Notre Dame Journal of International & Comparative Law

Volume 12 | Issue 2 Article 3

2022

Bias and Biometrics: Regulating Corporate Responsibility and New Technologies to Protect Rights

Erika R. George
S.J. Quinney College of Law, University of Utah, erika.george@law.utah.edu

Bias and Biometrics: Regulating Corporate Responsibility and New Technologies to Protect Rights

Cover Page Footnote

Samuel D. Thurman Professor of Law, University of Utah S.J. Quinney College of Law and Director Tanner Humanities Center. Helpful research assistance was provided by Hannah Taub, Hannah Pickett, Beth Jennings, and Melissa Bernstein. I also benefitted from conversations with Frank Pasquale and Ruha Benjamin. Thank you to Veronica Root Martinez, Michael Addo, and Kish Parella. I thank Abigail Allen, Ijeoma Oti, Jenae Longnecker, and the other organizers of the Race & the Law: Interdisciplinary Perspectives symposium.

BIAS AND BIOMETRICS: REGULATING CORPORATE RESPONSIBILITY AND NEW TECHNOLOGIES TO PROTECT RIGHTS

ERIKA GEORGE*

INTRODUCTION

A growing body of literature has documented the ways in which algorithms and new technology are being deployed in ways that discriminate and violate human rights. The regulatory environment is still evolving, but not as rapidly as new technologies are being introduced by private corporations and implemented in public settings. Governments are using AI in immigration and asylum determinations and law enforcement, arenas where racism and xenophobia can often arise. In the aftermath of the racial justice uprisings following the murder of George Floyd, some technology firms pledged to reconsider providing surveillance technology to police without protections in place. This essay explains algorithmic discrimination, examines emerging international and comparative legal and public policy initiatives to regulate AI and evaluates private sector voluntary guidelines intended to regulate the use of technology to respect human rights.

There is a growing awareness of what researchers at the intersection of critical race theory (CRT) and science and technology studies (STS) have identified as "algorithmic discrimination."[1] Avoiding and addressing bias in the

---

* Samuel D. Thurman Professor of Law, University of Utah S.J. Quinney College of Law and Director Tanner Humanities Center. Helpful research assistance was provided by Hannah Taub, Hannah Pickett, Beth Jennings, and Melissa Bernstein. I also benefitted from conversations with Frank Pasquale and Ruha Benjamin. Thank you to Veronica Root Martinez, Michael Addo, and Kish Parella. I thank Abigail Allen, Ijeoma Oti, Jenae Longnecker, and the other organizers of the *Race & the Law: Interdisciplinary Perspectives* symposium.

1 *See, e.g.,* THE INTERSECTIONAL INTERNET: RACE, SEX, CULTURE AND CLASS ONLINE (Safiya Umoja

ways new technologies are designed and deployed and adopting rights-respecting approaches have yet to gain significant traction in certain sectors of the tech community.[2] To reduce the adverse impact of new technologies on disfavored populations subjected to discrimination, interdisciplinary approaches to identifying and addressing injustice will be essential. I propose that: (1) emerging regulatory frameworks be crafted consistent with the procedural guidance articulated in the UN Guiding Principles on Business and Human Rights; and (2) efforts to diversify decision-making and sensitize those responsible for design in the technology sector to the potential human rights risks presented by technology products be strengthened.

I. ENGINEERING INEQUALITY: BIOMETRIC BIAS AND DISCRIMINATION BY DEFAULT

Biometric technologies "are used to identify, verify, or confirm a person's identity based on their physiological…or behavioral…characteristics."[3] Biometric technologies such as voice, face, or fingerprint recognition software or DNA matching may be used by private parties, including individuals and corporations, for privacy and identity confirmation in transactions or by government entities in law enforcement, surveillance, or administrative purposes. These technologies have the potential to be extremely useful and convenient, but they also have the potential to perpetuate biases and place human rights at risk. Researchers have documented the ways in which biotech can create privacy concerns,[4] perpetuate racial and gender biases contributing to inequality,[5] and present concerns about autonomy, choice, and other fundamental rights.[6]

Given the rapid rate of technological advances, it would not be unreasonable to imagine that humanity should be more easily able to detect and reduce bias, but *In Race After Technology: Abolitionist Tools for the New Jim Code*, Ruha Benjamin, Professor of African-American studies at Princeton University demonstrates that the opposite may, in fact, be the case. New technologies that are promoted and perceived as more objective and progressive than subjective and discriminatory systems of the past yet still reflect and reproduce existing

---

Noble & Brendesha M. Tynes eds., 2016); Ruha Benjamin, *Catching Our Breath: Critical Race STS and the Carceral Imagination*, 2 ENGAGING SCI., TECH., AND SOC'Y, 155-156 (2016); Taylor Synclair Goethe, *Bigotry Encoded: Racial Bias in Technology*, REPORTER MAG. (Mar. 2, 2019) https://reporter.rit.edu/tech/bigotry-encoded-racial-bias-technology.

2 For a general discussion of critical race theory, see e.g., Derrick A. Bell, *Who's Afraid of Critical Race Theory*, 1995 U. ILL. L. REV. 893 (1995).

3 TAMBIAMA MADIEGA & HENDRICK MILDEBRATH, REGULATING FACIAL RECOGNITION IN THE EU 1 (2021),https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf.

4 *See. e.g.,* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK AND AUTOMATED DISCRIMINATION (David Lyon ed. 2003).

5 *See, e.g.,* LISA NAKAMURA, CYBERTYPES: RACE, ETHNICITY, AND IDENTITY ON THE INTERNET (2002); JESSIE DANIELS, CYBER RACISM: WHITE SUPREMACY ONLINE AND THE NEW ATTACK ON CIVIL RIGHTS (2009); Safiya Umoja Noble, *How Search Engines Amplify Hate—in Parkland and Beyond*, TIME, Mar. 9, 2018.

6 *See, e.g.,* ALAN RUBEL, CLINTON CASTRO & ADAM PHAM, ALGORITHMS AND AUTONOMY: THE ETHICS OF DECISION SYSTEMS (2021).

inequities are the tools of what Benjamin describes as a "New Jim Code."[7] Indeed, computer scientists have found that algorithms exhibit the same biased tendencies evident in humans.[8] Racial bias has found its way into predictive models reinforced by institutional inequities and implicit bias. Research conducted to support the development of inclusive AI design has identified five different types of bias that can corrupt AI systems: dataset bias, associations bias, automation bias, interaction bias, and confirmation bias.[9]

To fully appreciate the human rights risks raised by new technologies that are presented as objective and efficient means of informing decision making, but that may, in fact, reinforce racism and other forms of inequity contrary to international human rights standards, it is helpful to start with a few illustrative examples: surveillance technology and search engines.

A. *SURVEILLANCE TECHNOLOGY: BUILT-IN BIAS*

One of the most used biometric technologies, facial recognition, has proven especially problematic. The data sets used to teach AI systems influences how individuals from different groups are identified. Algorithms recognize faces contained in the data sets used by engineers to train the system. Algorithms in Asia recognized East Asian faces more readily than Caucasians; the opposite was true in Western Europe and the US.[10] Researchers have found that facial recognition software consistently performs less accurately on women and darker-skinned individuals.[11]

Researchers at Georgetown University's Center on Privacy and Technology found that disparities in the ability of technology to recognize faces can occur at different points in the design process. For instance, an engineer may program to focus on particular facial features such as the shape and size of a person's eyes or nose based on their own experience and exposure, which is influenced by the engineer's own race.[12] Another study conducted by Georgetown Law School examined data from over 100 police departments across the US to determine how the use of facial recognition software impacts different communities. The study revealed that the training databases used to develop software

---

7 RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 5 (2019).

8 *See, e.g.,* Joy Buolamwinni & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RES. 1-15 (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

9 Joyce Chou, Roger Ibars & Oscar Murillo, *In Pursuit of Inclusive AI* 9, MICROSOFT (last accessed April 8, 2022), https://www.microsoft.com/design/assets/inclusive/InclusiveDesign_InclusiveAI.pdf (Dataset bias occurs when data used to train machine learn models are not sufficiently representative. Association bias occurs when data used to train reinforces stereotypical cultural assumptions (e.g., doctors are men, nurses are women). Automation bias occurs when predictive programing overrides the aims of a system's human users. Interaction bias occurs when AI learns in a tainted or toxic context (e.g., intentionally racist, or sexist interaction with a system to taint bots and computer programs). Confirmation bias occurs when AI interprets information to confirm preconceptions and reinforce popular preferences based on assumptions about a group or individual (e.g., algorithms do not offer contrasting views)).

10 Benjamin, *supra* note 7, at 112.

11 Alex Najibi, *Racial discrimination in Face Recognition Technology*, HARV. BLOG (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

12 Benjamin*, supra* note 7, at 113 (citing Clare Garvie & Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, THEATLANTIC, (April 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/).

disproportionately contained images of African Americans. Still, the software performed poorly in distinguishing between different Black people. This poor performance is a problem when police departments and private security increasingly depend on "digital eyes" trained on incomplete or inaccurate data.[13]

Facial recognition has been used in questionable ways that violate human rights, most notably in the US and in China. In the US, technology companies contract with federal agencies and other state or local police departments to provide data management and identification services. A 2018 report by the National Immigration Project of the National Lawyer's Guild, Immigrant Defense Project, and Mijente (a digital grassroots hub for the Latinx Community) identified Amazon and Palantir as industry leaders in the collection, management, storage and provision of the massive amount of personal information that Immigration Customs Enforcement (ICE) and the Department of Homeland Security (DHS) use to expand data-sharing capabilities in ways that "undermine and get around any local protections that were hard-fought and won by immigrant rights organizers."[14] Palantir makes case management software for ICE and other law enforcement agencies enabling information access across different government departments. Amazon holds more federal authorizations to maintain government data from government agencies than any other tech company.[15]

China is a global leader in designing and deploying biometric technologies to engineer behavior and limit autonomy.[16] The country's pervasive system of surveillance relies on the use of facial recognition technology to track and target its citizens.[17] The Chinese government has been criticized for its use of facial recognition technology against peaceful protesters in Hong Kong.[18] China has also been condemned for its use of biotech to racially profile, regulate, and marginalize Uyghurs and other ethnic and religious minorities.[19] In addition to forced political indoctrination, mass DNA collection and analysis, and mass arbitrary detention of these "sensitive groups of people,"[20] the Chinese government has used technology to make repression more efficient and effective by enforcing restrictions on the movements of Uyghurs and other Turkic Muslim

---

13 Benjamin, *supra* note 7, at 77.

14 NATIONAL IMMIGRATION PROJECT OF THE NATIONAL LAWYER'S GUILD, IMMIGRANT DEFENSE PROJECT, MIJENTE & EMPOWERLLC, WHO'S BEHIND ICE? THE TECH AND DATA COMPANIES FUELING DEPORTATION 3 (2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations_v3-.pdf

15 *Id.* at 5.

16 Alfred Ng, *How China Uses Facial Recognition to Control Human Behavior*, CNET (Aug. 11, 2020, 5:00 AM), https://www.cnet.com/news/politics/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/.

17 *Id. See also*, Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using AI 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.

18 Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, N. Y. TIMES (Jul. 26, 2019), https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

19 Lora Korpar, *U.S. Imposes Sanctions on Chinese Biotech, Surveillance Companies Over Abuse of Uyghurs*, NEWSWEEK (Dec. 16, 2021, 1:19 PM), https://www.newsweek.com/us-imposes-sanctions-chinese-biotech-surveillance-companies-over-abuse-uyghurs-1660222.

20 Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using AI 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.

minorities at "data doors"—checkpoints connected to Xinjiang's Integrated Joint Operations Platform (IJOP).[21]

Technology transfer, a desirable end to advance development and contemplated in many international instruments to advance sustainable economic development, takes on a sinister turn worthy of more scrutiny when designed and deployed by authoritarian regimes on an unsuspecting populace. In 2018, the Zimbabwean government contracted with a China-based company to create a population-wide recognition program, enabling the tracking of millions of Zimbabwean citizens while expanding the data set available for Chinese AI to improve identification of different ethnicities.[22] This type of technology transfer is an alarming development, in part, because, as Benjamin explains: "the biggest application of facial recognition is in the context of law enforcement and immigration control[;] Zimbabwe is helping Chinese officials to become more adept at criminalizing Black people within China and across the African diaspora."[23]

B. *SEARCH RESULTS: DISCRIMINATION, DISINFORMATION, AND DEMOCRACY*

Beyond biometric technologies, information technology also can present human rights risks by perpetuating and amplifying harmful racist stereotypes. Platforms personalize search results using prior search history and demographic information to generate results for viewers to see based on what Google search thinks advertisers want to target. Content is customized. In *Algorithms of Oppression: How Search Engines Reinforce Racism*, MacArthur Genius Safiya Umoja Noble recounts a chilling example of the consequences of an ecosystem of algorithmic power that holds a monopoly on public information with the power to shape perceptions tracing the online self-education and evolution of the White nationalist mass shooter Dylann Roof's thinking about race relations.[24] In 2015, Roof entered the Mother Emanuel African Methodist Episcopal Church during a bible study session and committed a racial and religious hate crime when he shot fourteen Black people, killing Reverend Clementa C. Pinckney and eight members of his congregation.[25] The massacre, in the mass murderer's own words, was motivated by his belief that Black people presented a dangerous threat based on information he found while searching for "Black on White Crime."[26]

---

21 Maya Wang, *The Robots Are Watching Us*, PEN/OPP (Apr. 6, 2020), https://www.penopp.org/articles/robots-are-watching-us?language_content_entity=en; HUMAN RIGHTS WATCH, CHINA'S ALGORITHMS OF REPRESSION: REVERSE ENGINEERING A XINJIANG POLICE MASS SURVEILLANCE APP (2019), https://www.hrw.org/sites/default/files/report_pdf/china0519_web.pdf.

22 Linsey Chutel, *China is exporting facial recognition software to Africa, Expanding its Vast Database*, QUARTZAFRICA, (May 25, 2018), https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/.

23 Benjamin, *supra* note 7, at 82.

24 Safiya Umoja Noble, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 110-118 (2018).

25 *See* Dennis Romero & Anthony Cusumano, *Death Sentence Upheld for Dylann Roof, Who Killed 9 South Carolina Church Shooting*, NBC NEWS (Aug. 25, 2021, 11:27 PM), https://www.nbcnews.com/news/us-news/death-sentence-upheld-man-who-killed-9-south-carolina-church-n1277667; Rachel Kaadzi Ghansah, *A Most American Terrorist: The Making of Dylann Roof*, GQ (Aug. 21, 2017), https://www.gq.com/story/dylann-roof-making-of-an-american-terrorist)

26 Noble, *supra* note 24, at 111.

Instead of FBI crime statistics on violence or information to dispel stereotypes disseminated by racist and white supremacist organizations, Roof's search returned the website of the Council of Conservative Citizens (CCC) along with other fascist, racist, anti-Semitic and anti-Black materials. The Southern Poverty Law Center (SPLC), a racial justice public interest legal organization that monitors hate groups, has identified the CCC as the modern reincarnation of White Citizens Councils.[27] Roof wore a jacket bearing the flags of Apartheid-era South Africa and White ruled Rhodesian to signify his solidarity with ideologies of racial hierarchies.[28] While she acknowledges that it is difficult to draw a direct line from search results to serial murder, Noble nonetheless presents a compelling case that we ignore search engine optimization algorithms that optimize hate to our peril.

In *Beauharnais v. Illinois*, 343 US 250 (1952), Justice Frankfurter provides powerful insights on the dangerous implications of racist hate speech "directed at designated collectivities" instructive for our present moment and amplification of abuse over social media and search engines.[29] Beauharnais, president of the White Circle League, organized the distribution of leaflets and petitions calling on "self respecting white people" to "unite" in order to "halt the further encroachment, harassment and invasion of white people, their property, neighborhoods and persons, by the Negro" and "prevent the white race from becoming mongrelized by the Negro."[30] He was convicted under a state statute making it unlawful to distribute any publication that "portrays depravity, criminality, unchastity, or lack of virtue of a class of citizens, of any race, color, creed or religion, which [publication] exposes the citizens of any race, color, creed or religion to contempt, derision, or obloquy or which is productive of a breach of the peace or riots" for stereotyping African Americans as a group as criminals responsible for "aggressions, [rapes], robberies, knives, guns and marijuana…" in his leaflet. Writing for the Court to affirm the conviction, Justice Frankfurter cited a long history of racial tensions often preceded by "extreme racial and religious propaganda" that is "calculated to have a powerful emotional impact" and explained the nature of the social and esteem injuries experienced by members of a targeted group noting that "the dignity accorded him may depend as much on the reputation of the racial and religious group to which he willy-nilly belongs, as on his own merits."[31] In the digital age, defamation of a group and repeated exposure to disinformation and stereotypes is perhaps more powerful.

Search result rankings reflect valuation and cultural values and can influence thought and inspire or impede action. Information access has implications for equal opportunity and public participation. The American Civil Liberties Union (ACLU), the Lawyers' Committee for Civil Rights Under Law,

---

27 Noble, *supra* note 24, at 111-117. According to the SPLC, hate groups hold beliefs or practices that malign or attack an entire class of persons usually based on immutable characteristics; for an updated list of hate groups based in the US, *see also*, Southern Poverty Law Center, Hate Map (2021) https://www.splcenter.org/hate-map.

28 Zack Beauchamp, *The Racist Flags on Dylann Roof's Jacket Explained*, VOX (Jun. 18, 2015, 1:50 PM), https://www.vox.com/2015/6/18/8806633/charleston-shooter-flags-dylann-roof (reporting "the lesson of Rhodesia, for white supremacists, is that black people are a threat to a healthy, white-run society. And they need to be kept down.")

29 Beauharnais v. Illinois, 343 US 250, 258 (1952).

30 *Id.* at 252.

31 *Id.* at 251-63.

the National Fair Housing Alliance, and other organizations allege that social media platforms that use personal data to target advertising based on race, gender and other protected categories are engaging in "digital redlining" to effectively excluding historically disadvantaged and disfavored groups from housing, credit, and employment opportunities.[32] For example, Facebook's ad delivery algorithm determines what users will see based on predictions using data about what they post or "like," what groups they join, where they live, and who they engage with regularly which allows advertisers to select who can and cannot see certain information. The ACLU's action before the Equal Employment Opportunity Commission (EEOC) on behalf of a class of millions of women who were excluded from learning about job opportunities in predominantly male industry sectors because of targeted ad practices did prompt Facebook to agree to changes including removing the ability of advertisers to discriminate in targeted advertising.[33] Still, civil rights organizations point to evidence that ad-delivery continues to be biased and maintain that companies should be accountable for digital discriminatory exclusion.[34]

Researchers have documented how targeted disinformation can change preferences and incentives in ways that alter election outcomes. As early as 2013, a study by the American Institute for Behavioral Research and Technology found that the manipulation of search rankings could significantly alter the preferences of voters without voters being aware that their search results were being manipulated.[35] Investigations of Russian government interference in the 2016 US Presidential elections found that Russian organizations conducted social media campaigns specifically targeted at audiences on Facebook and Twitter with the aim of "sowing discord in the US political system."[36] A Senate Intelligence Committee report found "race and related issues were the preferred target of the information warfare campaign" as Russia exploited America's existing racial divisions.[37] Voting rights activists have compared targeted disinformation on social media to past voter suppression strategies like poll taxes and literacy tests that operate to depress turnout among voters of color.[38]

---

32 Linda Morris and Olga Akselrod, *Holding Facebook Accountable for Digital Redlining*, ACLU (Jan. 27, 2022). https://www.aclu.org/news/privacy-technology/holding-facebook-accountable-for-digital-redlining (announcing amicus briefs in *Vargas v. Facebook* and *Opiotennione v. Bozzuto Management Company* — lawsuits filed by individuals who were excluded from viewing housing ads on Facebook based on protected characteristics.)

33 *Id*.

34 *Id*.

35 Noble, *supra* note 24, at 52-53.

36 SPECIAL COUNSEL ROBERT S. MUELLER, III, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION VOL. I OF II 14 (2019), https://www.justice.gov/archives/sco/file/1373816/download.

37 Alex Ward, *A GOP-led Senate intel committee report states the obvious: Russia favored Trump in 2016* (Oct. 8, 2019), https://www.vox.com/2019/10/8/20905160/senate-intelligence-russia-2016-election; *see also* Tim Mak, *Senate Report: Russians Used Social Media Mostly to Target Race in 2016*, NPR (Oct. 8, 2019, 2:50 PM), https://www.npr.org/2019/10/08/768319934/senate-report-russians-used-used-social-media-mostly-to-target-race-in-2016.

38 Shannon Bond, *Black and Latino Voters Flooded with Disinformation in Election's Final Days*, NPR, (Oct. 30, 2020, 7:49 AM), https://www.npr.org/2020/10/30/929248146/black-and-latino-voters-flooded-with-disinformation-in-elections-final-days.

II. STANDARDS: INTERNATIONAL AND DOMESTIC REGULATORY INITIATIVES

The International Bill of Human Rights prohibits racial discrimination and protects a range of different socioeconomic, civil, and political rights, including privacy and political participation. The Universal Declaration of Human Rights (UDHR) provides that "all human beings are born free and equal in dignity and rights;" both the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR) prohibit discrimination based on race, color, and national origin among other distinctions.[39] The International Convention on the Elimination of All Forms of Racial Discrimination (CERD) codifies the importance of taking effective measures to end policies that have the effect of creating racial divisions or perpetuating racial discrimination.[40] Racial discrimination violates international human rights law. International human rights law prohibits invasions of privacy that are arbitrary.[41] In 2013, the United Nations General Assembly adopted Resolution 68/167 on the Right to Privacy in the Digital Age, expressing "deep[] concern at the negative impact that surveillance and interception of communications may have on human rights" and affirming that the right to privacy must be protected and respected in digital communications.[42] The UDHR provides, and the ICCPR reaffirms that everyone has the right to take part in the government of their country directly or through freely chosen representatives.[43] The UDHR provides that the will of the people as expressed through free elections is the basis for legitimate governmental authority.[44] Human rights law protects participation in public life and political affairs.

There are ample examples of ways that biotech and information technology companies can contribute to placing these and other fundamental human rights. Companies are not countries and cannot become State parties to these international human rights instruments prohibiting racial discrimination and protecting participation in public life and governance. Still, this fact does not entirely absolve business enterprises from obligations to respect human rights.[45]

---

39 Universal Declaration of Human Rights Art. 1, G.A. Res. 217 (III) A, (Dec. 10, 1948) U.N. Doc. A/810 [hereinafter UDHR]; International Covenant on Civil and Political Rights, Art. 2, 999 U.N.T.S. 171, (Dec. 16, 1966) [hereinafter ICCPR]; International Covenant on Economic, Social and Cultural Rights, Art. 2, 993 U.N.T.S. 3, (Dec. 16, 1966) [hereinafter ICESCR]. Taken together the UDHR, ICCPR and ICESCR are referred to as the International Bill of Human Rights.

40 *See* International Convention on the Elimination of All Forms of Racial Discrimination, 660 U.N.T.S. 195 (Dec. 21, 1965) [hereinafter CERD] (CERD defines "racial discrimination" as "any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which as the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life.")

41 ICCPR, *supra* note 39, at Art. 17.

42 G.A. Res 68/167 (Dec. 18, 2013).

43 UDHR, *supra* note 39, at Art. 21(1); ICCPR, *supra* note 39, at Art 25 (a).

44 UDHR, *supra* note 39, at Art. 21 (3).

45 *See generally*, ERIKA GEORGE, INCORPORATING RIGHTS: STRATEGIES TO ADVANCE CORPORATE ACCOUNTABILITY 65-90 (2021) (providing a chronology of the emergence and evolution of a corporate obligation to respect human rights in international law and policy).

A. *THE UNITED NATIONS GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS (UNGPS)*

In 2011, the UN Human Rights Council unanimously endorsed the United Nations Guiding Principles on Business and Human Rights (UNGPs). The product of years of research and multistakeholder engagement by the Special Representative on the Issue of Human Rights and Transnational Corporations Professor John Ruggie, the UNGPs have come to serve as an "authoritative focal point."[46] The UNGPs set forth concrete recommendations to fortify a three-pillar "Protect, Respect, and Remedy" framework for avoiding and addressing human rights violations. States are responsible for protecting human rights by making and enforcing laws and policies; businesses have a responsibility to respect human rights by making policy commitments and conducting risk assessments to avoid becoming involved in rights abuses; victims of rights violations must have access to effective judicial and non-judicial remedies. The UNGPs hold promise for providing technology developers and policymakers a principled and pragmatic approach to designing and regulating technology in ways that advance respect for human rights.[47]

1. *Pillar I Progress: The State Responsibility to Protect Human Rights*

Some countries, including the US, have imposed sanctions on the offending tech companies contributing to human rights abuses.[48] The Biden-Harris Administration has indicated that meaningful action to curb the proliferation of technology, that has been misused by governments for repression, is central to its "commitment to put human rights at the center of US foreign policy."[49] At the Summit for Democracy in 2021, the United States, Australia, Denmark and Norway announced an *Export Controls and Human Rights Initiative* to help stem the tide of authoritarian government misuse of technology and promote a positive vision for technologies anchored by democratic values. Canada, France, the Netherlands, and the United Kingdom have also joined the initiative.[50]

---

46 The UN Guiding Principles on Business and Human Rights: An Introduction, UN Working Grp. on Bus. & Hum. Rts. (last visited May 4, 2022).

47 John Ruggie, *UN Guiding Principles for Business & Human Rights*, Harv. L. Sch. Forum on Corp. Gov. (Apr. 9, 2011), https://corpgov.law.harvard.edu/2011/04/09/un-guiding-principles-for-business-human-rights/ ("More recently, I am grateful to the many voices in the corporate governance field who provided feedback as I finalized the Guiding Principles. For instance, Martin Lipton of Wachtell, Lipton, Rosen and Katz has remarked that the "*Guiding Principles* insightfully marries aspirations with practicality. It identifies a host of tangible opportunities for Nations and businesses to contribute to the goal of preventing human rights abuses. ….. In short, *Guiding Principles* encapsulates the Special Representative's stated commitment to "principled pragmatism," reflecting the world's fundamental human rights expectations in a balanced way that takes account of the varied, complex global business landscape.").

48 U.S. Dep't Treasury, *Treasury Sanctions Perpetrators of Serious Human Rights Abuse on International Human Rights Day* (Dec. 10, 2021), https://home.treasury.gov/news/press-releases/jy0526.

49 The White House, Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy (Dec. 10, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/.

50 The White House, Joint Statement on the Export Controls and Human Rights Initiative (Dec. 10, 2021) https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/joint-statement-on-the-export-controls-and-human-rights-initiative/.

Last year, members of Congress introduced the Democracy Technology Partnership Act which would establish the International Technology Partnership Office and created a Special Ambassador for Technology in the Department of State to lead it.[51] The Office would be responsible for advancing US technology policy through the creation of partnerships with democratic countries to develop technology governance regimes, with a focus on key technologies such as artificial intelligence and machine learning and biotechnology, among other innovations.[52] Partner countries must have a demonstrated record of trust or an expressed interest in international cooperation and coordination with the United States on defense and intelligence matters. The Act would also establish the International Technology Partnership Fund in the Department of the Treasury. The State Department may use amounts from this fund to support joint research projects from International Technology Partnership member countries and technology investments in third-country markets. "The State Department must also submit reports (1) outlining a national strategy for technology and national security; and (2) assessing other countries' standards and governance regimes for privacy, human rights, consumer protection, and free expression."[53]

In 2019, a bill was proposed in Congress called the "Algorithmic Accountability Act" (AAA). This Act would have empowered the FTC to regulate biotech companies and assess algorithm accuracy and data privacy.[54] While the bill failed to gain traction at the time, a similar bill has been introduced recently with some changes.[55] Given the recent reckoning with racial bias in policing following the murder of George Floyd, advocates are hopeful that this or similar legislation may gain more traction. The new proposed bill would require companies to conduct impact assessments for their algorithms, including the reasons for the algorithms replacing manual decisions, a description of privacy risks and other negative impacts, and an evaluation of possible bias.[56] Other national legislation has been introduced, like the 2019 Commercial Facial Recognition Privacy Act, which generally prohibits using facial recognition data without notice and consent.[57]

Local jurisdictions in the US have also started to address these issues. San Francisco was the first city to ban government use of facial recognition tech in 2019.[58] Since then, Oakland, Berkeley, Somerville, Cambridge, and others have followed with bans.[59] In 2020, Washington state became the first to regulate the use of facial recognition tech, enacting legislation to regulate risks and reduce abuse.[60] Notably, Washington's law provides protection against the type of mass

---

51 Democracy Technology Partnership Act, H.R. 3426, 117th Cong. (2021). As of this writing, this bill has not been passed.

52 The Democracy Technology Partnership Act, S.604, 117th Cong. § 1(2021).

53 *Id*.

54 Hayden Field*, The Algorithmic Accountability Act is Back- Here's What's in It*, EMERGING TECH BREW (Feb. 11, 2022) https://www.morningbrew.com/emerging-tech/stories/2022/02/11/the-algorithmic-accountability-act-is-back-here-s-what-s-in-it.

55 *Id.*

56 *Id.*

57 *Blunt, Schatz Introduce Bipartisan Commercial Facial Recognition Privacy Act*, ROY BLUNT UNITED STATES SENATOR FOR MISSOURI (Mar. 14, 2019), https://www.blunt.senate.gov/news/press-releases/blunt-schatz-introduce-bipartisan-commercial-facial-recognition-privacy-act.

58 *See* MADIEGA & MILDEBRATH*, supra* note 3.

59 *Id.*

60 *See* Brad Smith, *Finally, Progress on Regulating Facial Recognition*, MICROSOFT ON THE ISSUES

surveillance system used in China by prohibiting public authorities from using facial recognition without having either a warrant or a court order to locate or identify a missing person or satisfying requirements that show "exigent circumstances."[61] Moreover, authorities cannot use facial recognition to record individuals engaged in exercising First Amendment rights or target individuals based on "religious, political, or social views or activities" or based on "actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender identity, sexual orientation or other characteristic protected by law."[62] A government agency must file a public notice of intent specifying the purpose for which facial recognition technology is to be used before it can be used. Government agencies must also have "a clear use and data management policy" explaining data retention, cybersecurity precautions and protocols for how the technology will be used.[63] Agencies using facial recognition technology must also meet public notice and consultation requirements.[64] In addition, government agencies must report to the public information about impacts on privacy and protected subpopulations as well as false matches and error rates.[65]

Comparatively, the EU has the most advanced tech regulatory regime. The EU has worked on addressing risks raised by biotech in a range of different ways. Some advocates focus on rights already well established within the EU, such as those contained in the Charter of Fundamental Rights (CFR), to support arguments for limiting the uses of biotech.[66] The CFR recognizes fundamental rights of privacy, non-discrimination, and data protection, all of which can be used to reduce risks to human rights associated with biotech.[67]

The Law Enforcement Directive (LED) and General Data Protection Regulation (GDPR) have also been referenced to support biotech regulation in Europe because these laws provide standards for government data processing to be transparent, accurate, and limited.[68] In addition, algorithmic discrimination should fall within the regulatory scope of a range of EU laws and directives that protect against discrimination.[69] Despite these existing frameworks of rights and protections in the EU that could be adapted for biotech, many gaps remain.[70] In April 2021, the EU released a draft artificial intelligence act aimed at limiting the use of AI for inappropriate surveillance.[71] This proposal creates categories of AI technology: unacceptable risk (prohibited), high-risk (subject to conformity assessments pre-market), limited risk (limited obligations), and

---

(Mar. 31, 2020) https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/; 2020 Wash. Sess. Laws 257.

61 *Id.*

62 *Id.*

63 *Id.*

64 *Id.*

65 *Id.*

66 *See* MADIEGA & MILDEBRATH, *supra* note 3.

67 *Id.*

68 *Id.*

69 *Id.* These EU rules and directives include Articles 2 TEU, 10 TFEU, Article 21 CFR, Directive 2000/43/EC, and more.

70 *Id.*

71 *Id.*

minimal risk (no additional obligations).[72] In 2021, the Council of Europe adopted guidelines on facial recognition technology.[73]

International entities have also sought to address biotech and information technology concerns. In 2019 the Office of the High Commissioner for Human Rights consulted with a range of stakeholders to create the "B-Tech Project" to "address the urgent need to find principled and pragmatic ways to prevent and address human rights harms connected with the development of digital technologies and their use by corporate, government and non-governmental actors, including individual users."[74] In 2020, the UN Human Rights Council adopted a resolution that condemned the use of facial recognition in peaceful protests because of the harmful chilling effect this can have on speech rights.[75] Consistent with the UNGPs call for countries to enact laws and create policies to prevent and punish rights abuses, including abuses involving commercial actors,[76] in order to protect human rights and prevent discrimination in the digital realm, it will be important for States to craft regulations that are conscious of racism as a human rights risk.

2. *Pillar II Progress: The Corporate Responsibility to Respect*

Several leading tech firms communicated an intention to make changes in response to protest movements resulting from the aftermath of George Floyd's death.[77] Some business leaders expressed interest in doing diligence to determine the ways their policies and practices serve to promote racism.[78] For example, Microsoft announced it would stop providing facial recognition technology to law enforcement due to racial bias until legal protections were put in place.[79] Amazon issued a self-imposed moratorium on the use of its facial recognition products by police.[80] IBM, a company that provided the tracking technology used by Nazis to facilitate crimes against humanity during WWII, went on record opposing the use of its technology for mass surveillance and

---

72 *Id.*

73 *See* COUNCIL OF EUROPE, GUIDELINES ON FACIAL RECOGNITION (2021), https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html.

74 For an overview of B-Tech Project research*, see generally*, B-TECH PROJECT: OHCHR AND BUSINESS AND HUMAN RIGHTS, https://www.ohchr.org/en/business/b-tech-project (last visited Apr. 8, 2022).

75 Human Rights Council Res. 44/20, U.N. Doc A/HRC/Res/44/20 (July 23, 2020).

76 John Ruggie (Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* Art. 1, A/HRC/17/31 (Mar. 21, 2011) [hereinafter UNGP].

77 Gillian Freidman, *Here's What Companies are Promising to Do to Fight Racism*, N.Y. TIMES (Aug. 23, 2020), https://www.nytimes.com/article/companies-racism-george-floyd-protests.html.

78 *Id. See also USA: Company executives speak out against racism following the killings of George Floyd, Breonna Taylor & Tony McDade by police*, BUSINESS & HUMAN RIGHTS RESOURCE CENTRE (Jun. 1, 2020) https://www.business-humanrights.org/en/latest-news/usa-company-executives-speak-out-against-racism-following-the-killings-of-george-floyd-breonna-taylor-tony-mcdade-by-police/.

79 Jay Greene, *Microsoft Won't Sell Police Its Facial Recognition Technology, Following Similar Moves By Amazon and IBM*, WASHINGTON POST (Jun. 11, 2020, 2:30 PM), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

80 Bobby Allyn, *Amazon Halts Police Use of Its Facial Recognition Technology*, NPR (Jun. 10, 2020, 6:59 PM), https://www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology.

racial profiling as violations of basic human rights and freedoms inconsistent with the company's stated values of trust and transparency.[81]

Even before the widespread civil unrest over police brutality that followed George Floyd's murder, technology professionals had expressed concerns over how their creations were being used in policing and surveillance. In 2018, a group of Microsoft employees penned an open letter condemning the company's collaborations with ICE, including processing data and providing artificial intelligence capabilities. Across the industry, tech employees vocally opposed policies of separating immigrant families at the US/Mexico border.[82] In 2018, several Google employees signed and published a petition protesting the company's cooperation with China to build a search engine tailored to the country's censorship requirements—code-named Dragonfly.[83] A leaked internal letter signed by over 1,000 Google employees called for more transparency and an ethical accounting of company projects; complaining "we do not have the information required to make ethically informed decisions about our work, our projects, and our employment" and citing Dragonfly as just one example of a project planned without adequate employee input.[84] Tech firms were among the first to denounce a 2017 Presidential Executive Order prohibiting citizens from seven Muslim-majority countries, in popular parlance the "Muslim Ban," with several firms filing an amicus brief opposing the order.[85]

Microsoft has adopted six core "Microsoft Responsible AI Principles" that are applied across the company with the assistance of advisory committees.[86] The principles are:

> Fairness: AI systems should treat all people fairly
> Reliability & Safety: AI systems should perform reliably and safely
> Privacy & Security: AI systems should be secure and respect privacy
> Inclusiveness: AI systems should employ everyone and engage people
> Transparency: AI systems should be understandable; [and]
> Accountability: People should be accountable for AI systems[87]

---

81 Hannah Denham, *IBMs Decision to Abandon Facial Recognition Technology Fueled by Years of Debate*, WASHINGTON POST, (Jun. 11, 2020, 4:58 PM). https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/

82 Sheera Frenkel, *Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration,* N.Y. TIMES (Jun. 19, 2018), https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html

83 Ariel Bogle, *Google Faces Staff Revolt Over Plans for Project Dragonfly Censored Search Engine in China*, ABC News (Nov. 27, 2018, 9:36 PM), https://www.abc.net.au/news/science/2018-11-28/google-china-project-dragonfly-search-engine-staff-protest/10561816 (Quoting Google employee open letter: "Our opposition to Dragonfly is not about China: we object to technologies that aid the powerful in oppressing the vulnerable, wherever they may be").

84 Hamza Shaban, *Google Employees Go Public to Protest China Search Engine Dragonfly*, THE WASHINGTON POST, Nov. 28, 2018. https://www.washingtonpost.com/technology/2018/11/27/google-employees-go-public-protest-china-search-engine-dragonfly/

85 *See* Jennifer S. Fan, *Woke Capital: The Role of Corporations in Social Movements*, 9 HARV. BUS. L. REV. 441 (2019).

86 MICROSOFT, RESPONSIBLE AI, https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1:primaryr6 (last visited Mar. 27, 2022); *Research Collection: Research Supporting Responsible AI,* MICROSOFT (Apr. 13, 2020), https://www.microsoft.com/en-us/research/blog/research-collection-research-supporting-responsible-ai/

87 *Id.*

Efforts to operationalize responsible AI across the company are centralized and coordinated through an Office of Responsible AI that sets company-wide governance policies. It is complemented by the Responsible AI Strategy in Engineering (RAISE) team which enables implementation of the principles in engineering groups. The "Aether" committee examines emerging issues and advises senior Microsoft leadership on best practices and processes and oversees research and development working groups.[88] Microsoft also makes responsible AI resources available to its customers and is working with other organizations to develop tools and guidance.

The Partnership on AI, a multistakeholder working group to discuss the impacts of AI on society, was co-founded by Microsoft. The Partnership on AI is a non-profit partnership between industry, research academies, media, and civil society organizations working to "pool collective wisdom to make change" to ensure "AI advances in positive outcomes for people and society."[89] The Partnership counts among its leadership representatives from the ACLU, PolicyLink, Apple, IBM, and Amazon.[90]

Despite modest progress by commercial actors making policy commitments and some encouraging resistance efforts on the part of tech employees, there are structural incentives that make self-regulation difficult for the information technology sector. In her groundbreaking work, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Shoshana Zuboff explains how society came to "conflate commercial imperatives and technological necessity," enabling companies like Google, Facebook, Microsoft, and others to "extract human experience" for profit. She raises concerns about the asymmetries of knowledge that power tech firms enjoy and explains how the "mutuality of interests between fledgling surveillance capitalists and state intelligence agencies" were preconditions for the success of a new form of capitalism—surveillance capitalism.[91] She cautions that the "smart" services we enjoy, enabled by technology, come with costs to autonomy and democracy.[92] People probably should not be products.

The UNGPs make clear that businesses must prevent and mitigate human rights risks where products or services can cause or contribute to human rights abuses. Yet, human rights risk mitigation consistent with the UNGPs will be difficult for corporations with business models based on monetizing private human experience by converting personal data and preferences into behavioral predictions for sale to the highest bidder or into behavior modifications.

---

88 MICROSOFT, PUTTING PRINCIPLES INTO PRACTICE AT MICROSOFT, https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1%3aprimaryr5 (last visited Apr. 8, 2022).

89 PARTNERSHIP ON AI, https://partnershiponai.org, (last visited Mar. 27, 2022).

90 PARTNERSHIP ON AI, OUR TEAM, https://partnershiponai.org/team/ (last visited Apr. 9, 2022).

91 SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 15, 19 (2019). *See also* Tanner Humanities Center, Utah College of Humanities, Tanner Lecture on Human Values & Artificial Intelligence (2021), https://thc.utah.edu/public-programs/tanner-lectures/shoshana-zuboff.php ; Shoshana Zuboff, *The real reason why Facebook and Google won't change,* FAST COMPANY (Feb. 22, 2019), https://www.fastcompany.com/90303274/why-facebook-and-google-wont-change ("Facebook, Google, and other masters of the surveillance economy have bred a virulent mutation of capitalism, which explains why they aren't interested in addressing their many scandals.").

92 Shoshana Zuboff, *Surveillance Capitalism has Gone Rogue. We Must Curb its Excesses*, WASHINGTON POST (Jan. 24, 2019, 8:11 PM), https://www.washingtonpost.com/opinions/surveillance-capitalism-has-gone-rogue-we-must-curb-its-excesses/2019/01/24/be463f48-1ffa-11e9-9145-3f74070bbdb9_story.html.

III. DECODE DISCRIMINATION

What if our technological innovations were used to analyze patterns of inclusion and exclusion? What if we used technology to help expose and eradicate bias rather than to promulgate bigotry and hatred? There are groups led by people of color who are studying and advocating for change in the tech sector, including the Algorithmic Justice League[93] and Data for Black Lives.[94] The United Nations Working Group on Business and Human Rights, responsible for the promotion, dissemination, and implementation of the UNGPs recently launched the "UNGPs+10" initiative to celebrate the tenth anniversary of the unanimous endorsement of the Guiding Principles on Business and Human Rights by the United Nations Human Rights Council in 2021 and to chart a course action for implementing the UNGPs more widely and broadly between now and 2030.[95] Technology has been identified as an important priority.[96] To the extent that regulatory measures are being debated and designed, centering human rights and the procedural protections outlined in the UNGPs, especially provisions on conducting human rights due diligence, risk assessment, and reporting, would be progress.

93 Algorithmic Justice League, https://www.ajl.org/ (last visited May 21, 2022).
94 Data for Black Lives, https://d4bl.org/ (last visited May 21, 2022).
95 UN WORKING GROUP ON BUSINESS AND HUMAN RIGHTS, RAISING THE AMBITION-INCREASING THE PACE: UNGPS 10+ A ROADMAP FOR THE NEXT DECADE OF BUSINESS AND HUMAN RIGHTS 9 (2021).
96 *Id.*