of the questions that executives at Apple likely mulled over. What is possible with facial recognition? What are the privacy concerns of the general public? What *should* society's privacy concerns be? Most importantly, how much autonomy are consumers willing to sacrifice in the name of safety and security, efficiency, and a heightened e-commerce experience?

This analysis, broken down into three parts, uncovers a broad lack of public awareness about the ways both governmental and private entities are utilizing facial recognition scans and how such uses may change current conceptions of privacy. Following a brief introduction, Section II discusses various governmental uses of facial recognition technology ("FRT"). This second section primarily focuses on China, where a rapidly developing national surveillance system leveraging FRT aims to combat universal evils like crime and terrorism. Section III explores how global corporations have leveraged facial recognition and AI. Although this paper attempts to segment uses of FRT into separate public and private spheres, such distinctions are not

4 Jeffrey D. Neuburger, *Court Refuses to Dismiss Biometric Privacy Action over Facial recognition Technology Used by Google Photos*, THE NATIONAL LAW REVIEW (Mar. 2, 2017), https://www.natlawreview.com/article/court-refuses-to-dismiss-biometric-privacy-action-over-facial-recognition-technology.

5 Zack Whittaker, *Apple confirms it will begin scanning iCloud Photos for child abuse images*, TECHCRUNCH (Aug. 5, 2021), https://techcrunch.com/2021/08/05/apple-icloud-photos-scanning/.

6 *Id*.

easily drawn. When it comes to FRT, governmental entities and boundary-pushing technology companies feed off each other in a demand and supply market that, without third party intervention, loses sight of pressing privacy issues. Section IV identifies key issues derived from the various case studies in Sections II and III, examines existing privacy regulation frameworks, and attempts to construct a broad, principle-guided regulatory framework specific to FRT.

Ultimately, I argue that corporations and law enforcement agencies distract consumers and citizens with convenient, new products and security mechanisms that promise to ward off crime and terrorism. The problem with these distractions is not that they are not commendable pursuits, but that such pursuits often mask the true intentions and future consequences of FRT utilization, robbing the public of a meaningful voice in the privacy discussion. Building an effective regulatory framework begins with pulling back the veils of consumer benefits and heightened security. Targeted pushes for transparency and accountability ultimately require a level of public awareness that does not yet exist. Rather than proposing technical country-specific solutions, this analysis serves as a primer on the privacy issues posed by the global advancement of FRT and the broad ways of addressing them. My hope is that this paper will spur young and seasoned academics, attorneys, scholars, and other privacy advocates to think deeply about these issues and imagine viable solutions that fit the needs and societal norms of their respective locales.

I. GOVERNMENTAL USES OF FRT: CHINA & INDIA CASE STUDIES

By the end of 2022, economists have estimated that the global market for facial technology will surpass seven billion dollars.[7] A very large portion of that market comes from a growing list of countries interested in bolstering existing security mechanisms or

7 Sintia Radu, *The Technology That's Turning Heads: From a store in Portland to a high school in Hangzhou, the use of facial recognition technology is becoming widespread in countries*, US NEWS (Jul. 26, 2019), https://www.usnews.com/news/best-countries/articles/2019-07-26/growing-number-of-countries-employing-facial-recognition-technology.

building new ones altogether. China is a primary developer and supplier of facial recognition technology. In 2019, Freedom House published a report that found that eighteen countries spanning multiple continents have purchased Chinese FRT.[8] Attached with these purchases is a training program for government officials on how to "better watch their own people."[9] Although nation-state customers are free to use the technology how they see fit, China's national surveillance framework has undoubtedly provided inspiration for other nation states. With an estimated 200 million security cameras (all of which are now equipped with FRT), China accounts for the largest share of installed security cameras globally.[10] The United States is second in terms of the overall number of cameras, but when population differences are accounted for, both countries have roughly one security camera for every four citizens.[11]

In recent years, the Chinese government has made artificial intelligence development a focal point. The country's "National AI Team" consists of government-selected technology companies who are granted special access to public databases and repositories.[12] This public-private partnership aims to streamline innovation and harness new technologies for predetermined government-minded goals.[13]

---

8 *Id.*

9 *Id.*

10 Coco Feng, *China the most surveilled nation? The US has the largest number of CCTV cameras per capita*, SOUTH CHINA MORNING POST (Dec. 9, 2019), https://www.scmp.com/tech/gear/article/3040974/china-most-surveilled-nation-us-has-largest-number-cctv-cameras-capita; Paul Bischoff, *Surveillance camera statistics: which cities have the most CCTV cameras?* COMPARITECH (last updated July 11, 2022Jul. 11, 2022), https://www.comparitech.com/studies/surveillance-studies/the-worlds-most-surveilled-cities/.

11 Thomas Ricker, *The US, like China, has about one surveillance camera for every four people, says report; One billion cameras will be installed globally by 2021, says IHS Markit*, THE VERGE (Dec. 09, 2019), https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens.

12 Benjamin Larsen, *Drafting China's National AI Team for Governance: Companies get special roles, but they're expected to serve as platforms for others*, NEW AMERICA (Nov. 18, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/drafting-chinas-national-ai-team-governance/.

13 *Id*.

Each company is designated a specific sector and is meant to work with the public office for that sector.[14] For example, iFlytek cooperates with courts to create a more efficient case-handling system.[15] Other companies work with China's education department to incorporate AI in school curricula.[16] SenseTime, a large AI company, handles the collection of data from China's CCTV surveillance cameras.[17] In 2018, the company provided Chinese police forces with high-powered glasses equipped with FRT that connects to China's state criminal database, allowing police officers to identify potential suspects in real time.[18]

At face-value the use of FRT in policing seems laudable,[19] but human rights advocates and academics have expressed concerns about the specific ways the Chinese government has utilized the technology. In 2019, FRT was trained by government officials to identify individuals of Uighur descent, a largely Muslim minority group primarily located in the western Xinjian region, purely based

14 *Id*.
15 *Id*.
16 *Id*.
17 *Id*.
18 Jon Russell, *Chinese Police are Using Smart Glasses to Identify Potential Suspects,* TECHCRUNCH (Feb. 8 2018), https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/.
19 Steve Lasky, *Unique web-based facial recognition tool enhances security and fights crime: Clearview AI facial search engine brings more than 20 billion facial images to its software solution enabling law enforcement and federal agencies to investigate suspects*, SECURITY INFO WATCH (Mar. 23, 2022), https://www.securityinfowatch.com/access-identity/biometrics/facial-recognition-solutions/article/21261325/unique-webbased-facial-recognition-tool-enhances-security-and-fights-crime.; Monica Rewutzer, *The use of facial recognition to fight crime: Japan case*, GEOSPATIAL WORLD (Jan. 01, 2021), https://www.geospatialworld.net/blogs/the-use-of-facial-recognitiorin-to-fight-crime-japan-case/.; Jenny Rees, *'Let police fight crime with facial recognition' plea*, BBC NEWS (Jan. 05, 2021), https://www.bbc.com/news/uk-wales-55369387.

on physical attributes.[20] China sparked wide international condemnation when law enforcement officials, in a self-proclaimed fight against threats of terrorism, imprisoned hundreds of thousands of Uighur nationals and were accused of destroying mosques in an effort to suppress the religious group.[21] Allegations of forced hard labor, forced sterilizations, and overall mistreatment resulted in increased criticism of China's use of FRT in furthering what some world leaders have called a genocide.[22]

Clare Garvie of Georgetown Law's Center of Privacy and Technology has said, "if you can make a technology that can classify people by ethnicity then people will use it to repress that ethnicity."[23] Many regulators in other developed nations share Garvie's view. Article 9 of the EU's General Data Protection Regulation (GDPR) specifically bans the collection of data that identifies subjects through biometric data or data based on ethnicity, race, sexual-orientation, political opinions, philosophical beliefs, trade union membership, or religion without clear and explicit consent.[24] In the United States, the state of Illinois recently passed the Biometric Information Privacy Act ("BIPA") with similar goals and concerns in mind.[25] Both Texas and

---

20 Raymond Zhong, *As China Tracked Muslims, Alibaba Showed Customers How They Could, Too: The website for the tech titan's cloud business described facial recognition software that could detect members of a minority group whose persecution has drawn international condemnation*, THE NEW YORK TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/12/16/technology/alibaba-china-facial-recognition-uighurs.html.

21 WION Web Team, *Mosques disappear as China strives to 'build beautiful Xinjiang'*, WION NEWS (May 14, 2021), https://www.wionews.com/world/mosques-disappear-as-china-strives-to-build-beautiful-xinjiang-384889.

22 BBC News, *Who are the Uyghuyrs and why is China being accused of a genocide?* BBC NEWS (June 21, 2021), https://www.bbc.com/news/world-asia-china-22278037.

23 Niraj Chokshi, *Facial Recognition's Many Controversies, From Stadium Surveillance to Racist Software*, THE NEW YORK TIMES (May 15, 2019), https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html.

24 GDPR Article 9 Council Regulation 2016/679, 2016 O.J. (L 199) 1.

25 740 ILL. COMP. STAT. 14/15 (2008).

Washington followed suit soon after with their own laws restricting biometric data collection.[26]

FRT's propensity for misidentification compounds growing concerns. Independent studies from the National Institute of Standards and Technology and the Gender Shades Project highlighted FRT's propensity for misidentification of certain demographics.[27] For instance, Amazon's patented Rekognition system demonstrated a tendency to misidentify women with darker-skin (31% error in biological sex classification).[28] Apple faced backlash when reports surfaced that its facial recognition screen-locking mechanism could not differentiate between eastern Asian faces as well as other demographics, resulting in weaker security for those individuals.[29] Chinese CCTV footage is often affected by weather and lighting conditions. Furthermore, China's AI relies on input of police officers to "teach" the system how to categorize humans based on "social definitions of ethnicity."[30] Human input inherently introduces the

---

26 Wash. Rev. Code Ann. § 19.375.020 (2022); TEX. BUS. & COM. CODE ANN. § 503.001 (2017).

27 Emily Kwong, *Why Tech Companies Are Limiting Police Use of Facial Recognition*, NPR (Feb. 18. 2021), https://www.npr.org/2021/02/17/968710172/why-tech-companies-are-limiting-police-use-of-facial-recognition.

28 James Vincent, *Gender and racial bias found in Amazon's facial recognition technology (again); Research shows that Amazon's tech has a harder time identifying gender in darker-skinned and female faces*, THE VERGE (Jan. 25, 2019), https://www.theverge.com/2019/1/25/18197137/amazon-rekognition-facial-recognition-bias-race-gender.

29 Guy Birchall, *Is the iPhone Racist? Chinese users claim iPhoneX face recognition can't tell them apart* THE SUN (Dec. 21, 2017), https://www.thesun.co.uk/news/5182512/chinese-users-claim-iphonex-face-recognition-cant-tell-them-apart/; Sophie Curtis, *iPhone X racism row: Apple's Face ID fails to distinguish between Chinese Users*. MIRROR (Dec. 22, 2017), https://www.mirror.co.uk/tech/apple-accused-racism-after-face-11735152.

30 Paul Mozur, *One Month 500,000 Face Scans: How China is Using A.I. to Profile a Minority; In a major ethical leap for the tech world, Chinese-start-ups have built algorithms that the government uses to track members of a largely Muslim minority group,* THE NEW YORK TIMES (April 14, 2019), (https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

possibility of bias, which is particularly problematic in policing systems accused of racial bias or prejudice.

In 2016 Detroit, Michigan orchestrated a large-scale surveillance program called Project Green Light (PGL).[31] High-definition cameras, equipped with FRT, were installed throughout the metropolitan area and were linked to Detroit Police Department criminal databases. PGL cameras were distributed more heavily in majority-black neighborhoods.[32] A closer look at PGL's regulation provisions revealed a vague public notification policy stating that the public "may or may not" be notified, and that only one individual is devoted to addressing bias related-complaints.[33]

In August of 2020, NYPD attempted to arrest a Black Lives Matter protest leader who was identified through facial recognition scrapes from CCTV camera footage and social media accounts.[34] Amnesty International, the New York Civil Liberties Union, and many other human-rights and privacy-minded organizations have taken the stance that the NYPD's use of facial recognition places New Yorkers in a "perpetual line-up" when they are in public.[35] Representatives from Amnesty International have taken a more direct stance, asking for a complete ban of the municipality's use of facial recognition for law enforcement purposes, stating that "facial recognition risks being weaponized by law enforcement against marginalized communities

---

31 Jacob Yesh-Brochstein, *A Critical Summary of Detroit's Project Green Light and Its Greater Context*, DETROIT COMMUNITY TECHNOLOGY PROJECT (June 9, 2019), https://detroitcommunitytech.org/system/tdf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force=.

32 *Id*.

33 *Id*. at 8.

34 Liam Stack, *N.Y.P.D. Besieges a Protest Leader as He Broadcasts Live; A helicopter and dozens of officers, some in tactical gear, were deployed for an arrest at a Manhattan apartment but withdrew after protesters arrived*, THE NEW YORK TIMES (Aug. 07, 2020) https://www.nytimes.com/2020/08/07/nyregion/nypd-derrick-ingram-protester.html.

35 Matt Mahmoudi, *Ban dangerous facial recognition technology that amplifies racist policing*. AMNESTY INTERNATIONAL (Jan. 26, 2021) https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

around the world. From New Delhi to New York, this invasive technology turns our identities against us and undermines human rights."[36]

New York is not a standalone case. Many municipal and state law enforcement agencies have begun utilizing FRT, and allegations of racial profiling and prejudicial policing continue to arise throughout the country.[37] However, some U.S. cities, including Portland, Boston, Oakland, Berkeley, and San Francisco, have taken a strong position against FRT by banning its use by police entirely.[38] Despite being located in one of the first states to experiment with law enforcement use of FRT, Portland passed the most stringent U.S. ban on FRT in 2020.[39] The Portland law bans both private and governmental uses of FRT.[40]

In multiple countries, governmental uses of FRT have expanded beyond security. A high school in Hangzhou implements an FRT that

---

36 *Id.*

37 Kate Cox, *Cops in Miami, NYC arrest protestors from facial recognition matches,* ARS TECHNICAL BLOG (Aug. 08, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/.; Mike Holden, *Pittsburgh police used facial recognition technology during Black Lives Matter protest*. WPXI-TV (May 21, 2021), https://www.wpxi.com/news/top-stories/pittsburgh-police-used-facial-recognition-technology-during-black-lives-matter-protests/VT52MGWM3VCDJINJSZPOO5NHKU/; Drew Harwell, *Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?* THE WASHINGTON POST (Apr. 30, 2019), https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/.

38 Taylor Hatmaker, *Portland passes expansive city ban on facial recognition tech*, TECHCRUNCH+ (Sept. 09, 2020), https://techcrunch.com/2020/09/09/facial-recognition-ban-portland-oregon/.

39 Rachel Metz, *Portland passes broadest facial recognition ban in the US*, CNN BUSINESS (Sept. 10, 2020) https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

40 *Id*.

scans students' faces every thirty seconds.[41] The scans check students' emotional status and physical actions, including reading, writing, raising a hand, and sleeping.[42] Some schools cited the technology's efficiency in taking class attendance,[43] a typically short and non-intensive task. Seemingly following the wave of increased surveillance in eastern Asian countries, India's capital city, Delhi, installed CCTV cameras in all government schools in 2018.[44] In 2021, schools began adding FRT capabilities to their CCTV systems.[45] Delhi Chief Minister Arvind Kejriwal cited security and transparency as the primary reasons behind the decision.[46] However, privacy experts have expressed special concern because the new systems

41 Johnny Lieu, *Eyes to the front camera: Chinese facial recognition tech targets inattentive students*, MASHABLE (May 18, 2018), https://mashable.com/article/chinese-facial-recognition-class.

42 The FRT categorized emotional states into five categories: happy, angry, fearful, confused, and upset. Tara Francis Chan, *A School in China is monitoring students with facial-recognition technology that scans the classroom every 30 seconds,* BUSINESS INSIDER (May 20, 2018), https://www.businessinsider.com/china-school-facial-recognition-technology-2018-5#:~:text=1%20A%20Chinese%20high%20school%20in%20Hangzhou%20is,being%20used%20to%20predict%20crime.%20More%20items...%20.

43 *Id*.

44 Gaurav Vivek Bhatnagar, *Pandora's Box of Privacy Issues': Experts on Delhi Govt Schools' Use of Facial Recognition Tech*, THE WIRE (Feb. 24, 2021) 'Pandora's Box of Privacy Issues': Experts on Delhi Govt Schools' Use of Facial Recognition Tech (thewire.in).

45 *Id*.

46 Child safety in Delhi school systems became a major concern after multiple shocking incidents occurred in the latter half of 2017. A Delhi school security guard was arrested for raping a five-year-old girl at school in September of 2017. Express News Service, *Guard arrested for 'raping' 5-year old girl inside school in Delhi*, THE INDIAN EXPRESS (Sept. 10, 2017). https://indianexpress.com/article/india/guard-arrested-for-raping-5-year-old-girl-inside-school-in-delhi-4836414/.; in the same month, a student at Ryan International School was found dead with a slit-throat. A school bus driver and a fellow student were primary suspects in the case. *India student arrested for murder of child at Gurgaon school*, BBC NEWS (Nov. 8, 2017) https://www.bbc.com/news/world-asia-india-41914082.

implicate minors[47] and threaten fundamental rights to privacy. Measured by cameras per square mile, Delhi is currently the most surveilled city in the world.[48] Some studies have shown that facial recognition policing in Delhi may expose the community to religiously-targeted surveillance similar to that occurring in China. One study analyzed the geographic distribution of FRT-enabled CCTV cameras throughout the city, finding that a vastly higher number (proportionate to population size and geography) of cameras were installed in neighborhoods with a significant Muslim presence.[49] The study notes that this kind of targeted over-policing may apply to other vulnerable minority groups, including populations of lower castes, sex workers, and homeless communities.[50]

Most countries recognize some form of a right to privacy. However, the respective sources of privacy vary. In the United States, the emergence of a right to privacy is largely credited to a Harvard Law Review article written by Samuel D. Warren and Louis Brandeis in 1890.[51] The EU's right to privacy is more firmly rooted as a founding principle, much like the freedom of expression and speech in the United States. The Universal Declaration of Human Rights, which includes a 12th amendment right to privacy.[52] In 2000, the EU created the Charter of Fundamental Rights of the European Union, which delineated a clear right to privacy in Article 7.[53] In India,

47 Cyber law expert, Pawan Duggal, was quoted saying "CCTV cameras in school opens up a Pandora's Box of legal issues specifically privacy issues. These issues have to be appropriately addressed given the fact that we all have a fundamental right to privacy, which derives from the judgment of Justice K.S. Puttaswamy versus Union of India." *Russel, supra* note 18.

48 Feng, *supra* note 9.

49 Jai Vipra, *The Use of Facial Recognition Technology For Policing in Delhi: An Empirical Study of Potential Religion-Based Discrimination*, MEDIANAMA (Aug. 23, 2021) https://www.medianama.com/2021/08/223-facial-recognition-technology-policing-delhi/.

50 *Id*.

51 Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

52 Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Docs. A/RES/217(III) (Dec. 10, 1948).

53 EU CHARTER OF FUNDAMENTAL HUMAN RIGHTS, art. 7.

however, a clear right to individual privacy was only established in a 2018 Indian Supreme Court ruling surrounding Aadhaar in *Justice K. S. Puttaswamy v. Union of India*.[54]

Aadhaar is a 12-digit identification number issued by the government to provide subsidies, benefits, and other services to citizens.[55] Any Indian resident can voluntarily apply with basic demographic and biometric information, including fingerprint and iris scans and facial photographs.[56] The Aadhaar system is the largest biometrics-based identification system in the world.[57] In *Puttaswamy*, a retired high court Judge challenged the constitutionality of Aadhaar, claiming that it violated citizens' right to privacy based on Article 21 of the Indian Constitution, which guarantees the right to "life or personal liberty."[58] Judge Puttaswamy argued that the government had not implemented adequate safeguards to prevent the misuse of Aadhaar information. Although the ruling by a panel of the nine-judge Supreme Court upheld the constitutionality of Aadhaar, it also acknowledged, for the first time, a right to privacy based on Part III of the Constitution.[59] *Puttaswamy* established that claims could be brought for violations of the right to privacy by both state and non-state actors.[60] Informational privacy, or the right to control one's own data, was found to be a part of the general right to privacy, but the Court was careful to state that this was not an absolute right,[61] setting out a three-part test to determine whether an invasion of privacy may be permissible.[62]

54 *Justice K.S. Puttawswamy v. Union of India*, (1994) (10) SCC 1. (India).

55 *Unique Identification Authority of India*, GOVERNMENT OF INDIA https://uidai.gov.in/what-is-aadhaar.html. (last visited Oct. 05, 2022).

56 *Id*.

57 *Id*.

58 *Unique Identification Authority of India*, *supra,* note 54.

59 Chokshi*, supra*, note 23.

60 *Unique Identification Authority of India*, *supra,* note 54.

61 *Id*.

62 "The Court also declared that the right to privacy is not an absolute right and any invasion of privacy by state or non-state actor must satisfy the triple test i.e. 1. Legitimate Aim 2. Proportionality 3. Legality" *Id*.

In recent years, Aadhaar has been used to distribute COVID-19 vaccinations to citizens at designated vaccination centers.[63] In 2021, the Indian government began developing a pilot program to implement FRT in favor of fingerprints or retina scans to verify vaccine beneficiaries.[64] RS Sharma, CEO of the National Health Authority and former chief of the Unique Identification Authority of India (UIDAI), highlighted FRT's capability to create touchless checkpoints, which would reduce the spread of the virus.[65] Ten human rights organizations and over 150 digital rights organizations have signed a complaint created by the Internet Freedom Foundation (IFF) in response to this news, highlighting the global unreliability of FRT systems and inherent privacy risks.[66] A large-scale rollout of FRT at Aadhaar vaccination centers is likely to bring a new wave of constitutionality arguments before the Supreme Court.

The IFF's complaint delineates some primary concerns and recurring themes:

> Facial recognition technologies (FRT) pose a grave threat to human rights, including privacy, and are being rolled out in the absence of a valid legal basis. We recogni[z]e that the timely and efficient delivery of vaccines is vital. However, the use of facial recognition for authentication does little to ensure this and will in addition put in place rights-infringing technologies that enable mass surveillance and the erosion of fundamental rights. The unchecked rollout of FRTs increases the risk of unchecked government surveillance, and mission creep. Evidence has shown that FRTs are not accurate and linking this untested technology to

63 Monit Khanna, *India Test Touchless Covid Vaccination with Aadhaar Face Detection: Do We Need it?* INDIA TIMES (Apr. 07, 2021). https://www.indiatimes.com/technology/news/india-covid-19-vaccination-touchless-aadhaar-biometric-authentication-537768.html

64 *Id*.

65 *Id*.

66 The Wire Staff, *Digital Rights Bodies Warn Against Use of Facial Recognition Technology in Vaccination Drive*, THE WIRE (Apr. 14, 2021) https://thewire.in/rights/covid-19-vaccination-facial-recognition-technology-aadhaar-vaccine.

> the vaccination roll-out will only exclude persons from the vaccine delivery system.[67]

The complaint effectively demonstrates how the government uses the COVID emergency as a veil to distract citizens from privacy concerns. The IFF alleges that rather than focusing on "increasing the speed, range and efficacy of vaccine delivery," the government is seizing an opportunity to "test out privacy harming technologies."[68] As the IFF states, the proposed benefits of introducing FRT at vaccine centers are unproven and do not meet the standards of legality, proportionality, and legitimacy required to excuse the invasions of individual privacy.

The Chinese and Indian case studies present two different introductions of FRT into society. The former is more brazen and unapologetic, whereas the latter presents a risk of mission creep." In most countries, the introduction of FRT has been more subtle, often sneaking in under facially valiant pursuits, such as anti-terrorism and crime, public health and safety, and increased efficacy in education or distribution of financial benefits.

II. PRIVATE USES OF FRT

In 2021, the Chinese based social media company, TikTok, made a vague and broad change to its U.S. privacy policy, stating that the company, "may collect biometric identifiers and biometric information" from users, including "faceprints and voiceprints."[69] In an eye-catching headline, TechCruch states that "TikTok just gave itself permission to collect biometric data."[70] Ignoring the exaggerative effect of the headline, the article highlights a common practice by numerous technology companies to reserve broad rights

---

67 *Id.*

68 *Id.*

69 Sarah Perez, *TikTok just [g]ave itself permission to collect biometric data on US users, including 'faceprints and voiceprints'*, TECHCRUCH (June 03, 2021, 5:57 PM) https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/?guccounter=1.

70 *Id.*

for the company to collect, use, and store data by sneaking such rights into lengthy privacy policy addendums.

The news of the conspicuous policy change follows other negative press releases surrounding the social media company: namely, a class action suit resulting in a $92 million settlement for violations of Illinois' Biometric Information Privacy Act ("BIPA").[71] Although prior attempts to ban the app in the United States have been put on hold,[72] the Biden administration has expanded an order promulgated under the Trump administration that prohibits U.S. investment in Chinese companies implicated in the surveillance and persecution of Uyghurs.[73] The new order initially lists fifty-nine Chinese firms engaged in making and deploying surveillance technology.[74] Chinese officials would likely respond in kind by arguing that the order inappropriately stifles transnational investment and is plagued by hypocrisy, as the United States reportedly employs similar technologies in anti-terrorism and anti-drug trafficking efforts.[75]

Similarly, in 2019 Facebook was embroiled in a biometrics scandal in violation BIPA. The allegations, resulting in a record breaking $550 million settlement, were that Facebook began scanning and storing users' facial data from photos without their consent or prior notice.[76] The scans appeared as tagging suggestions for friends of users.[77]

---

71 *Id.*

72 "Under the Trump administration, the federal government attempted to ban TikTok operating in the U.S. entirely." *Id.*

73 [David Sanger], *Biden issues an order banning U.S. investment in firms that aid surveillance and repression[*, N.Y.] TIMES[,] (June 3, 2021)[,] https://www.nytimes.com/live/2021/06/03/us/biden-news-today#biden-china-surveillance-order. [The new order includes firms engaged in making and deploying the surveillance technology used against Muslim minorities and dissidents around the globe. George P. Bus, son of Jeb, is running for Texas attorney general.]

74 *Id[.*]

75 *Id[.]*

76 Rachel Pester, *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit*, JOLT [DIGEST] (Feb. 14, 2020)[,] https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit.

77 *Id.*

These instances highlight a common practice by technology giants: to take action and ask for forgiveness rather than to ask for permission beforehand. Tech companies thrive on their ability to adapt, innovate, and predict consumer demands. The most successful companies *create* rather than predict consumer demand. However, these skillsets are not limited to product development. They are also leveraged to evade privacy regulations that are detrimental to their business. The issue is that, unlike the injuries of the industrial revolution that necessitated heightened labor regulations, privacy injuries are not immediately recognizable because they are shrouded in a technological enigma. Tech companies skirt regulation by design, but they also arguably fail to comply with privacy regulations because they themselves don't know how they intend to use data. Innovation occurs at such a high rate that companies may temporarily ignore privacy implications and opt for damage control when and if circumstances require it.

Additionally, the line between private profit-driven uses of FRT and governmental uses is blurry. In 2021, it was reported that the Amazon Ring smart doorbell company had partnerships with over 1,800 law enforcement agencies nationwide.[78] To put that into perspective, some sources estimate that, due to the partnerships, one in ten law enforcement agencies can access Ring video footage without a warrant.[79] This is worthy of attention because the smart doorbell industry has skyrocketed since Amazon's acquisition of Ring in 2018 for over a billion dollars.[80] As of 2020, approximately 16%

78 Lauren Bridges, *Amazon's Ring is the largest civilian surveillance network the US has ever seen*, GUARDIAN (May 18, 2021[, 8:51AM),] https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us.

79 *Id*.

80 Jefferson Graham, *How Ring's Founder Created a Doorbell Worth $1 Billion To Amazon*, INVESTOR'S BUS. DAILY INVESTORS (Oct. 11., 2021, 09:46 AM),) https://www.investors.com/news/management/leaders-and-success/jamie-siminoff-created-a-doorbell-worth-1-billion-to-amazon/#:~:text=Ring%20Founder%20Jamie%20Siminoff's%20Keys,%241%20billion%20six%20years%20later.

of U.S. households use a smart doorbell.[81] Ring's privacy policy describes a hands-off approach to these partnerships. Once footage is downloaded by law enforcement, Ring neither requires agencies to delete footage after any amount of time nor requires agencies to agree to any specific restrictions.[82] The ACLU uncovered Amazon's sales of Rekognition to law enforcement agencies from documents acquired through Freedom of Information Act Requests.[83]

Amazon reportedly stores Ring footage that consists of unknowing passersby filmed by households fitted with the smart doorbells.[84] In October of 2019, Ring released a promotional video on Twitter, clearly showing the faces of children trick-or-treating captured through Ring footage.[85] As of now, Ring is not capable of distinguishing between an adult and a minor.[86] The pervasive network of cameras has riled privacy rights advocates who have concerns about the distribution of recordings of unconsenting minors and adults.[87]

---

81 Carl Weinschenk, *Video Doorbell Research: Amazon Ring Tops in Market Share with 16% of Households Opting In*, TELECOMPETITOR (Feb.14, 2020), https://www.telecompetitor.com/video-doorbell-research-amazon-ring-tops-in-market-share-with-16-of-households-opting-in/.

82 Kate Cox, It's the user's fault if a Ring camera violates your privacy, Amazon says; The company answers to congressional questioning only evades the question, ARS TECHNICA (Nov. 11, 2019, 3:58 PM), https://arstechnica.com/tech-policy/2019/11/cops-can-keep-ring-footage-forever-share-it-with-anyone-amazon-confirms/.

83 Kate Cox, ACLU sues feds to get information about facial-recognition programs, ARS TECHNICA (Oct. 31, 2019, 3:01 PM), https://arstechnica.com/tech-policy/2019/10/aclu-sues-feds-to-get-information-about-facial-recognition-programs/.

84 Cox, *supra* note 82.] OR [Bridges, *supra* note 78.

85 *Ring Video Doorbell 3 TV Spot, 'Happy* Halloween', ISPOT.TV, https://www.ispot.tv/ad/toS1/ring-video-doorbell-3-happy-halloween.

86 *Id.*

87 *Id*.

Although Ring does not currently employ FRT in its products, the company has stated that it may do so.[88] This would be unsurprising as Amazon has reportedly sold FRT to government and law enforcement agencies.[89] The ACLU, with the support of several politicians,[90] has filed numerous Freedom of Information Act requests to compel the government to disclose the ways agencies like the FBI utilize facial recognition technology.[91] As of October 2019, they have received no response.[92] The ACLU highlights Rekognition's propensity for misidentification as highly problematic if used by investigative agencies like the FBI.[93] Moreover, the ACLU released a report revealing that Rekognition technology falsely matched 27 professional athletes from New England major league sports teams to mugshots.[94]

The ACLU has further argued that even in the scenario where FRT used by law enforcement is 100% accurate, it still creates a perpetual

---

88 Tristan Greene, *Why Amazon's Ring and facial recognition technology are a clear and present danger to society*¸ TNW (Jan. 31, 2020, 10:37 PM) https://thenextweb.com/news/why-amazons-ring-and-facial-recognition-technology-are-a-clear-and-present-danger-to-society.

89 Elizabeth Dwoskin, *Amazon is selling facial recognition to law enforcement – for a fistful of dollars*, THE WASHINGTON POST (May 22, 2018, 12:53 PM), https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/.

90 Kate Cox, *Senator pushes Amazon for details about Ring "partnerships" with police; Privacy and civil rights advocates are increasingly concerned about the deals*, ARS TECHNICA (Sept. 05, 2019, 3:53 PM), https://arstechnica.com/tech-policy/2019/09/senator-pushes-amazon-for-details-about-ring-partnerships-with-police/.

91 Kate Cox, *ACLU sues feds to get information about facial-recognition programs; Inquiring lawsuits want to know what the DOJ, DEA, & FBI are using the tech for*, ARS TECHNICA (Oct. 10, 2019), https://arstechnica.com/tech-policy/2019/10/aclu-sues-feds-to-get-information-about-facial-recognition-programs.

92 *Id.*

93 *Id*.

94 Kate Cox, *Amazon wrongly IDed 28 members of Congress and they're not happy about it; Sen. Markey and other ask Amazon to show how it tests Rekognition for "racial bias."*, ARS TECHNICA (July 07, 2018, 4:30 AM), https://arstechnica.com/tech-policy/2018/07/congress-wants-immediate-meeting-with-amazon-to-talk-facial-recognition/.

surveillance scenario that impinges on the liberties of all U.S. citizens.[95]

> Even in the highly unlikely event that face recognition technology were to become 100 percent accurate, the technology's threat to our privacy rights and civil liberties remains extraordinary. This dystopian surveillance technology threatens to fundamentally alter our free society into one where we're treated as suspects to be tracked and monitored by the government 24/7. That's why a number of cities and states are taking action to prevent the spread of ubiquitous face surveillance and why law enforcement agencies, at minimum, must come clean about when, where, and how they are using face recognition technology. There can be no accountability if there is no transparency.[96]

Amazon has reportedly filed patents that would allow its Ring line of home surveillance cameras to ship with Rekognition in them.[97] Amazon's potential future employment of FRT in Ring cameras would accelerate a "dystopian" surveillance society. Fight for the Future deputy director Evan Greer described the problem this way: "Through consumer products like Ring, Amazon is collecting footage and all the data needed to build a nationwide surveillance network… they leverage government relationships to promote their own products, gain consumer trust, and secure their position in the market. This is an unprecedented assault on our society."[98]

In another scheme where public entities become primary clients of FRT developers, schools and summer camps in the United States have begun purchasing FRT as a school-shooter prevention tool and/or simply to capture photos of their kids during playtime more

---

95 *Id*.

96 Kade Crockford, *The FBI is Tracking Our Faces in Secret. We're Suing*, ACLU (Oct. 31, 2019) https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing.

97 Cox, *supra* note 92.

98 *Id*.

efficiently.[99] The primary concern from privacy experts is less about these proposed uses, but rather about the very realistic probability that FRT in schools may "one day be used for purposes other than that for which they are currently intended."[100] In response to the Lockport City School District in upstate New York being the first school system to adopt FRT technology as a school-shooter prevention tool, State Assemblywoman Monica Wallace expressed concern about the lack of policies in place surrounding FRT and the supposed lack of thought put into the decision in the first place. She asked, "is this going to be a surveillance state for our kids?"[101] The FTC is currently reviewing the Children's Online Privacy Protection Act to determine whether biometric data should be a category of "personal information" that the act protects.[102]

III. BUILDING BLOCKS FOR REGULATORY FRAMEWORKS

During this analysis, it is important to acknowledge the vast array of stances and approaches to privacy that independent nation states have. Instead of attempting to construct a uniform set of rules, regulations, or systemic solutions that would apply globally, in a one-size-fits-all fashion, this analysis looks to draw out some foundational principles for an ideal, or at least favorable, FRT framework. First, the veils of consumer benefit and heightened security need to be removed. Said differently, there needs to be more transparency surrounding the true and complete current uses of FRT and more focus on the prevention of harmful future uses that companies and governments could implement under surreptitious policy changes and programs. Second, there needs to be a clear remedial measure for FRT misuse or malfunction: a private right of action, a statutory penalty, or a retraction. Individual governments should develop a mechanism that best fits their legal and social backdrop. Third, certain uses of

99 Julie Jargon, *Facial Recognition Tech Comes to Schools and Summer Camps; Smart cameras and imaging software are coming to summer program and school campuses and focusing on children*, THE WALL STREET JOURNAL (July, 2019, 12:19 PM), https://www.wsj.com/articles/facial-recognition-goes-to-camp-11564479008.

100 *Id*.

101 *Id*.

102 *Id*.

FRT, specifically surrounding particularly vulnerable populations, should be categorically banned. Although I posit several potential specific measures, individual governments should ultimately develop their own way of achieving these goals.

A. Option I - Increased Transparency (Removing the "Veil")

In a predominantly capitalist society, the strongest catalyst for change is consumer demand. Put simply, if consumers actively push for more transparency, private companies will oblige. As we acknowledged earlier, however, the relative invisibility of harms makes it difficult for consumers to stay informed about privacy issues. Even when consumers are aware of potential harms, the options available to combat such harms are intentionally inconvenient and cumbersome.

Despite the challenges, some privacy academics have espoused a way of fighting back, known as "obfuscation." Developed by Helen Nissenbaum, obfuscation is essentially a revolution against data tracking and surveillance.[103] Its goal is to subvert companies' ability to track and manipulate users.[104] Privacy-minded consumers can proactively take steps to confuse the systems that are tracking them or to prevent tracking overall. A simple example of an obfuscation action is to place a sticker over one's smartphone camera. Other methods include using browsers like AdNauseam that prevent companies like Google from tracking and storing URL data and search history.[105]

Other privacy specialists prefer enhanced regulation to Nissenbaum's obfuscation revolution. In the U.S., Woodrow Hartzog and Neil Richards argue that U.S. law and regulation can create meaningful relationships between companies and consumers that could mitigate harmful practices surrounding user data.[106] Enhanced Federal Trade Commission ("FTC") power, a strengthened breach of

103 HELEN NISSENBAUM & FINN BRUNTON, OBFUSCATION; A USER'S GUIDE FOR PRIVACY AND PROTEST (2015).

104 *Id*.

105 *Id*. at 26.

106 Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L. J. 985 (2022).

confidentiality tort, or a duty of loyalty[107] would make it easier for individuals and enforcement agencies to hold companies liable for deceitful and problematic behavior. Another issue with obfuscation is that it puts the onus on the user, rather than companies, to create a more balanced power dynamic. This is problematic for the obvious reason that it is arduous for the consumer, but also because it ignores the reality that not all asymmetrical power relationships are adversarial.[108] Hartzog and Richards argue that we can use increased awareness and market forces to create more equitable relationships through legislation.[109] In a sense, the pair have also pushed for a revolution (an awareness revolution), but not of the kind that Nissenbaum envisioned. It is important to note, however, that Richards's theory is premised on statutory reform in the United States.

In either case, these experts clearly believe that consumers can push back. In other words, some sort of revolution is *possible*. By highlighting some of the most visible problematic FRT practices, such as those used to further a Uighur genocide, consumers are more likely to be riled in a way that would force companies to respond. Academic theories and legal doctrines have noticeably been useful in pushing the ball forward in both state and federal legislatures. However, these types of works are unlikely to sway private companies to *voluntarily* take action and are rarely read or understood by the average consumer. Additionally, academic papers generally do not have a broad readership and certainly do not make their way into the masses; a privacy scholar would need to boil down the issues into something short and digestible by the average citizen to sufficiently affect the general population. A well-curated and highly entertaining documentary on major video streaming platforms might be conducive to this goal. We have seen this done before with the NSA revelations from Edward Snowden and the subsequent documentaries and Oliver Stone film that followed. Ironically, it is even plausible that dissemination about the harms of FRT through social media might be the key to inhibiting FRTs power.

---

107 *Id*.

108 Woodrow Hartzog & Neil Richards, *Privacy's Trust Gap*, 126 YALE L. J. 1180, 1215 (2017).

109 *Id*.

During the Arab Spring, the Black Lives Matter movement, and a multitude of other events, social media has been instrumental in spurring ideological revolutions. It is not unforeseeable that a succinct and digestible video exposing the nefarious uses of FRT and related human rights violations could go viral, acting as the primary catalyst for the kind of awareness revolution that Hartzog and Richards envision. This is complicated by the fact that most major social networks are banned in authoritarian countries like China. However, although the Chinese government may be insulated from global pressure by allies and key economic partners, private Chinese companies who are hurt economically by changing global norms are not.

Consumer demand is the end all be all for global companies that utilize FRT. In this sense, I believe that a consumer awareness revolution about the dangers of FRT is the most efficacious manner to spur voluntary change from private companies. The problem with current media coverage of issues stemming from FRT use is that they rarely highlight the technology's role in causing harm. During the 2022 Olympics, many broadcasters acknowledged the ongoing Uighur genocide but virtually none identified China's use of FRT in carrying out the human rights violations. Bad actors will naturally gain the spotlight, but it is important to recognize that bad actors are further empowered by FRT.

Rapid technological innovation almost ensures that private companies will periodically drum up new ways to leverage FRT. Problems arise where those novel uses are at odds with the uses that are initially presented to consumers. Instead of seeking meaningful informed consent from users, companies will often sneak new uses into updated privacy policies that consist of hundreds to thousands of provisions. One way to proactively mitigate the risk of "innovative" future uses of FRT is require tech companies to get approval from an existing or new regulatory body for every new use of FRT that they implement.

In the United States, a reimagined FRT regulatory agency could operate similarly to the U.S. Patent and Trademarks Office. Traditional regulation simply cannot keep up with innovation. The only way to prevent unethical privacy practices is to regulate

innovation itself. I propose that, like patents, tech companies should have to submit proposals or applications for every new use of data that they develop. Opponents of this model may argue that it would stifle technological innovation. This is true; however, it is also true for patents, and Congress had little trouble justifying the necessity of a separate patent agency and an entire patent regulatory/legal framework.

The FTC has begged Congress for more regulation that can be enforced directly. The key is to implement regulations that put less responsibility in the hands of consumers and more in the hands of companies. Preemptively listing specific banned practices is ineffectual, as technological advancements will soon make such practices extinct or inapplicable. A patent office model would eliminate the difficult guessing game where Congress must constantly try to predict the things tech companies want to do with facial scans. Instead, by implementing the "patent" model Congress rightfully places the onus on the tech companies to list their own desired future practices and justify them before the Privacy Agency.

Alternatively, the U.S. might find it more feasible to bolster an existing regulatory body, like the FTC, than create a new one altogether. In response to the Cambridge Analytica Scandal,[110] the FTC fined Facebook five billion dollars (the largest fine ever levied by the FTC).[111] Yet, some prominent actors argue that such a punishment was not enough. Commissioner Rohit Chopra stated in her dissent to the Cambridge Analytica settlement that "$5 billion dollar penalties make for a good headline, but terms and conditions including blanket immunity for Facebook executives and no real restraints on Facebook's business model, do not fix the core problems

110 The Cambridge Analytica scandal implicated a breach of more than 87 billion Facebook users' personal data. The third-party political consulting firm utilized a personal quiz to scrape the preferences and leanings of all who took the quiz *and* all of their connections/friends. Although, not wholly proven, it is posited that the scandal may have affected the outcome of the 2016 US presidential election. Alvin Chang, *The Facebook and Cambridge Analytica Scandal Explained With A Simple Diagram,* VOX (May 2, 2018) https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

111 *Facebook 'to be fined $5bn over Cambridge Analytica Scandal*, BBC NEWS (July 13, 2019) https://www.bbc.com/news/world-us-canada-48972327.

that led to these violations."[112] Chopra argues that outside of the fine, the "restrictive" mechanisms attached would essentially allow Facebook to assess for themselves whether they are following adequate privacy practices.[113] The FTC agreement does not contain any hardline provisions on how Facebook collects, share or uses personal data.[114] Chopra's most convincing argument is that, although five billion dollars is a historically large number, the fine is wholly inadequate as a deterrent because it is likely that Facebook's difference in earnings as a result of privacy violations (unjust gains) matched or exceeded that number.[115]

A potentially less dismal view of the five billion dollar fine might be that a fine of this caliber signals a willingness by the courts to impose even higher penalties in the future. Imagine that Facebook again breaks their existing consent decree; if the FTC can impose penalties that are high enough that they deter unethical privacy practices, we might begin to see the origin of an effective enforcement mechanism.

B. Option II - Categorical Bans on FRT

Although efforts to neutralize FRT are laudable, in certain contexts and applied to certain groups, the risk of abuse is too high to warrant any continued use of the software. With vulnerable populations like minors, refugees, and socially/economically disenfranchised groups, categorical bans are the only way to prevent future oppression and abuse.

1. Minors

---

112 *Dissenting Statement of Commissioner Rohit* Chopra; *In re Facebook, Inc. Commission File No. 1823109*, UNITED STATE OF AMERICA FEDERAL TRADE COMMISSION: OFFICE OF COMMISSIONER ROHIT CHOPRA (July 24, 2019) Accessed at:
https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

113 *Id*.

114 *Id*. at 1.

115 *Id*.

In the United States, both law and corporate policy often protect minors' privacy at a higher level than legal adults.[116] Still, minors are not insulated from many increasingly relevant privacy harms, including harms from algorithmic and/or targeted advertising.[117] Justifications like enhanced education, safety, and behavioral monitoring ring hollow in light of a clear consent problem. Providing children with a special level of protection and care in different contexts is an international norm.[118] This international norm is partially premised on the lack of capacity for children to give informed consent. In the specific case of FRT, it is unreasonable to expect a child, who is still "evolving (in) capacity, age and maturity," to make rational decisions surrounding FRT because they do not fully understand the dangers associated with giving companies or individuals access to their facial scans.[119]

Justices Warren and Brandeis argued that an individual ought to be able to form opinions and ideas without being watched or being worried about being watched.[120] This is especially true for minors, who are physically and mentally in the developmental stages of their lives.[121] Studies show that being surveilled changes the way that human beings operate and interact with each other.[122] Indeed, some

116 Katie Hanna, *COPPA (Children's Online Privacy Protection Act),* TECHTARGET https://www.techtarget.com/searchcio/definition/COPPA-Childrens-Online-Privacy-Protection-Act.

117 Gilad Edelman, *Biden Puts Big Tech's Favorite Business Model on Notice; The regulation of surveillance advertising used to be a fringe idea. Now it's in the State of the Union Address, at least when it comes to kids*, (Mar. 2022) https://www.wired.com/story/biden-targeted-ads-state-of-the-union/.

118 Convention on the Rights of the Child, Preamble (Nov. 1989), accessed at https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

119 CRC Committee General Comment No. 4: Adolescent Health and Development in the Context of the Convention on the Rights of the Child, (Jul. 2003), accessed at https://www.refworld.org/docid/4538834f0.html.

120 *See generally,* Warren and Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

121 NEIL RICHARDS, WHY PRIVACY MATTERS, 117 (2022).

122 *Id*. at 113-120.

entities leverage FRT to change behavior in the classroom.[123] To interfere with the natural experimentation and growing process of young people is morally and ethically questionable. Whether or not these FRT systems increase test scores or behavioral statistics is irrelevant. An argument for sacrificing privacy in the effort to create a more "perfect" society is grossly problematic and reminiscent of outlandish dystopian novels.[124] As such, FRT use on minors should be categorically banned. Whether this is feasible depends on the context.

2. Special Groups

The GDPR already has provisions in place to protect "special groups" of people.[125] The GDPR delineations of special populations are fairly similar to that of the U.S. and include primarily racial/ethnic minorities, LGBTQ individuals, different gender groups, and religious groups.[126] However, the groups of people that need most protection from FRT may be different. Racial minorities are defined differently in South Africa than they are in Japan.[127] The key is identifying the most vulnerable populations in the relevant community and ensuring that FRT cannot be used to identify or differentiate individuals based on those population groups. This is the only way to prevent governments and companies from inadvertently causing biased outcomes or intentionally oppressing weak populations.

C. Assessing the Feasibility of Categorical Bans

The EU has already taken significant action to identify some of the most harmful uses of artificial intelligence and ban them outright. The

123 Nila Bala, *The Danger of Facial Recognition in Our Children's Classrooms*, (Apr. 2020) https://www.rstreet.org/2020/04/30/the-danger-of-facial-recognition-in-our-childrens-classrooms/.

124 *See generally*, GEORGE ORWELL, 1984 (1949).

125 *See generally*, General Data Protection Regulation, Art. 9 (2018).

126 *Id*.

127 *Race in South Africa: 'We Haven't Learned We Are Human Beings First',* BBC (Jan. 21, 2021) https://www.bbc.com/news/world-africa-55333625.

2021 AI (Artificial Intelligence) Act creates four tiers of artificial intelligence based on their potential for harm.[128] Those categorized in tier one are regarded as threatening "unacceptable risk" and are banned entirely.[129] The AI Act subjects the second-tier uses, falling under "high-risk," to regulations and legal requirements.[130] Notably, the AI Act website specifically mentions the uses of the Chinese government as falling into the first category.[131] It is possible that the AI Act, like the GDPR, will set create a blueprint for the global community to follow.

Woodrow Hartzog has been a staunch supporter of a categorical ban on FRT use by law enforcement.[132] But how feasible is this idea? For some scholars, a complete prohibition of this nature seems completely out of reach and misplaced.[133] However, major municipalities, including San Francisco, Portland (Oregon), Portland (Maine), Springfield (Massachusetts), and Boston, have successfully implemented such restrictions.[134] In 2021, Maine passed state facial

---

128 Firm Memoranda, *The EU's Regulation on Artificial Intelligence*, QUINN EMANUEL (Sept. 13, 2022) https://www.quinnemanuel.com/the-firm/publications/client-alert-the-eu-s-regulation-on-artificial-intelligence/#_ftnref3.

129 *Id*.

130 *Id*.

131 THEAIACT, *What is the EU AI Act?,* https://artificialintelligenceact.eu/ (last visited Oct. 31, 2022).

132 Woodrow Hartzog, *Facial Recognition Is the Perfect Tool For Oppression*, MEDIUM (Aug. 2, 2018) https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

133 *Id.* (citing Judith Donath).

134 The San Francisco bill follows neighbors Oakland and Berkeley and "states unequivocally that the risks involved in using the technology substantially outweigh... its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring*."* (internal quotations omitted). Cyrus Farivar, *San Francisco lawmaker: Our cops should be banned from using facial recognition; Bill says risk to civil liberties "substantially outweighs its purported."* ARS TECHNICA (Jan. 01, 2019) https://arstechnica.com/tech-policy/2019/01/san-francisco-lawmaker-our-cops-should-be-banned-from-using-facial-recognition/.; *13 Cities Where Police Are Banned from Using Facial Recognition Tech*, INNOTECH TODAY (Nov. 18, 2020) https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/.

recognition ban that the ACLU described as "groundbreaking." [135] The ban prohibits Maine police from accessing FRT directly; they must instead submit requests for FRT searches to the FBI.[136] The Maine law closed a "loophole[] that police have used in the past … by informally asking other agencies or third parties to run backchannel searches for them."[137] The law only allows FRT use in the specific instance that police have "probable cause that an unidentified person in an image committed a serious crime, or for proactive fraud prevention."[138] Whether this signals a future trend toward FRT bans or is simply representative of the views of constituents in a small subset of regions is hard to say, as not all state facial recognition bans have been heralded as victories. Privacy advocates were generally disappointed with Washington state's FRT ban enacted in 2021 because it contained large carve-outs for police to take advantage of.[139] This was unsurprising to many, as the author of the bill, State Senator Joe Nguyen, is an employee of Microsoft.[140] However, it is without question that opposition to FRT use by law enforcement is not insignificant.[141]

---

135 Michael Ratsimbazafy, *Maine's Landmark Facial Recognition Law: Preserving Our Rights in the 21st Century*, ACLU OF ME., https://www.aclumaine.org/en/draft-maines-landmark-facial-recognition-law-preserving-our-rights-21st-century#:~:text=The%20bill%2C%20now%20law%2C%20prohibits,schools%2C%20and%20for%20surveillance%20purposes.

136 Dave Gershgorn, *Maine passes the strongest facial recognition ban yet; The law bans most use of the technology and adds accountability measures*, THE VERGE (June 31, 2021) https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law.

137 *Id*.

138 *Id*.

139 *Id*.

140 *Id*.

141 Additionally, The Congressional Black Caucus wrote a letter to Amazon CEO Jeff Bezos in response to sale and distribution of Amazon's Rekognition technology. Congressional Black Caucus, *Final Cbc Amazon Facial recognition Letter*, (May 24, 2018) accessed at: https://www.documentcloud.org/documents/4618699-Final-Cbc-Amazon-Facial-Recognition-Letter.html.

However, in other parts of the world, where there is historically less emphasis on individual rights and more emphasis on community safety and wholistic society, such categorical bans are probably not likely.

D. Option III - Remedial Measures

If complete bans on FRT by governmental organizations do not come to fruition soon, how else can we mitigate the current harms stemming from law enforcement use of FRT? In this instance, remedial measures need to be put in place for harmed individuals to receive restitution. As FRT technology is still in its early stages, reports of consequential misidentification are not uncommon.[142] In situations where individuals are wrongly identified and suffer harm, such individuals should have an avenue to right those wrongs. Possible remedial measures include private rights of action, mandatory investigations upon receipt of complaints by independent investigatory agencies, and penalties for misidentification.

Standing is an issue in many parts of the world, including the US. The hurdle for standing to bring misidentification actions in the United States against private companies is apparent in *TransUnion v. Ramirez*.[143] In *Ramirez*, a class action suit was rejected due to a lack of Article III standing where plaintiffs alleged harm caused by their names being erroneously placed on a Treasury Department terrorist database.[144] The primary plaintiff, Sergio Ramirez, successfully alleged harm because he was denied the ability to buy a car when the dealership's credit check returned a terrorist threat warning.[145] However, the Supreme Court ruled that a subclass of plaintiffs failed to meet the standard required for injury because the erroneous reports were never actually sent to third-party credit agencies.[146] As such, *Ramirez* presents an additional impediment for plaintiffs that may

142 *Supra*, note 30.

143 *TransUnion v. Ramirez*, 141 S. Ct. 2190 (2021).

144 *Id.*

145 "Standing; *TransUnion v. Ramirez*", 135 HARV. L. REV. 333 (Nov. 10, 2021).

146 *TransUnion, 141 S. Ct. 2190 at 2202.*

have been misidentified by FRT unless they can show actual damages.[147]

Similarly, in India, although *Ramaswamy* established a legal right to privacy, the scope of this privacy right is not definitive and evidently does not cover the intrusions of Adhaar. With the possibility of an FRT-equipped Adhaar system, it is possible that more suits will be brought in India's court system. However, as of now, we have no way of knowing whether FRT encroachments will pass the balancing test set forth by *Puttaswamy*. Likewise, China is unlikely to recognize any sort of private right of action for privacy violations given its more deeply rooted history of government-sanctioned surveillance. For China, I would argue that market forces are even more important in trying to curb the effects of FRT use.

To get around the standing problem in the United States, there is perhaps a novel argument that a facial scan constitutes a "search" under the fourth amendment. In *Carpenter v. United States*, the Supreme Court ruled that location data was pervasive and specific enough to constitute a fourth amendment search.[148] In the case, law enforcement used cellular data to track the plaintiff's whereabouts for four months and ultimately used such data to convict him of a robbery.[149] The Supreme Court's decision in *Carpenter* reflected Justice Alito's concern in his concurrence in *Jones v. United States* that "dramatic technological change" allows for a higher level of invasiveness that the legislature is best suited to address.[150] In considering whether the use of location data in law enforcement investigations is legal, courts have considered whether the actions being monitored were actually "exposed to the public"[151] and whether a person took outward action to shield himself from the public.[152] In *United States v. Maynard*, the Court determined that the plaintiff's

147 Standing; *TransUnion v. Ramirez*, *supra* note 147.

148 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

149 *Id.* at 2212.

150 *United States v. Jones*, 565 U.S. 400, 429 (2012).

151 *United States v. Knotts*, 460 U.S. 276, 281-82 (1983).; *Katz* 389 U.S. 437 (1967).

152 *Kyllo v. United States*, 533 U.S. 27, 28-29 (2001); *Florida v. Riley*, 488 U.S. 445, 450 (1989).

whereabouts over the course of a month were not readily "exposed to the public," despite them traveling in primarily public spaces, because "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[153] By this line of reasoning, just because one's face is readily and necessarily exposed to the public does not mean that the information it can provide through FRT scans is completely up for grabs. Furthermore, the Supreme Court in *Carpenter* gave great weight to the fact carrying a cell phone everywhere is "indispensable to participation in modern society," making it possible for law enforcement to catalog a person's every movement in real-time.[154] Even more than our cellphones, we "carry" our faces everywhere we go. The vast amount of information that can be revealed through a facial scan necessitates strengthened fourth amendment protection. Otherwise, an inevitable configuration of CCTV cameras with FRT will create a society with perpetual surveillance. Virtually *every* individual's location would be known at any time.

CONCLUSION

In its brief lifespan, FRT has shown a tremendous breadth of potential applications. However, it has also quickly been revealed as a tool for the oppressor. The issue is that FRT currently is wielded by only the most powerful actors in society; law enforcement agents and tech industry giants hold the keys to the castle, and the general public has demonstrated very little opposition to that. While consumers are enraptured by the ways that FRT makes life more convenient, the marketed conveniences and benefits are, in actuality, a very small part of how private companies leverage FRT in their business model. Moreover, inevitable innovation will likely spawn a platter of brand-new harms that tech companies will add to existing products, packaged as "enhancements" or "upgrades." By purchasing an Amazon Ring now, consumers open the door to the possibility that FRT will be implemented in the future. Surely, few purchasers have considered the privacy harms that FRT implementation in those cameras can incur.

153 *United States v. Maynard*, 615 F.3d 544, 560 (D.C. Cir. 2010).

154 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Governments praise FRT's efficacy in crime prevention and overall safety enhancements. Yet the same technology that is touted for its ability to keep civilians safe is being used to target and persecute particular communities. Many are aware of the human rights violations the Uighur community is experiencing, but few are privy to FRT's role in hastening it. The issue with singling out the Chinese government as the bad actor in this scenario is that it ignores the weapon that enables the "bad guy" to commit crimes in the first place. The case studies discussed above demonstrate that we are already beginning to see FRT being wielded as a tool for oppression in other countries like India. Ignoring FRT's weaponization only allows it to spread further throughout the globe.

Awareness is the surest catalyst for change. The difficulty in the case of FRT is that the harms are not obvious; understanding the injuries that FRT levies requires a certain degree of technical knowledge. However, just because it is difficult does not mean it is impossible to enlighten the general public of "invisible" harms. It wasn't until 1990 that nutrition facts labels became a federal requirement in response to increased public demand for detailed product information.[155] People wanted to know more about their food, and the government responded by creating an incredibly complex and effective regulatory agency in the FDA. There is no reason that a similar regulatory agency cannot manage FRT innovation requests and determine which proposed uses would be harmful to society. Arguments that an FRT regulatory agency would be overwhelmed with requests are misguided. The US Patent Office received and processed over 650,000 patent applications in 2019.[156]

Lastly, there are certain contexts in which the introduction of FRT presents such a high risk of harm that its use should be banned entirely. Minors are particularly susceptible to abuse, and FRT in particular would facially interrupt the natural development of

155 *Factual Food Labels: A Closer Look at the History*, The University of Texas at Austin Department of Nutrtional Sciences (April 06, 2018) https://he.utexas.edu/ntr-news-list/food-labels-history.

156 U.S. Patent and Trademark Office, *U.S. Patent Statistics Chart Calendars Year 1963-2020*, https://www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.htm (last updated May 5, 2021).

children in the classroom and other public spaces. Hopefully, the EU can set a global standard with GDPR and future legislation to prevent FRT identification of any individual based on special categories. Repeating the words of Claire Garvie, "If you can make a technology that can classify people by ethnicity then people will use it to repress that ethnicity."[157] The same goes for religion, gender, and sexual orientation. Political affiliation can be isolated and weaponized to change the outcome of elections, as the Cambridge Analytica scandal has shown us. Ultimately, each respective locale needs to identify their most vulnerable populations and protect them with legislation. In the U.S., this seems like a very real possibility. However, in other countries with differing social norms, change will necessarily begin with an awareness revolution.

Christopher Ian Kim

157 Paul Mozer, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority* NY TIMES (Apr. 14, 2019) https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html#:~:text=%E2%80%9CIf%20you%20make%20a%20technology,it%20to%20repress%20that%20ethnicity.%E2%80%9D&text=From%20a%20technology%20standpoint%2C%20using,sort%20people%20into%20broad%20groups.