Facial Recognition Technology and a Proposed Expansion of Human Rights

Catherine Ryan*

TABLE OF CONTENTS

* J.D., May 2024, The George Washington University Law School; Editor-in-Chief, Federal Communications Law Journal, Volume 76; B.S., June 2017, Finance, California Polytechnic State University. I would like to thank the entire FCLJ staff for their incredible work in producing this publication. A special thanks to Professor Ralph Steinhardt, who inspired this Note, for his perpetual guidance and kindness. I would also like to thank my best friend, who makes everything in my life better. Finally, I would like to extend gratitude to my parents and brother for their unconditional love and support in all my endeavors, regardless of their practicality.

I. INTRODUCTION

One way to understand technology is through how it distributes power. The classic technological innovation—the wheel—began as a pottery tool in 3500 B.C.[1] When turned on its side, it resulted in a dramatic increase in farming capacity and an improved economy for agrarian societies.[2] The wheel also removed barriers to going to war, as soldiers no longer had to walk on foot.[3] While food output increased, benefitting communities generally, so did the ease with which wealthier nations could exert military power over poorer nations.

This is an important lens because the distribution of power is rarely equitable, and an imbalance of power invites abuse. For example, the crossbow appeared in Italy in the 10th and 11th centuries when metals were substituted for wood in its construction, making it a much-feared weapon of war.[4] Decades later, in 1139, Pope Innocent II attempted to outlaw crossbows as too dangerous of a weapon for war, realizing the disproportionate advantage this innovation would give certain countries.[5] More recently, wiretapping was invented in the late 19th century and became a common practice for the government and commercial industries in the early 20th century.[6] Public opinion soon soured on the practice following the Watergate scandal, as individuals realized the threat this technology could pose to the private citizen if it were abused.[7] Even the Laws of War respond to technological innovation to prevent abuse by ensuring regularly updated elementary considerations of humanity.[8]

Extreme abuses of power, those that create an unease in peoples' deeply held notions of humanity, lead countries to identify violations of fundamental human rights and act to prevent such atrocities from occurring again. The use

---

1. Megan Gambino, *A Salute to the Wheel*, SMITHSONIAN MAG. (Jun. 17, 2009), https://www.smithsonianmag.com/science-nature/a-salute-to-the-wheel-31805121/ [https://perma.cc/UN7F-NH7A].

2. Cody Cassidy, *Who Invented the Wheel? And How Did They Do It?*, WIRED (May 6, 2020), https://www.wired.com/story/who-invented-wheel-how-did-they-do-it/ [https://perma.cc/EMW6-7KKL].

3. Tanu Rao, *The Invention that Changed the World: The Wheel*, INTERSTEM (Mar. 31, 2021), https://www.interstem.us/events/the-invention-that-changed-the-world-the-wheel.html#:~:text=The%20wheel%20was%20first%20used,of%20getting%20tired%20of%20walking [https://perma.cc/KV7N-X4L4].

4. *Crossbow*, ENCYC. BRITANNICA, https://www.britannica.com/technology/crossbow [https://perma.cc/87CY-AENA] (last visited Jan. 28, 2023).

5. H. J. SCHROEDER, DISCIPLINARY DECREES OF THE GENERAL COUNCILS: TEXT, TRANSLATION AND COMMENTARY 195-96, 213 (B. Herder Book Co., 1937) (https://archive.org/details/DisciplinaryCouncils/page/212/mode/2up) [https://perma.cc/5LET-XR78].

6. April White, *A Brief History of Surveillance in America*, SMITHSONIAN MAG. (Apr. 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ [https://perma.cc/DFT9-X7W9].

7. *Id.*

8. Rain Liivoja, *Technological change and the evolution of the law of war*, 97 INT'L REV. OF THE RED CROSS 1157, 1157-77 (2016) (https://international-review.icrc.org/sites/default/files/irc_97_900-10.pdf) [https://perma.cc/Q9KH-9YYW].

of facial recognition technology (FRT) poses a great and systemic risk to individuals worldwide and violates notions of humanity. An individual's facial biometric data, often exploited using FRT without the individual's consent, is unique and inherently individualistic data that should be protected and codified as a human right. The best way to codify such a privacy right is through domestic legislation and executive action, and international agreements, specifically in applying the Ruggie Principles to facial recognition.

This Note begins with a background on the development of human rights, focusing on the process by which human rights are determined. This section concludes by proposing a process by which human rights come to fruition, the Progressive Theory of Human Rights, following events that upend peoples' deeply held notions of humanity. Next, this Note explains the relevant technology and terms of Artificial Intelligence (AI) and of FRT as a sub-category of AI. This section provides the reasoning for assuming that FRT is a substantially distinct form of AI and requires specialty rules and regulations. The Note then examines existing FRT case law, regulations, and authoritative statements and actions, both domestic and international. This section concludes by highlighting the most influential authorities that will inform the structure and substance of the proposed legal scheme. The background section ends with an exploration of the real-world implications of the use of facial recognition and the misaligned incentives of large corporations.

The Note proposes why the right to privacy of one's facial biometric data should be a protected human right. This section first argues how this right to privacy is a natural extension of the existing doctrine of human rights. It then argues in the alternative that the right to privacy of one's facial biometric data fits squarely within the first stage of recognizing a new human right. It concludes with a proposed framework of (1) domestic legislation, pulling from sources like the European Union's (EU) General Data Protection Regulation (GDPR) and domestic state privacy laws; (2) executive branch action in the form of agency mandates and exploration of AI-specific committee formation; and (3) international action through applying the Ruggie Principles to FRT to guide understandings of corporate responsibility for human rights in the use of FRT and through coordinated international agreements.

II. BACKGROUND

A. A Brief History of Human Rights

Human rights did not descend as proclamations from the skies, nor were they created and codified out of the goodness of those in powers' hearts. They developed from the ground up—through organizing and activism—following atrocities and major technological developments that created sufficient unease with currently accepted practices that violate deeply-held notions of humanity. Nor do they exist in a vacuum: any consideration of human rights

must acknowledge and incorporate the intersecting considerations of modern philosophy, society, culture, and politics.[9]

Take for example the freedom from "torture or cruel, inhuman, or degrading treatment or punishment."[10] Beginning in ancient Greece and continuing well into the 20th century, physical torture was a common form of punishment and often used as a means of justice.[11] The practice held significant political and social value, as well as a means for judicial expedition, as those accused of heresy or witchcraft favored admitting guilt over potential torture.[12] Nations with similar progressive ideologies began abolishing the practice in the 18th century for, among others, practical and moral reasons, as social understandings of humanity and dignity evolved.[13] However, the practice of torture was first recognized as a violation of international law in 1948 with the Universal Declaration of Human Rights, a direct response to the atrocities witnessed in the Second World War.[14] It was only through tireless efforts by non-governmental organizations and community groups in the 1970s, 80s, and 90s raising sufficient cries of outrage that actual instruments were put in place to hold perpetrators liable for acts of torture.[15]

The question then is, if not from the sky, nor from the better angels of our nature, where did human rights originate? While subtly hinted at in revolutionary declarations such as the 1776 American Declaration of Independence and the 1789 French Declaration des droits de l'Homme et de du citoyen (Declaration of the Rights of Man and Citizen), the enshrining of human rights into international law is a relatively recent development, beginning most notably with the aforementioned Universal Declaration of Human Rights (UDHR) of 1948.[16] The UDHR was an atonement for sins of the past and a promise to generations of the future, where—as of this writing—192 member nations have signed and mutually agreed upon basic understandings of human rights. Each subsequent treaty and convention reflects the growing understanding of what rights individuals must possess to maintain their inherent dignity and humanity.[17] The UDHR originally listed

9. A thorough analysis of the broad range of considerations and infuences on human rights is beyond the scope of this Note.

10. G.A. Res. 217 (III) A, ¶ 5 Universal Declaration of Human Rights (Dec. 10, 1948).

11. Nigel Rodley, *Torture*, ENCYC. BRITANNICA, https://www.britannica.com/topic/torture [https://perma.cc/N2HS-DG5H] (last visited Jan. 28, 2023).

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

16. Nancy Flowers, *A Short History of Human Rights*, UNIV. OF MINN., http://hrlibrary.umn.edu/edumat/hreduseries/hereandnow/Part-1/short-history.htm [https://perma.cc/DZ7Q-FJ7Z] (last visited Jan. 28, 2023); Frans Viljoen, *International Human Rights Law: A Short History*, U.N. CHRONICLE, https://www.un.org/en/chronicle/article/international-human-rights-law-short-history [https://perma.cc/XPK5-HMM7] (last visited Jan. 28, 2023).

17. Viljoen, *supra* note 16.

six "families" of human rights[18] which the United Nations broadly categorized into three "generations" of human rights, " . . . as an echo to the cry of the French revolution: Liberté (freedoms, "civil and political" or "first generation" rights), Egalité (equality, "socio-economic" or "second generation" rights), and Fraternité (solidarity, "collective" or "third generation" rights)."[19]

This Note focuses on the first generation of rights, civil and political rights, as FRT poses the biggest risk to this collection of freedoms. The foundation of these rights is based on the UDHR, the European Convention on Human Rights, and the International Covenant on Civil and Political Rights (ICCPR), which was adopted in 1966 and makes up one-third of the Geneva Convention.[20] The ICCPR in particular enshrines certain personal liberties and freedoms to all persons to liberty and security within their person, the right to liberty of movement, and to be free from restrictions on such liberties unless necessitated by law or national security.[21] Article 17 in particular guarantees the freedom from "arbitrary or unlawful interference with [one's] privacy."[22] The use of biometric data arbitrarily or unlawfully—that is, without proper consent or knowledge—directly violates the basic rights protected by the ICCPR, and therefore, the right to one's own biometric data should be considered a civil human right.

Consistent among these foundational documents—the UDHR, the European Convention on Human Rights, and the ICCPR—are the principles of freedom, self-determination, and the individual states' obligations to protect those rights and address any threats to them.[23] These documents also create the parameters within which new human rights might emerge to ensure the continued protection of these freedoms.[24] However idealistic this may sound, the actual process is much trickier.

With every generation of rights comes the benefit—and burden—of hindsight to better understand the process that leads to the creation of a

---

18. "(1) Security rights that protect people against murder, torture, and genocide; (2) Due process rights that protect people against arbitrary and excessively harsh punishments and require fair and public trials for those accused of crimes; (3) Liberty rights that protect people's fundamental freedoms in areas such as belief, expression, association, and movement; (4) Political rights that protect people's liberty to participate in politics by assembling, protesting, voting, and serving in public office; (5) Equality rights that guarantee equal citizenship, equality before the law, and freedom from discrimination; and (6) Social rights that require that governments ensure to all the availability of work, education, health services, and an adequate standard of living." *Human Rights*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Apr. 11, 2019), https://plato.stanford.edu/entries/rights-human/ [https://perma.cc/4PU8-T7GA].

19. Viljoen, *supra* note 16.

20. The European Convention on Human Rights followed shortly after the UDHR in 1950; other notable treaties include the American Convention on Human Rights and the African Charter on Human and People's Rights. *See* Viljoen, *supra* note 16.

21. G.A. Res. 2200A (XXI) A, Articles 9 and 11, International Covenant on Civil and Political Rights (Dec. 16, 1966).

22. *Id.*

23. *See* Universal Declaration of Human Rights, *supra* note 10; International Covenant on Civil and Political Rights, *supra* note 21.

24. *See* International Covenant on Civil and Political Rights, *supra* note 21.

recognized human right. This process never exactly repeats itself, but it does rhyme. This Note examines the creation of a human right as broadly occurring within three linear stages, with many zigs and zags, steps forward and backward, in between. This process is referred to in this Note as the Progressive Theory of Human Rights Development (Progressive Theory). The 1979 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) is used to illustrate this Progressive Theory.

Stage One of the Progressive Theory begins with quiet whisperings, where small groups sound an alarm regarding the subject's destructive nature and propose aspirational change.[25] The multiple alarms likely approach the subject from different angles but reach the same conclusion. In the lead-up to the drafting of CEDAW, these angles included gender-based discrimination spanning marriage, the legal status of women, the economic status of women, employment opportunities, and educational opportunities.[26] All of these approaches ultimately zeroed in on common themes and proposed reforms.[27] Group advocacy for heightened protections for women resulted in the creation of the Commission on the Status of Women in 1946 to address urgent human rights issues facing women.[28] As important as the work in the Commission was, it failed to provide comprehensive protection for women against discrimination and therefore failed to promote equal rights.[29]

Down the line, either such alarms are tragically legitimized, following one or a series of major incidents, or societal consciousness reaches a point where the subject is no longer tolerable, thus marking Stage Two of the Progressive Theory.[30] For CEDAW, it was an emergence in the 1960s "of a new consciousness of the patterns of discrimination against women and a rise in the number of organizations committed to combating the effect of such discrimination."[31] Finally, and most importantly, in Stage Three of the Progressive Theory, the aspirational ideas become binding, as nations collectively choose not to turn their back on the atrocities experienced and pain suffered, but instead to codify the recognition of specific rights to prevent similar future tragedies.[32] This Progressive Theory highlights the

25. Th importance of grassroots activism is a fundamental principle of the Progressive Theory. *Human Rights Activism and the Role of NGOs*, COUNCIL OF EUROPE, https://www.coe.int/en/web/compass/human-rights-activism-and-the-role-of-ngos [https://perma.cc/VL6T-JX69] (last visited Jan. 28, 2023).

26. United Nations Convention on the Elimination of All Forms of Discrimination against Women, Dec. 18, 1979, 1249 U.N.T.S. 13.

27. *Id.*

28. *Short History of CEDAW Convention*, UNITED NATIONS, https://www.un.org/womenwatch/daw/cedaw/history.htm [https://perma.cc/J85D-6NR7] (last visited Jan. 28, 2023).

29. *Id.*

30. *See An Introduction to Human Rights*, AUSTL. HUM. RTS. COMM'N, https://humanrights.gov.au/our-work/education/introduction-human-rights#Where%20do%20human%20rights%20come%20from? [https://perma.cc/RG6Y-ZD26] (last visited Jan. 28, 2023).

31. UNITED NATIONS, *supra* note 28.

32. Nancy Flowers, *From Concept to Convention: How Human Rights Law Evolves*, UNIV. OF MINN., http://hrlibrary.umn.edu/edumat/hreduseries/hereandnow/Part-1/from-concept.htm [https://perma.cc/SD2L-TZ9N] (last visited Jan. 28, 2023).

intersectional nature of human rights: as cultural norms change and new philosophical ideas gain popularity, political forces slowly take notice and, after sufficient advocacy following a human rights crisis, take action.

Extrapolating from this Progressive Theory must be done with discernment and care. There is no dearth of atrocities occurring in the world, but to push them all through this Progressive Theory may create what is called "human rights inflation," where recognizing too many human rights will lead to a devaluation of human rights as a whole.[33] One theory proposed in avoiding such inflation is that human rights "only deal with extremely important goods, protections, and freedoms."[34] This implies some threshold level of severity of the threat. One commonality among widely accepted human rights that deal with such extremely important needs is that they posed and continue to pose a threat so great and systemic that individuals require international legal protections.[35] To understand why facial recognition through AI poses a similarly great and systemic threat, it is essential to first understand the fundamental framework and incentive model of AI generally, and facial recognition specifically.

B. What Is Artificial Intelligence?

Although a ubiquitous term, AI's lack of a clear definition both infuriates and excites. The former is a common reaction among self-described realists and those less technologically inclined who have found no satisfying reason why the thing (AI) that they are expected to trust and rely on cannot be defined. The latter group, those excited by AI's lack of clear definition, would tell the realists that they still just don't get it. They would say that the evergreen promise of technology like AI is that it has the capacity, in the most theoretical terms, to transcend any form of subjectivity. To define it would be to prematurely limit its capabilities. They might suggest that popular understanding of AI is likely to go the way of the Internet: one cannot easily define the thing itself, but one can explain everything involved in it and around it until it is fully captured.

Etymologically, the term originated at Dartmouth in 1956, where scientists convened to test the theory that "every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it."[36] Sixty-seven years later, the technology has drastically improved and grown in complexity, but the aim remains the same.

---

33. *See Human Rights*, *supra* note 18.
34. *Id.*
35. *Id.*
36. *Artificial Intelligence (AI) Coined at Dartmouth*, DARTMOUTH COLL., https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth [https://perma.cc/85XS-QJYM] (last visited Jan. 28, 2023).

At its most technical level, an AI algorithm is a binary code of zeros and ones that analyzes other zeros and ones to give outputs.[37] Most technical communities, however, explain it simply as applying complex algorithms and systems to reach desired outcomes.[38] AI is often thought of not as a tangible thing in itself, but instead as a process by which data is analyzed.[39] An AI system "learns" through "training" on a particular set of data.[40] The process of AI learning is not relevant for purposes of this Note—which will focus on the data. Just as Peter Norvig, Google's Chief Scientist, said on the matter, "We don't have better algorithms than anyone else; we just have more data."[41] The more data that algorithms are trained on, the more accurate and efficient they become, creating a clear incentive for AI companies to gather as much data as possible.[42]

The pace of AI development is fundamental to understanding the power of the technology and why there is an imperative for legal action. All AI available today is considered Artificial *Narrow* Intelligence (ANI), meaning the system can complete one prescribed task but not much beyond that.[43] Containment of the problem (regulation of AI) is, therefore, relatively straightforward given the inherent limitations. However, technological developments of AI are headed for Artificial *General* Intelligence (AGI), "systems with general intelligence comparable to, and ultimately perhaps greater than, that of human beings." AGI is orders of magnitude more powerful and capable than ANI.[44] While in its current state, ANI poses a reasonably known and controllable threat given the simplicity of the technology, similar to food dye in a bottle. Once it progresses to AGI, the increase in relative difficulty in regulating it will be like trying to collect that food dye once it is poured into a bowl of water. It is therefore imperative to take legal action before this significant technological breakthrough.

To underscore this imperative, consider Stanford University's annual AI Index Report, which is useful in tracking both the rate of development of

---

37. *Zeros & ones: The fundamental building blocks of computing*, UNIV. OF OXFORD, https://atozofai.withgoogle.com/intl/en-US/zeros-and-ones/ [https://perma.cc/K8VA-6YYN] (last visited Jan. 28, 2023).

38. *How Does AI Actually Work?*, CSU GLOBAL (Aug. 9, 2021), https://csuglobal.edu/blog/how-does-ai-actually-work#:~:text=AI%20systems%20work%20by%20combining,performance%20and%20develops%20additional%20expertise [https://perma.cc/GA6Y-UTKJ].

39. Jeff Holmes, *The AI Process*, TOWARDS AI (May 18, 2022), https://towardsai.net/p/l/the-ai-process [https://perma.cc/BNJ3-6Q3W].

40. *Id.*

41. Ben Buchanan and Taylor Miller, *Machine Learning for Policymakers What It Is and Why It Matters*, HARV. BELFER CTR. FOR SCI. AND INT'L AFFS. 13 (Jun. 2017), https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf [https://perma.cc/25B6-YYZC].

42. *Artificial Intelligence Factsheet*, HARV. BELFER CTR. FOR SCI. AND INT'L AFFS. 2 (Jan. 2020), https://www.belfercenter.org/sites/default/files/2020-01/AI.pdf [https://perma.cc/D58C-9SRD].

43. *Id.*

44. Ben Goertzel, *Artificial General Intelligence: Concept, State of the Art, and Future Prospects*, J. OF ARTIFICIAL GEN. INTEL. 1 (2014), https://sciendo.com/downloadpdf/journals/jagi/5/1/article-p1.pdf [https://perma.cc/SMS6-BAPP].

AI and changing outlooks on its cultural and technological relevance.[45] The 2019 report crucially noted that, "[p]rior to 2012, AI results closely tracked Moore's Law, with compute[46] doubling every two years. Post-2012, compute has been doubling every 3.4 months."[47] The more compute ability increases, the more concentrated technological power becomes. The significance of this is that it creates an imperative for action to address this massive leap in technology. As will be explored in later sections, activists are sounding the alarm about the potential for harm that is festering in the gap between societal expectations around FRT and the existing legal system.

Stanford's 2022 AI Index Report solidifies this imperative for action.[48] Among other rapid developments, the report cites a significant increase in global legislation and the demand for formal AI ethics, both coinciding with a general realization of the increasingly severe risks posed by AI.[49] A prime example of why both legislation and ethics are crucial to AI is the reaction to ChatGPT beginning with its debut on November 30, 2022.[50] ChatGPT is an AI model that uses a massive amount of data that is organized in a neural network.[51] The neural network essentially means that ChatGPT can quickly understand writing and become very good at it, allowing the technology to answer questions and have conversations with users in a way that mimics human interactions.[52] Its astonishing capabilities underscore just how powerful such technology can be and how safeguards are in place to control it. While ChatGPT can help answer questions and recommend dinner recipes, it can also create "policy briefs, fake news reports or, as a Colombian judge has admitted, court rulings. Other models trained on images rather than text can generate everything from cartoons to false pictures of politicians."[53] The

45. *About*, STAN. UNIV., https://aiindex.stanford.edu/about/ [https://perma.cc/T9SU-X5YL] (last visited Jan. 28, 2023).

46. "Compute" is a "generic term used to reference processing power, memory, networking, storage, and other resources required for the computational success of any program." *What is Compute?*, AMAZON WEB SERVICES, https://aws.amazon.com/what-is/compute/ [https://perma.cc/LVN2-5H7C] (last visited Mar. 1, 2023).

47. Raymond Perrault et al., *The AI Index 2019 Annual Report*, STAN. UNIV. HUMAN-CENTERED A.I. INST. 5 (Dec. 2019), https://hai.stanford.edu/sites/default/files/ai_index_2019_report.pdf [https://perma.cc/5ZHA-SXP3].

48. *See* Daniel Zhang et al., *The AI Index 2022 Annual Report*, STAN. UNIV. HUMAN-CENTERED A.I. INST. 10-12 (Dec. 2022), https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf [https://perma.cc/A6EP-23DD].

49. *Id.*

50. Grace Kay, *Elon Musk founded — and has since criticized — the company behind the buzzy new AI chatbot ChatGPT. Here's everything we know about OpenAI.*, BUS. INSIDER (Dec. 11, 2022), https://www.businessinsider.com/history-of-openai-company-chatgpt-elon-musk-founded-2022-12 [https://perma.cc/RE53-QAPS].

51. Matt Crisara, *ChatGPT Is a 'Very Sophisticated Guessing Engine' That Probably Won't Steal Your Job*, POPULAR MECHANICS (Feb. 3, 2023), https://www.popularmechanics.com/technology/a42733497/how-does-chatgpt-work/ [https://perma.cc/WW8E-WAYV].

52. *Id.*

53. Gian Volpicelli, *ChatGPT broke the EU plan to regulate AI*, POLITICO (Mar. 3, 2023), *https*://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/ [https://perma.cc/ZTS3-2J7A].

U.S. Congress is scrambling to respond, heeding the "ills" that flowed from fast-growing unregulated social media companies.[54] So, too, is the European Union (EU) grappling with the implications of the pace of development of AI, as ChatGPT has forced lawmakers to revise their proposed Artificial Intelligence Act to include stricter requirements.[55] While fascinating in its current state, scientists and researchers do not believe that AI models have a sufficient substantive or ethical understanding of the responses they provide.[56]

The state of AI today is one of promise and hazard. The move from ANI to AGI, powered by this rapid pace of development, would mean a significant leap in technology that is largely inconceivable now. ChatGPT is a good example of what the leaps look like, and the U.S. and EU's flat-footed responses further prove why there is an imperative for proactive legal action.

C. Facial Recognition Technology and Biometric Data

Facial recognition falls under the broad umbrella of AI but includes unique characteristics and poses novel legal questions that warrant separate consideration. To begin technically, FRT transforms "an image of a face into a numerical expression" that can then be compared to other faces rendered into a numerical code.[57] FRT ". . . works by identifying and measuring facial features in an image. Facial recognition can identify human faces in images or videos, determine if the face in two images belongs to the same person, or search for a face among a large collection of existing images."[58]

FRT requires a separate consideration from AI generally because the use of the technology directly concerns humans in a way that is not present with other categories of AI. The direct concern involves human rights considerations in ways that will be explored in this Note.

While the specific *technology* utilizing facial recognition is a subsection of AI, the actual *data collected* belongs to the family of biometric data. The EU defined biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique

---

54. Grace Yarrow, *Democrat pushes Congress to get a jump on regulating ChatGPT*, THE HILL (Feb. 16, 2023), https://thehill.com/policy/technology/3862109-democrat-pushes-congress-to-get-a-jump-on-regulating-chatgpt/ [https://perma.cc/6HXF-KN5C].

55. Volpicelli, *supra* note 53.

56. Melanie Mitchell, *What Does it Mean for AI to Understand?*, QUANTA MAG. (Dec. 16, 2021), https://www.quantamagazine.org/what-does-it-mean-for-ai-to-understand-20211216/ [https://perma.cc/RG6F-P5KP]; *see, e.g.*, Breena R. Taira et al., *A Pragmatic Assessment of Google Translate for Emergency Department Instructions*, 36 J. GEN. INTERNAL MED. 3361, 3361-65 (2021).

57. William Crumpler and James A. Lewis, *How Does Facial Recognition Work? A Primer*, CTR. FOR STRATEGIC AND INT'L STUD. at 3 (Jun. 10, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210610_Crumpler_Lewis_FacialRecognition.pdf?VersionId=xdae_qQa80_Fimc1mzF3wxN6KIp.01Xg [https://perma.cc/SWN4-WVBR].

58. *What is Facial Recognition?*, AMAZON WEB SERVICES, https://aws.amazon.com/what-is/facial-recognition/#:~:text=It%20works%20by%20identifying%20and,large%20collection%20of%20existing%20images [https://perma.cc/USH6-SB4M] (last visited Jan. 28, 2023).

identification of that natural person, such as facial images or dactyloscopic [fingerprint] data."[59] The National Institute of Standards and Technology (NIST) has a similar definition: "[a] measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics."[60]

Facial images are distinct from other forms of biometric data for two reasons: one legal and practical, the other moral and philosophical.[61] The practical reason is that the taking of facial images and the use of facial recognition poses challenging questions regarding consent.[62] Unlike with, for example, a fingerprint, an individual does not always know when the biometric data of their face is being collected.[63] In fact, the U.S. Government Accountability Office (GAO) has raised this as a main concern around facial recognition since 2015: an individual's face can be recorded, and their movements tracked through FRT without their knowledge, much less consent.[64] This exponentially elevates the difficulty of protecting consumers in an already difficult and confusing realm of biometric data consent.[65]

The philosophical reason is that because so much of one's sense of individualism and humanity is tied to the face and its unique features, there is a moral inclination to regard it as a separate consideration from one's fingerprint or the sound of one's voice.[66] Recent biological research indicates that certain parts of the human brain have developed exclusively to identify faces.[67] The human face has also always been a foundational subject in art, literature, and academia.[68] Finally, arguments of philosophy have traditionally found a home in legal discussions regarding the consideration of

---

59. Council Regulation 2018/1725, Art. 3 2018 O.J. (L 295) 39 (EU).

60. Michael Nieles et al., *An Introduction to Information Security*, NATL. INST. STAND. TECHNOL. SPEC. PUBL. 800-12 REV. 1, 77 (Jun. 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf [https://perma.cc/WJX7-YGC2].

61. *See generally* Kelly A. Gates, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE (Sarah Banet-Weiser and Kent A. Ono eds., 2011).

62. *Id.* at 18.

63. *Id.*

64. *Id.* at 63; U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW (Jul. 2015).

65. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 64; *infra* notes 79-84.

66. Evan Selinger and Brenda Leong, *The Ethics of Facial Recognition Technology*, THE OXFORD HANDBOOK OF DIGITAL ETHICS (forthcoming) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3762185_code1279812.pdf?abstractid=3762185&mirid=1&type=2 [https://perma.cc/YVR2-8SQK].

67. Elizabeth Norton, *Identifying the Brain's Own Facial Recognition System*, SCIENCE (Oct. 23, 2012), https://www.science.org/content/article/identifying-brains-own-facial-recognition-system [https://perma.cc/4D2E-J3VX].

68. *See, e.g.*, Bernard Rhie, The Philosophy of the Face and 20th Century Literature and Art 1-14 (2005) (Ph.D. dissertation, University of Pennsylvania) (on file with Penn Libraries, University of Pennsylvania) (on file with author).

human rights, providing rationale when the law has not yet caught up to the collective moral understanding of a specific issue.[69]

Therefore, due to the legal issues surrounding consent in collecting facial images and the deep sense of humanity of the face, facial data should be considered significantly distinct from other forms of biometric data and therefore treated as such. This Note will address this point later.

D. Domestic and International Government Action

1. The United States Federal Outlook on Facial Recognition Technology

In July of 2023, the Biden-Harris Administration announced an agreement with seven large AI companies to implement AI safeguards, including impacts for FRT.[70] The announcement highlighting the principles of the commitment—safety, security, and trust—demonstrates the White House's outlook on AI generally.[71] To understand the U.S. government's outlook on FRT specifically, consider reports from the GAO from 2015 and 2020 on the commercial use of FRT and the White House's proposed Blueprint for an AI Bill of Rights.

The 2015 and 2020 GAO reports present a useful comparison across three distinct benchmarks on the state of FRT: (1) the technology's uses; (2) risks associated with FRT; and (3) existing federal law.[72] For the first benchmark, what is notable in the findings of the 2015 report is the admission of the extent of the unknowns, as well as the conclusion that, in practice, it is not used to identify unique individuals.[73] The report states, "Facial recognition technology can be used in numerous consumer and business applications, but the extent of its current use in commercial settings *is not fully known* . . . Some security systems serving retailers, banks, and casinos incorporate facial recognition technology, but the extent of such use at present *is not fully known*."[74]

---

69. Randy E. Barnett, *Why We Need Legal Philosophy*, 8 HARV. J. L. & PUB. POL'Y 1, 4-5, 9-10 (1985) (Foreword to the "Symposium on Law and Philosophy").

70. Fact Sheet, *The White House, Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, THE WHITE HOUSE (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/ [https://perma.cc/7CK3-PMZH]; Michael D. Shear, Cecilia Kang and David E. Sanger, *Pressured by Biden, A.I. Companies Agree to Guardrails on New Tools*, N.Y. TIMES (July 21, 2023), https://www.nytimes.com/2023/07/21/us/politics/ai-regulation-biden.html [https://perma.cc/QZX8-BF4U].

71. *Id.*

72. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 64, at 6, 10, 32; *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-522, FACIAL RECOGNITION TECHNOLOGY: PRIVACY AND ACCURACY ISSUES RELATED TO COMMERCIAL USES 13 (Jul. 2020).

73. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 64, at 6, 10, 32.

74. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 64.

The 2020 report, by comparison, highlights the expanded use cases of FRT in commercial settings to include the identification of unique individuals: "[T]he technology can be used to count people in stores, amusement parks, or waiting in lines . . . Retailers and others can use facial analysis to analyze emotions, gender, and age to deliver targeted signs or billboards."[75] The technology has many uses, including security, as a method of loss prevention in retail stores, or for venues to use at large events to identify previously-banned fans.[76] One major driver of the increased use of FRT is the financial services sector, where "wider adoption of facial recognition technology was bolstered, in part, by regulatory changes included in the European Union's payment services regulation . . . [T]his regulation requires strong user authentication for payments which includes two-factor authentication—one of which can be biometric, such as face recognition."[77]

For the second benchmark, the 2015 report's characterization of the risks illustrates a situation that seems firmly planted within the first stage of the previously mentioned Progressive Theory: "Privacy advocacy organizations, government agencies, and others have cited several privacy concerns related to the commercial use of facial recognition technology."[78] Foundational to these risks is the difficulty in consent: "[I]f its use became widespread, it could give businesses or individuals the ability to identify almost anyone in public without their knowledge or consent and . . . that [the data] could be used, shared, or sold in ways that consumers do not understand, anticipate, or consent to."[79] The lack of consent and threat of use beyond consent are just a couple of examples of the different angles from which advocacy groups are sounding the alarm on the potential human rights threat of FRT.

The 2020 report highlights two key risks of FRT, the first previously mentioned in the 2015 report, the second a new conclusion based on ongoing research: privacy and inaccuracy concentrated in specific demographic groups.[80] Inaccuracy can mean one of two types of misidentification: a false positive, where the technology "incorrectly declar[es] two images to be a match when they are actually from two different people," and a false negative, where the technology "fail[s] to declare two images to be a match when they are actually from the same person."[81] The inaccuracy report for FRT underscores the inherently intersectional nature of the technology, further proving the danger it could pose to certain individuals (emphasis added):

> [A]lgorithms performed more accurately on white males. White males had the lowest false positive rate . . . while black females had the highest false positive rate. In verification algorithms, false positive rates for white males and black

75. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72, at 13.
76. *Id.* at 11.
77. *Id.* at 10.
78. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 64.
79. *Id.*
80. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72.
81. *Id.* at 26.

> females varied by factors of 10 to more than 100, meaning the lowest-performing algorithm could be *over 100 times more accurate* on white male faces than on black female faces. Additionally, for verification and identification vendor tests, false positives were higher for women than men.[82]

The consequences of misidentification range from mild (being incorrectly blocked from accessing a building) to traumatic (an anti-theft system misidentifying a shopper as a previous shoplifter based on some combination of their age, race, and gender).[83]

Similar to the 2015 report, the 2020 privacy concerns focus on data collection and consent.[84] The most obvious privacy risk identified is when facial and biometric data is collected entirely without consent.[85] The 2020 report details other risks unknown at the time of writing the 2015 report, as well as analyzes previously known risks with a more thorough understanding of consequences, both of which point to a more nuanced understanding of the potential privacy violations, as well as the severity of the risk.[86] While knowledge of risks is still insufficient to protect citizens, it indicates that the U.S. government may be primed for meaningful action.[87]

One such novel risk covered is when data is collected with the individual's consent for one use, but the actual use exceeds that consent, also known as "secondary use."[88] Another is the practice known as "web scraping," where companies will "scrape" the web for individual consumer data, often including location data collected by apps, without the knowledge or consent of the data owners.[89] This will be explored in more detail later in this Note when discussing the company Clearview AI. There is also the risk of aggregating facial data with other parts of the image:

> [T]hese data sets may include or reveal personal information beyond the individual's image . . . The data sets contain information that could potentially be identifiable, because . . . two surveillance camera data sets included data on the time and day of the week of collection, and the data set titles and publication information also included locations where the images were taken.[90]

Web scraping represents another angle from which advocacy groups are warning of the human rights threat posed by FRT: "Several privacy advocacy groups and academics have raised concerns that location and time

82. *Id.*
83. *Id.* at 31.
84. *Id.* at 14.
85. *Id* at 1.
86. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72.
87. *See id.* at 38-44.
88. *Id.* at 15.
89. *Id.*
90. *Id.* at 20.

data could allow individuals in anonymous data sets like these to be identified."[91]

Finally, the 2020 report mentions another privacy issue regarding reference data sets: nonpublic data sets that companies hold containing highly sensitive personal information tied to biometric data, such as one's face.[92] The use of reference data sets—with no public to answer to nor regulation imposed on data collection and storage—is a significant privacy concern: "[R]epresentatives of one financial institution we spoke with said that they stored member identification numbers with the biometric information linked to their account, and a privacy advocacy group said that location data may also be commonly collected in reference data sets."[93]

For the final benchmark, the 2015 report looks to the (nearly nonexistent) state of federal law: "No federal privacy law expressly regulates commercial uses of facial recognition technology, and laws do not fully address key privacy issues stakeholders have raised, such as the circumstances under which the technology may be used to identify individuals or track their whereabouts and companions."[94] However, there are certain laws "… governing the collection, use, and storage" of personally identifiable information that may apply to FRT in certain contexts such as data "… collected by health care entities or financial institutions."[95]

The state of federal law in 2020 is largely the same as it was in 2015: limited to data protection through orthogonal channels and lacking any comprehensive structure to protect consumers.[96] The two risks mentioned in the 2020 report, inaccuracy and privacy, demonstrate two major fundamental issues with the technology that have a disparate impact and are not being addressed in any meaningful way by the U.S. government.[97] The report does, however, highlight one promising avenue of individual protection: state law.[98] A handful of states have adopted laws protecting the collection and use of biometric data, with Illinois's Biometric Information Privacy Act (BIPA) as the most thorough.[99] However, a patchwork of state regulations is insufficient because the protection of national citizens becomes unequal and allows for strategic business practices to avoid liability.[100]

The 2020 GAO report is an effective comparison of growth in knowledge and technological capability to the 2015 report, referencing its own findings relative to those of the prior report.[101] Analyzed along the same three benchmarks—use cases, risks, and federal law—the 2020 report indicates the current U.S. government has a better understanding of the

91. *Id.*
92. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72, at 14.
93. *Id.* at 22.
94. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 64.
95. *Id.*
96. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72, at 39.
97. *See id.* at 24-25, 38-39.
98. *Id.* at 42.
99. *See id.*
100. *See id.* at 42, 44.
101. *Id.* at 1, 8, 11.

technology than it did in 2015, as well as heightened suspicion.[102] However, the gap created by the risks mentioned, where threats to human rights are proliferating with little to no intervention by the government or private actors, has all the telltale signs that FRT has already reached the first stage in the Progressive Theory.[103]

In October 2022, the White House published a 73-page Blueprint for an AI Bill of Rights, putting forward key principles that should guide the creation, implementation, and use of AI.[104] The five principles are (1) protecting people from unsafe or ineffective automated systems, (2) preventing discrimination by algorithms, (3) safeguarding people from abusive data practices and giving them agency over how their data is used, (4) informing people that an automated system is being used, and (5) letting users opt out of automated systems.[105] The Blueprint, while ambitious, remains nonbinding and aspirational, appealing to ideas instead of suggesting practical steps.[106] In response to the Blueprint, the former chief executive of Alphabet Inc.'s Google, Eric Schmidt, said, "I would not regulate things until we have to."[107] As will be explored in the next section, there is little to no incentive for companies to slow the pace of development through self-regulation, barring a government mandate.

In the context of its peers, the White House's Blueprint leaves much to be desired by activists. GDPR presents an unflattering comparison, as it authorizes significant fines for companies that are not in compliance with its strict regulations and limits the amount and ways companies may collect data.[108] GDPR's success in holding tech companies accountable provides a useful framework for the White House in crafting future regulatory recommendations.

Another comparison is Stanford University's Institute for Human-Centered Artificial Intelligence "AI Bill of Rights," published months before the Blueprint and with far more specific guiding principles and suggested areas of further exploration.[109] The Institute's research and publications are innovative and influential given their emphasis on the role of human-centered

---

102. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72.

103. *See supra* text accompanying note 25.

104. *Blueprint for an AI Bill of Rights*, WHITE HOUSE OFF. OF SCI. AND TECH. POL'Y 4 (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/43QK-3ZYH].

105. *Id.* at 5-7.

106. *Id.* at 2.

107. Angus Loten, *White House Issues 'Blueprint for an AI Bill of Rights'*, WALL ST. J. (Oct. 4, 2022), https://www.wsj.com/articles/white-house-issues-blueprint-for-an-ai-bill-of-rights-11664921544 [https://perma.cc/E7RQ-UQJB].

108. *Id.* GDPR is Europe's data privacy and security law. It was put into regulation in 2018.

109. Michele Elam & Robert Reich, *Stanford HAI Artificial Intelligence Bill of Rights*, STAN. UNIV. HUMAN-CENTERED A.I. INST. 1 (Jan. 2022), https://hai.stanford.edu/sites/default/files/2022-01/Stanford%20HAI%20Artificial%20Intelligence%20Bill%20of%20Rights_0.pdf [https://perma.cc/GQ2P-PDH7]. While this comparison is not one-to-one, given the relative constraints of a government versus a university, it is a useful benchmark.

AI in determining public policy.[110] Similar to GDPR, the White House can leverage this "Bill of Rights" in creating more robust recommendations by prioritizing a focus on ethics in future policies.

Actions taken at the federal level, including agency reporting and congressional calls for investigation into FRT, both inform the state of FRT in the U.S. and influence the future regulatory framework. As was explored in a prior section, the GAO has published detailed reports on the state of FRT and its commercial use. The knowledge gathered in these reports, as well as the relationships built with the private companies and non-governmental organizations that contributed, will be essential to informing future legislative action regarding FRT. More recently, in May of 2022, a group of congresspeople urged the Federal Trade Commission (FTC) to investigate the identity verification company, ID.me, for misleading comments made about their use of FRT.[111] The letter lays out a terrifying possibility: the company's use of data may have gone far beyond what users consented to, where "millions of innocent people will have their photographs endlessly queried as part of a digital line up."[112] The request makes clear the severity with which congresspeople are addressing the harms of unregulated FRT, as well as the influence of activists in calling out potential harms to privacy and human rights: this request followed mere weeks after activists, in conjunction with members of Congress, urged the Internal Revenue Service to halt their deployment of ID.me, citing privacy concerns in their use of FRT.[113]

2. Domestic Case Law

There have been few domestic cases involving the legal use of FRT given the nascency of the technology, but those that have arisen demonstrate both public sentiment about the use of the technology and the gravity of the risk the technology poses when unregulated.[114] A high-profile example came in 2020, following the publishing of the explosive exposé in the New York Times of a secretive company called Clearview AI which designed and deployed a nefarious facial recognition app.[115] Shortly afterward, eight

110. *See id.*

111. Letter from Senators Ron Wyden et al., to Lina Khan, Federal Trade Commission Chairperson (May 18, 2022), https://www.wyden.senate.gov/imo/media/doc/Letter%20to%20FTC%20on%20ID.me%20deceptive%20statements%20051822.pdf [https://perma.cc/Z8AK-XQMG].

112. *Id.*

113. Joseph Cox, *Lawmakers Urge FTC to Investigate ID.me and its Facial Recognition Tech*, VICE (May 18, 2022), https://www.vice.com/en/article/4awj7j/lawmakers-urge-ftc-to-investigate-idme-and-its-facial-recognition-tech [https://perma.cc/EEU5-V4ME].

114. Andrew Blancher, *An Analysis of Facial Recognition Technology Lawsuits*, VERISK (Nov. 30, 2022), https://www.verisk.com/insurance/visualize/an-analysis-of-facial-recognition-technology-lawsuits/#:~:text=In%202019%2C%20plaintiffs%20filed%20a,and%20receive%20a%20written%20release.&text=The%20plaintiffs%20alleged%20that%20they,use%20of%20their%20biometric%20data [https://perma.cc/SHR5-QXPD].

115. 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/W8HW-DZZP].

separate class action suits were filed against Clearview AI, with each case arising out of "Clearview's conduct in: (a) allegedly scraping billions of facial images from the Internet; (b) performing facial scans of those images; and (c) creating a biometric database that allows users of the database to immediately identify a member of the public merely by uploading a person's image to the database."[116]

This collection of cases (which, as of this writing, is still in litigation) demonstrates three important consequences. The first is the severity of the impact on the end user. Individuals are effectively helpless in preventing their face, and therefore their identity, from being added to these massive databases, which can be sold and used for any number of purposes with no clear repercussions. Second, the Illinois Northern District Court ruled that the plaintiffs had "sufficiently alleged that defendants' disclosure of their private information without their consent caused them the concrete harm of violating their privacy interests in their biometric data."[117] Identifying concrete harm under which to sue is a fundamental step in the creation of a legal scaffolding from which to build a regulatory framework. Finally, the causes of action in the respective cases against Clearview AI are brought primarily under state privacy acts, as there are no federal laws providing protection in facial recognition cases.[118]

The majority of the cases against Clearview AI, as well as the majority of facial recognition-related cases generally, have been successfully brought in Illinois under BIPA.[119] The Act "[p]laces restrictions on how private entities retain, collect, disclose, and destroy biometric identifiers and biometric data, and [r]equires companies to provide notice and obtain consent for collection, capture, purchase, or receipt of such data."[120] Most importantly, BIPA creates a private right of action for individuals, a right to which many activists credit the Act's success in suing large tech companies over their use of facial recognition.[121] Such private rights of action in issues of personal privacy are a useful but short-term, stop-gap tool. Many other states have passed similar, albeit less forceful, privacy acts, which provide some form of protection for individuals.[122] However, reliance on a patchwork of state laws is an insufficient solution. While the success of the Acts may help inform best

116. Calderon v. Clearview AI, Inc., No. 20 CIV. 1296 (CM), 2020 U.S. Dist. LEXIS 94926, at *5 (S.D.N.Y. 2020).

117. *In re* Clearview AI, Inc., Consumer Priv. Litig., 585 F. Supp. 3d 1111, 1126 (N.D. Ill. 2022).

118. Blancher, *supra* note 114; *Calderon*, 2020 U.S. Dist. Lexis 94926 at 8-10.

119. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72; *In re Clearview AI, Inc.*, 585 F. Supp. 3d at 8-10.

120. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 64.

121. Rachel Metz, *Here's why tech companies keep paying millions to settle lawsuits in Illinois*, CNN (Sept. 20, 2022), https://www.cnn.com/2022/09/20/tech/illinois-biometric-law-bipa-explainer/index.html [https://perma.cc/YH58-9S8G].

122. States whose laws specifically cover biometric data include Arizona, Arkansas, California, Colorado, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, New York, North Carolina, South Dakota, Washington, Wisconsin, and Wyoming; U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72.

practices, a federal regulatory framework is necessary to provide equal protection.

This federal regulatory framework for FRT should build off common throughlines among the state laws mentioned above, executive orders, legislative statements, and, most importantly, international successes.

3. International Action

It is important to juxtapose the current state of U.S. policy with that of the EU. Technology does not respect borders, and FRT is no different. The EU has presented a far more robust and actionable plan in addressing not only AI generally but FRT specifically. Beginning notably with the passage of GDPR in 2016, the EU has put forward a white paper on how best to approach AI and passed an Act on regulating AI.[123]

Article 9 of the GDPR lays out a key principle of the regulation, which explicitly prohibits the processing of "biometric data for the purpose of uniquely identifying a natural person" without the individual's explicit consent.[124] Article 22 goes even further, giving individuals the right "not to be subject to a decision based solely on automated processing." This right has broadly been applied to cases utilizing FRT to prove that such technology must operate within clearly defined parameters.[125]

In 2020, as a follow-up to the successes and shortcomings of GDPR, the European Commission published a white paper on AI.[126] Not only does this paper more clearly define biometric data to include facial images, but it also concludes that "in accordance with the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards."[127] The paper then goes on to propose how the Commission might approach defining these justified uses.[128]

The Commission's work culminated in the previously mentioned proposed Artificial Intelligence Act in 2021.[129] What is most important about this Act is its objective: to create harmonized rules on AI in anticipation of its potential.[130] While simple, this objective recognizes not only the promise of the benefits of AI but also the importance of coordinated regulation to address the risks and negative consequences that individuals and society could face.[131]

---

123. *Infra* notes 126 and 129.

124. Council Regulation 2016/679 General Data Protection Regulation, 2016 O.J, (L 119) 1 (EU).

125. *Id.*

126. *Commission White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, COM (2020) 65 final (Feb. 19, 2020).

127. *Id.* at 22.

128. *Id.* at 16-18.

129. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021).

130. *Id.* at 1.

131. *Id.* at 1, 6.

A final consideration of relevant international action is the Ruggie Principles. Beginning in 2005 and unanimously endorsed by the United Nations Security Council in 2011, the Ruggie Principles were created as both a recognition of the further breaking down of siloes between business and human rights and as a workable mandate to nations and corporations of what the responsibilities of each might look like in protecting human rights.[132] Fundamentally, they are meant to encapsulate three guiding principles:

> (1) States' existing obligations to respect, protect and fulfill human rights and fundamental freedoms; (2) [t]he role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights; (3) [t]he need for rights and obligations to be matched to appropriate and effective remedies when breached.[133]

The Principles—31 in total, expanding on each of these three guiding principles—recognize, among other things, corporations as major stakeholders and influencers of human rights and their obligations to individuals.[134] While not yet explicitly applied to AI and FRT, these three main principles could potentially provide an existing framework for future international cooperation regarding the regulation of FRT.

While considerations of aspirational goals for AI and FRT on the international level are useful for this analysis, they cannot fully communicate the gravity of what is at stake for individuals. Beginning in 2017, reports came out about the Chinese government using FRT to monitor, track, and ultimately suppress the Uyghurs, a Muslim minority living in the western region of China.[135] This surveillance is one of the many atrocities committed by the Chinese government against the Uyghurs, including arbitrary detention and forced re-education camps, which many nations in the international community are calling a human rights crisis.[136] The technology, developed largely by local start-ups, engages in racial profiling to identify Uyghurs, bringing to life one of the fears of activists calling for regulation of the technology.[137] Reports continued to come out about how the Chinese

---

132. Special Representative of the U.N. Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) [https://perma.cc/9KC2-6T5N].

133. *Id.*

134. *Id.*

135. Lindsay Maizland, *China's Repression of Uyghurs in Xinjiang*, COUNCIL ON FOREIGN RELS. (last updated Sept. 22, 2022), https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights [https://perma.cc/NS5P-859R].

136. *Id.*

137. 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/SL56-Q65Xv].

government exploited the group by setting up "U[y]ghur alarms"[138] and testing new software on them to detect emotions.[139] In recognizing the gravity of the human rights violations, the U.S. and many other nations and organizations formally recognized the actions taken against the Muslim Uyghur population as genocide.[140] For purposes of this Note, the fundamental point is that at the end of all the technology and legislative formal discussions and writings, there are individuals whose fundamental rights are at risk.

III. THE RIGHT TO PRIVACY OF ONE'S FACIAL BIOMETRIC DATA SHOULD BE CONSIDERED A HUMAN RIGHT

The use of FRT poses a great and systemic risk to individuals worldwide and violates deeply held notions of humanity. One's facial biometric data is unique and inherently individualistic data. Individuals should have the right to such data as a protected and codified human right. The best way to codify such a right is through domestic legislation, executive action, and international agreements, specifically by applying the Ruggie Principles to facial recognition.

A. Biometric Data as a Civil Human Right

As stated above, biometric data refers generally to personal data based on measurable physical or behavioral characteristics that are used to identify an individual, including facial images and fingerprints.[141] The use of this data to identify a specific individual threatens, and by the same token is protected by, the civil and political human rights as agreed upon in the International Covenant on Civil and Political Rights (ICCPR).[142] The use of biometric data arbitrarily or unlawfully—that is, without proper consent or knowledge—directly violates the basic rights protected by the ICCPR, and therefore, the right to one's own biometric data should be considered a civil human right.

As in previous sections, discussion of the category of biometric data generally leads to the focus on facial images and the use of FRT specifically. There are two compelling reasons to regard facial images as significantly distinct and worthy of separate consideration. The first is legal, that this specific biometric data can be captured without one's knowledge and therefore raises unique issues of consent.

---

138. Dres Harwell & Eva Dou, *Huawei tested AI software that could recognize Uighur minorities and alert police, report says*, WASH. POST (Dec. 8, 2020), https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/ [https://perma.cc/WFT9-N8YU].

139. Jane Wakefield, *AI emotion-detection software tested on Uyghurs*, BBC (May 26, 2021), https://www.bbc.com/news/technology-57101248 [https://perma.cc/QZ2W-7KE7].

140. Press Statement, U.S. Department of State, Determination of the Secretary of State on Atrocities in Xinjiang (Jan. 19, 2021), https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/index.html [https://perma.cc/9Y67-G3XC]; Maizland, *supra* note 135.

141. *See supra* notes 58-59.

142. *See supra* notes 21-23.

The second reason is more philosophical: one's face is so deeply tied to one's individualism and humanity that it must necessarily be regarded separately. The philosophical appeal is made to the moral sense of self and identity—ideas that are not unheard of in discussions of human rights.

These arguments are also bolstered by the sense of unease and the cultural reaction to exploitations that occur using FRT, most notably the mass injustice inflicted on the Uyghurs, such that the exploitation upends some deeply held notion of humanity, and the law has not yet caught up to punish this specific violation of human rights. For these reasons, facial image biometric data should be considered significantly distinct from other forms of biometric data and should receive heightened protection.

The heightened protection afforded to facial image data should be its recognition as a human right. The ICCPR occupies the field of civil human rights: adopted in 1966 with 173 state parties and a further six signatories, it sets out widely accepted norms of international human rights that continue to wield influence.[143] It is grounded in ideas of certain freedoms and liberties endowed to individuals. Given the date of its writing, it is not too radical to imagine it might need to act as a malleable instrument for human rights lawyers facing technological exploitations unforeseeable in the mid-20th century. The freedom from surveillance, from having facial image biometric data collected without one's knowledge or consent, is a natural extension of the freedoms stated in the ICCPR and should, therefore, be a human right.

If so recognized, this right should be clearly codified through domestic legislation and executive action, as well as international agreements to ensure individual protection and to promote ethical private commerce.

If the right to privacy of one's facial biometric data is not recognized as a human right, it has, at the very, least reached Stage One of the Progressive Theory. Therefore, it is crucial to enact domestic legislation and executive action, as well as international agreements, in order to ensure individual safety and to prevent a human rights crisis. Good human rights lawyers are good historians, and good humans know it is far preferable to prevent a crisis than to repair the damage after one occurs.

The warnings from activists can be heard domestically and internationally. Domestically, they can be heard from both citizens who are filing lawsuits against companies unfairly using their facial data, as is seen in the class action suits against Clearview AI,[144] as well as from activists urging the GAO to research FRT and urging Congress to investigate specific companies' use of facial data.[145] Internationally, multiple governing bodies have acted to address the threat of FRT. The EU has enacted multiple pieces of legislation to address the risks and existential threats posed by AI and

143. Interactive Dashboard, *Status of Ratification* (from dropdown menu under "Select a treaty", select "International Covenant on Civil and Political Rights), https://indicators.ohchr.org/ [https://perma.cc/E64T-ABJV] (last visited Jan. 28, 2023); International Covenant on Civil and Political Rights, *supra* note 22.

144. Hill, *supra* note 115; *Calderon*, 2020 U.S, Dist. Lexis; *In re Clearview AI Inc.*, 585 F Supp. 3d; Blancher, *supra* note 114; U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72.

145. Letter from Senators Ron Wyden et. al, *supra* note 111; Cox, *supra* note 113.

FRT.[146] Finally, nations have responded in alarm to the atrocities committed against the Uyghur population in China that are facilitated by FRT, with many formally referring to it as genocide.[147] Taken collectively, these pieces of evidence point to disruption in the global understanding of humanity. As governments and non-governmental organizations (NGOs) look for solutions, one glaring issue they must face is the misalignment of incentives for companies who create and use FRT.

B. Business Incentives in Facial Recognition Technology

John Ruggie opened his 2007 report to the United Nations Human Rights Council by stating, "[t]here is no magic in the marketplace. Markets function efficiently and sustainably only when certain institutional parameters are in place."[148] One of the primary reasons FRT requires legal intervention in the form of regulation is because there is an inherent friction between corporate incentives and societal interests coupled with a severe imbalance of power. The major themes running through this divide are a capitalistic drive for power, collectivist issues mischaracterized as individual responsibility, and a patchwork governmental response.

Private companies are interested in collecting as much data as they can to better "train" their systems. Google's Chief Scientist Peter Norvig's sentiment is worth reiterating here: "We don't have better algorithms than anyone else; we just have more data."[149] This drive to collect more individual data is in contention with the strong public interest in data privacy and transparency around how consumer data is collected, stored, and used.[150] A benevolent hostile solution pushed by incentivized private companies is simply to shift the responsibility of protecting an individual's online data from the company to the individual in response to this systemic issue of the company's own making.[151] Private companies also justify the drive to collect data and improve their algorithms by appealing to the pathos of the noble pursuit of technological innovation: moving fast and breaking things in theory is exciting but in practice leads to unexpected outcomes and individual injury.[152] The tension between private and public interest necessitates

146. Council Regulation 2016/679, *supra* note 122; *Commission White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, *supra* note 124, at 1; *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts*, *supra* note 127, at 1-3.

147. Maizland, *supra* note 135; Press Statement, *supra* note 140.

148. Special Representative of the U.N. Secretary-General, *Business and Human Rights: Mapping International Standards of Responsibility and Accountability for Corporate Acts*, ¶ 1, U.N. Doc. A/HRC/4/35 at 3 (Feb. 19, 2007).

149. Buchanan and Miller, *supra* note 41.

150. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72.

151. Charlie Warzel & Stuart Thompson, *Tech Companies Say They Care*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/interactive/2019/04/10/opinion/tech-companies-privacy.html [https://perma.cc/W6FK-ZJ3F].

152. *Id.*; "Move Fast and Break Things" was the motto of Facebook up until 2014, when it was updated to "Move Fast with Stable Infrastructure." Speculation abounds as to the motivation for such a change.

government intervention to protect consumers, as has been done at the state level for consumer data privacy.

Another private interest running against public interest is that companies may gather and eventually sell facial data specifically and biometric data more generally without individuals' consent or in excess of the use cases the consumer can consent to—risks previously highlighted in the 2020 GAO report.[153] There is little to no business incentive for private companies to prioritize the best interest of consumers through self-imposed requirements of explicit consent for all use cases when consumers share their data.[154]

A perfect example of this inherent friction and severe imbalance of power is Clearview AI, the facial recognition software start-up mentioned above.[155] The incentive of an AI company is to collect data to "teach" its FRT to improve its accuracy and thus sell it to more customers.[156] The company is therefore incentivized to maximize data collection through much-maligned tactics, like web scraping.[157] On the other side, consumers want restrictions placed on such tactics and to have control over their own data and to not have their face, and thus identity, added to massive data sets.[158] There is an imbalance of power between individuals and Clearview, where Clearview can scrape the deepest corners of the web to gather individuals' data with no mechanisms in place for individuals to stop it.[159] This illustrates the frustrating trend mentioned above of tech companies benevolently suggesting individuals are responsible for fixing the systemic problems that the companies create.[160] Here, tech companies are careless with data; thus, it becomes scrapable and ends up in the hands of an unregulated start-up that can use and sell individuals' data without their knowledge.[161] As mentioned in the GAO reports, this web scrapping by companies allows for data to be used beyond what customers consented to or without their full knowledge of the potential downstream uses.[162] The self-help advice is therefore reductive and ultimately punishing to individuals. Therefore, the solution must be one that works towards protecting individual consumers and incentivizing businesses to be responsible with user data and disclosures.

---

153. Press Release, Federal Trade Commission, Biometric Information and Section 5 of the Federal Trade Commission Act 1-3 (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers [https://perma.cc/T74M-B7BR].

154. Alan McQuinn, *The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules*, INFO. TECH & INNOVATION FOUND. (Oct. 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/ [https://perma.cc/S7RK-T5WQ].

155. Hill, s*upra* note 115.

156. Buchanan and Miller, *supra* note 42, at 13-14.

157. *Id.*; Hill, *supra* note 115.

158. Buchanan and Miller, *supra* note 42, at 29-31.

159. *Id.*

160. *See supra* text accompanying notes 149-152.

161. Hill, s*upra* note 115.

162. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 72, at 15.

C. *Proposed Domestic and International Action*

Regardless of whether the right to privacy of one's facial biometric data is a bone fide human right or merely at Stage One of *becoming* a human right, both require the same solution: a framework of domestic legislation and executive action, in tandem with international agreements.

Domestically, the federal government should conduct research into FRT and its current commercial uses through executive agencies and the legislature. The executive branch should issue an executive order aimed at research and development of FRT that provides a mandate to executive agencies like GAO, FTC, and NIST to investigate and report on the state of FRT, existing business practices that utilize FRT, and consumer privacy risks. These reports should be treated like an iterative process, adjusting in scope and focus as the technology develops. The most important domestic action that needs to be taken is the passing of federal regulations around FRT. Such action should be informed by the above executive agency reporting, regular congressional hearings on developing technology, meetings with business leaders, and consultations with foreign governments who are also addressing the domestic threat of FRT. This legislation should use the relevant articles in the EU's GDPR on the right to privacy, the fundamental principles of the EU's AI Act, and Illinois's BIPA as scaffolding from which to build a federal regulatory scheme that creates clear guidelines for companies to ensure the safe collection, storage, and use of facial biometric data. Specifically, the legislation should include a private right of action similar to that in BIPA, which was the basis for the lawsuits against Clearview AI, to provide immediate remedies to individuals whose rights have been violated. The language of the legislation should also be sufficiently malleable to account for future developments in the technology and to allow for rapid response to technologies. The flat-footed response of the government to ChatGPT should serve as a sufficient incentive for such flexibility. Finally, the executive branch should explore creating a committee focused on AI ethics, partnering with private technology companies and technology ethicists to address the future of FRT and the proper handling of user data.

In tandem with the domestic framework, there should be an international effort, led by the EU and U.S., to further break down the silos of business and human rights. International change takes time, and so much of international cooperation is dependent on creating proper economic incentives for governments and transnational corporations. The optimal way of working towards the goal of international cooperation and the protection of this right is to utilize existing international law principles that can be applied to FRT to empower domestic governments, regional organizations, and global bodies to respond efficiently to violations of rights.

The best option to facilitate international cooperation is by applying the Ruggie Principles to AI and FRT, clearly defining the role of corporations in the protection of human rights. A notable aspect of these Principles that lends well to the nature of FRT is that the Ruggie Principles "reflect international

law obligations but propose no new ones."[163] The Ruggie Principles merely state commonly accepted ideas in a way that creates a coherent framework and ensures uniform applications. Similarly, recognizing the right to privacy of one's facial biometric data as a human right does not propose an entirely new human right but instead the extension of an existing framework (the right to privacy) to this new area of technology.

The three Guiding Principles (GPs) also provide an immediately applicable framework, which nations can use to address FRT. The first GP clearly explains the State's obligation "to respect, protect and fulfill human rights and fundamental freedoms," a concept common to many human rights treaties and conventions.[164] In application here, this GP would create a baseline understanding of the State's role in addressing FRT and protecting its citizens' rights to privacy. The second GP recognizes the special function business enterprises play in respecting and protecting human rights.[165] So many of the uses of FRT that could violate individuals' rights to privacy would be facilitated, knowingly or otherwise, by private businesses. Therefore, creating this positive obligation of business enterprises to respect and protect human rights would create a sizable incentive for companies to act with care when handling individuals' data and provide proper disclosures. These actions would be further incentivized by the third GP, which creates a need for the obligations stated in GPs one and two to be matched with an adequate remedy.[166] Not only would this language of an "adequate remedy" allow for changes to be made commensurate with the developing technology, but it would also give redress to individuals whose rights had been violated.[167]

The application of the Ruggie Principles would create a solid foundation upon which nations can build multilateral agreements regarding the regulation of FRT. As previously stated, technology does not respect international boundaries. In order to enact a robust system of regulation to protect individuals, there must be international cooperation regarding fundamental rights.

Any discussion of technology regulation, however, must mention the substantial barriers to its mere passage in the U.S. The 26 words of Section 230 of the Communications Decency Act of 1996 still heavily influence the fundamental business of massive technology companies like X (formerly "Twitter") and Google, as demonstrated in two Supreme Court cases heard in 2023 interpreting the Section.[168] A convenient argument is that the Principles, while influential and widely respected, were introduced twelve years ago and have not resulted in any major changes. However, such arguments of

---

163. John Ruggie, *A UN Business and Human Rights Treaty? An Issues Brief by John G. Ruggie*, HARVARD KENNEDY SCH. OF GOV'T (Jan. 28, 2014), https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/UNBusinessandHumanRightsTreaty.pdf [https://perma.cc/7HE6-U7N2].

164. U.N. Human Rights Council, *supra* note 132.

165. *Id.*

166. *Id.*

167. *Id.*

168. 47 U.S.C. § 230; *see generally* Twitter, Inc. v. Taamneh, 143 S. Ct. 1206 (2023); Gonzalez v. Google LLC, 143 S. Ct. 1191 (2023).

convenience do not recognize the importance of incremental change. International and domestic regulatory frameworks change over time to respond to developing technologies, and there are ample reasons to believe such changes are taking place now. In 2014, three years after debuting the Principles, John Ruggie penned a brief on a potential future business and human rights treaty.[169] In it, he explores the complexities involved in creating such a treaty, ending with the same refrain as that of the Principles: that this is "the end of the beginning."[170]

Since then, lawmakers have pushed forward. In February 2021, the U.N. Human Rights Council Intergovernmental Working Group on Transnational Corporations and Other Business Enterprises with Respect to Human Rights (Working Group) published the third revised draft of a business and human rights treaty.[171] In January 2023, Congressman Ted Lieu called for a federal agency dedicated to AI regulation.[172] Sam Altman, CEO of OpenAI and advocate for AI regulation, recently suggested lawmakers should have insight into the products and capabilities AI companies are building.[173]

While the problem of unregulated AI and FRT persists, commonly held beliefs have changed. John Ruggie wrote the Principles and his follow-up treaty brief with a look to a future that was ready to accept a business and human rights treaty. It seems that time has come.

IV. CONCLUSION

Human rights concerns are no longer in a silo to be observed as a tragic but noble cause; they are a quickly growing concern in nearly all areas of law. Most lawyers must, in some way, become human rights lawyers, and good human rights lawyers are good historians. They understand that the benefits of technological development are not shared equally and, without proper action, may result in crises of human rights. The development of AI, and specifically facial recognition technology, is the perfect embodiment of this principle.

FRT, through scanning faces without consent and collecting facial biometric data, upends a deeply held notion of humanity. Moral arguments aside, it poses significant legal concerns. Given the violation to privacy posed,

169. Ruggie, *supra* note 163.

170. *Id.* at 5.

171. U.N. Human Rights Council, *Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises*, U.N. Doc. A/HRC/49/65/Add.1 (Aug. 17, 2021), [https://perma.cc/F8J2-BRAL] (published on U.N. Digital Library Feb. 28. 2022 [https://perma.cc/JY3D-QQX7]).

172. Ted Lieu, *I'm a Congressman Who Codes. A.I. Freaks Me Out*, N.Y. TIMES (Jan. 23, 2023), https://www.nytimes.com/2023/01/23/opinion/ted-lieu-ai-chatgpt-congress.html [https://perma.cc/8HFC-GWA3].

173. On With Kara Swisher, *Sam Altman on What Makes Him 'Super Nervous' About AI*, N.Y. MAG. (Mar. 23, 2023), https://nymag.com/intelligencer/2023/03/on-with-kara-swisher-sam-altman-on-the-ai-revolution.html [https://perma.cc/PB92-3SB6] (Transcript of podcast).

the right to one's facial biometric data should be considered a human right. Indeed, there are several indicators supporting the conclusion that the right to one's facial biometric data is squarely within Stage One of the Progressive Theory and there is a significant possibility of a major human rights crisis in this area, large enough to spur international response out of a sense of loss and regret. In either scenario, the threat posed to individuals creates an imperative for a coordinated domestic and international response.