Response to Request for Information (RFI)
FR Doc. 2021–21975

CHR&GJ center for human rights and global justice nyu school of law

Temple University Beasley School of Law | Institute for Law, Innovation and Technology

January 14, 2022

To the White House Office of Science and Technology Policy:

We are writing on behalf of the Digital Welfare State & Human Rights Project, Center for Human Rights and Global Justice (CHRGJ), NYU School of Law,[1] and the Institute for Law, Innovation & Technology (iLIT), Temple University, Beasley School of Law,[2] as well as a group of international legal experts and civil society representatives with extensive experience studying the impacts of biometric technologies.[3]

We welcome the focus on human and civil rights within the Bill of Rights for an AI-Powered World ("AI Bill of Rights") initiative and the focus on the *impacts* of biometric technologies.[4] Where industry has long pushed for *ethical* principles, this is an opportunity to protect rights through binding regulations, an essential step given the existential threats such technologies pose to human rights, democracy, and rule of law. OSTP should reflect on both the substance of rights and potential barriers for enforcement. This includes striving to distinguish—as many new technology developers fail to do—between the need for innovation, new laws and new rights, and the need to fix what is broken in existing laws, rules, policies, practices, and institutions.

This response provides international and comparative information to inform OSTP's understanding of the social, economic, and political impacts of biometric technologies,[5] in research and regulation. Biometrics fuel automation globally,[6] often at an accelerated, reckless pace, and these concerns transcend both political and geographic boundaries. Other powerful political actors—perceived as both peers and competitors—are attempting to understand and regulate in this area. This is an opportunity for the United States to be a world leader in ensuring that innovation is pursued in a way that safeguards human rights, both at home and abroad.

While we look forward to a consultative and transparent process for the AI Bill of Rights, we also note that the speed with which such technologies are being deployed requires urgent action. OSTP should work to establish immediate checks on the deployment of some of the most high-risk and contested tools, including an immediate moratorium on mandatory use in critical sectors such as health, education, and welfare, allowing time and space for democratic oversight before further intractable harms emerge. Our complete recommendations can be found in Section V.

I. The need for a comprehensive federal government response

There is already significant evidence that use of biometric identification in the United States can lead to harm, disproportionately impacting communities already discriminated against on the basis of, *inter alia*, race, sex, and national origin. For example, facial recognition technology disproportionately misidentifies

[1] The Digital Welfare State and Human Rights Project at the Center for Human Rights and Global Justice at NYU School of Law aims to investigate systems of social protection and assistance in countries worldwide that are increasingly driven by digital data and technologies. From NYU, Katelyn Cioffi (katelyn.cioffi@nyu.edu), Victoria Adelmant (victoria.adelmant@law.nyu.edu), and Christiaan van Veen (cvv221@nyu.edu) contributed to this response.

[2] The Temple University Institute for Law, Innovation & Technology, pursues research, instruction, and advocacy with a mission to deliver equity and inform new approaches to innovation in the public interest. Contributors: Laura Bingham (laura.bingham@temple.edu), Ed DeLuca (edward.deluca@temple.edu), Sarbjot Kaur Dhillon (sarbjotkd@temple.edu), and Bianca Evans (bianca.evans@temple.edu).

[3] This response benefited from invaluable input from a group of international experts with deep knowledge of the impact of AI and biometric identification technologies on human rights, including Gautam Bhatia, Yussuf Bashir (Haki na Sheria Initiative), Olga Cronin (Irish Council for Civil Liberties), Reetika Khera, Matthew McNaughton (Slashroots), Grace Mutung'u, Usha Ramanathan, and Anand Venkatanarayanan.

[4] Eric Lander & Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, WIRED, Aug. 10, 2021, https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/.

[5] Rashida Richardson & Amba Kak, *Suspect Development Systems: Databasing Marginality and Enforcing Discipline*, UNIV. MICH. J. L. REF., Vol. 55 (forthcoming), https://ssrn.com/abstract=3868392. (highlighting "counterproductive siloes between the Global South and Global North")

[6] *Id*.

people of color; use in law enforcement thus perpetuates racial bias, false arrests, and police brutality.[7] Moreover, the Department of Homeland Security's (DHS) transnational network of biometric records, tracking, and automated profiling consistently evades scrutiny, but shows evidence of arbitrary, discriminatory, and harmful practices.[8]

Despite evidence of the harms of biometric technologies, regulation is woefully lacking,[9] with the exception of some cities and states.[10] A significant part of the population is not covered by this patchwork of prohibitions,[11] and while litigation and local regulation provide some oversight, the federal government and its contractors are not held accountable even to these inadequate standards.[12] The absence of, for instance, guidance for development and use of AI by the federal government and its agencies, as well as common binding standards for private actors, risks perpetuating fragmented and insufficient rights protection. Further, the federal government has a vital role to play in regulating *all* biometric technologies, including those which have been in place for decades, such as fingerprint-scanning in the law enforcement and immigration contexts, as well as the extraterritorial application of technologies developed, produced, sold, and promoted by U.S. government agencies and corporations.

Two initial, fundamental concerns with a "Bill of Rights" approach must be highlighted, based on expert comparative legal analysis from several constitutional democracies. First, such an approach, if taken at face value as an effort to amend or modernize textually anchored rights, may exclude structural constitutional questions, such as separation of powers, the scope and quality of judicial review, and standing. Adoption of biometrics and predictive technologies increasingly concentrates power in executive agencies, inviting structural, slow-onset forms of injury.[13] Yet, unlike most constitutional systems, U.S. judicial review of administrative actions is structurally divorced from constitutional law and rights protection. Much relevant technology is predicated on "improving" or "modernizing" the administrative state, but "administrative law in the USA is not concerned primarily with basic rights."[14] Rights, however formulated, therefore risk being effectively unenforceable as executive discretion continues its extra-constitutional expansion.

Second, the absence of a cause of action for indirect discrimination ("disparate impact") that applies generally across different sectors and to state, local, and federal departments, as well as private actors, is concerning in this context. In contrast to proportionality tests applied in the majority of constitutional frameworks,[15] U.S. constitutional balancing tests are rigid and rules-driven, restricting serious scrutiny to the most obvious and intentional instances of racial discrimination.[16] Though disparate impact exists

[7] *See* Joy Adowaa Buolamwini, *Gender shades: intersectional phenotypic and demographic evaluation of face datasets and gender classifiers*, 2017, https://dspace.mit.edu/handle/1721.1/114068; Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face recognition vendor test part 3: demographic effects,* NIST IR 8280, 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[8] Ryan Calo & Danielle K. Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L. J. 797, 830, 2021, https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj (finding that no-fly algorithms are unable to distinguish names, and that rules are not disclosed under executive and state secrets privileges); Sam Biddle & Maryam Saleh, *Little-Known Federal Software Can Trigger Revocation of Citizenship*, INTERCEPT, Aug. 25, 2021, https://theintercept.com/2021/08/25/atlas-citizenship-denaturalization-homeland-security/; Richardson & Kak, *supra* note 5.

[9] Todd Feathers, *Why It's So Hard to Regulate Algorithms*, MARKUP, Jan. 4, 2022, https://themarkup.org/news/2022/01/04/why-its-so-hard-to-regulate-algorithms.

[10] Facial recognition has been banned or restricted across many cities and several states: *see* Fight for the Future, *Map*, Ban Facial Recognition , https://www.banfacialrecognition.com/map/ (last visited Jan. 13, 2022). *See also* No Biometric Barriers to Housing Act of 2021, H.R. 4360, 117th Cong. (2021–22).

[11] Tom Simonite, *Face Recognition is Being Banned—But It's Still Everywhere*, WIRED, Dec. 22, 2021, https://www.wired.com/story/face-recognition-banned-but-everywhere/.

[12] Calo & Citron, *supra* note 8, at 815 (citing the APA's restrictions on challenging federal agency action).

[13] *See, e.g.*, *id.* at 845; Marielle Debos, *Biometrics and the Disciplining of Democracy: Technology, Electoral Politics, and Liberal Interventionism in Chad*, DEMOCRATIZATION 1, Mar. 31, 2021, https://doi.org/10.1080/13510347.2021.1907349.

[14] Vicki C. Jackson & Mark Tushnet (eds.), PROPORTIONALITY: NEW FRONTIERS, NEW CHALLENGES 111, 2017. *See also* David Engstrom et al., *Government By Algorithm: Artificial Intelligence in Federal Administrative Agencies*, 2020, https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf (highlighting lack of public remedies under APA where a private right of action under federal discrimination statutes is "adequate").

[15] Jackson & Tushnet, *Id.*, at 111.

[16] *Id.*

as a theory of liability under some federal civil rights statutes,[17] even here the availability of disparate impact claims is at executive agencies' discretion in their enforcement of federal anti-discrimination laws.[18] In most other jurisdictions, and under international treaties like the Convention on the Elimination of All Forms of Racial Discrimination, ratified by the United States in 1994, the term "indirect discrimination" is used to denote liability for discrimination based on the *effect* of laws and practices.[19]

The limited availability and lax enforcement of disparate impact leaves the equal protection clause gutted and insufficient to deal with AI-enabled biometric discrimination.[20] Without providing for disparate impact claims, rights protections in the U.S. fall beneath international equality standards that the government has pledged to uphold and are not fit for purpose in an automated society which already exhibits structural bias and discrimination.

II. International evidence provides a critical resource

There is now a significant body of evidence that illuminates both the potential benefits and harms of biometric technologies in different contexts.[21] This response reflects input from leading experts who have worked in India, Jamaica, Kenya, and Ireland,[22] where governments, international organizations, and private actors have used a combination of biometrics, data sets, and machine learning to mediate access to fundamental rights.[23] With cities and states in the United States poised to follow suit,[24] this research provides an invaluable resource, allowing for proactive actions that anticipate and mitigate known harms.

Most critically, evidence now extends beyond frequently raised concerns about surveillance and privacy in the context of law enforcement and national security, to encompass concerns about social rights such as health, social security, education,[25] housing, and employment.[26] A recurring finding is that biometrics have potential to generate and exacerbate patterns of social exclusion, as well as direct and indirect discrimination. These technologies thus increasingly affect access, availability, affordability, and quality of fundamental public services.

A. How do AI and biometric technologies generate exclusion and discrimination?

[17] *See Texas Dep't of Hous. & Cmty. Affs. v. Inclusive Communities Project, Inc.*, 576 U.S. 519 (2015). *See* Cass R. Sunstein, *Algorithms, Correcting Biases*, 86 Soc. Res.: Int'l Q. 499, 510, 2019 (noting disparate impact liability presents some of the most important issues for challenging algorithmic discrimination in the future), http://eliassi.org/sunstein_2019_algs_correcting_biases.pdf.

[18] *See, e.g.*, *HUD's New Rule Paves the Way for Rampant Algorithmic Discrimination in Housing Decisions*, New Am., Oct. 1, 2020, http://newamerica.org/oti/blog/huds-new-rule-paves-the-way-for-rampant-algorithmic-discrimination-in-housing-decisions. On disparate impact generally, see *Tex. Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc.*, 576 U.S. 519 (2015). *See also Griggs v. Duke Power Co.*, 401 U.S. 424 (1971).

[19] *See* Audrey Daniel, *The Intent Doctrine and CERD: How the United States Fails to Meet Its International Obligations in Racial Discrimination Jurisprudence*, 4 DePaul J. Soc. Just. 263, 2011, https://via.library.depaul.edu/jsj/vol4/iss2/3. *See also* EU Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, 2000 O.J. (L 180) 22 (requiring EU Member States to prohibit direct and indirect discrimination on the basis of racial or ethnic origin); *D.H. and Others v. the Czech Republic*, App. No. 57325/00, 47 EUR. H.R. REP. 3, 2008.

[20] *See, e.g.*, Mark MacCarthy, *Fairness in algorithmic decision-making*, Brookings, 2019, https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/.

[21] A 2013 survey found at least 230 instances of developmental programs using biometric identification tech. *See* Alan Gelb & Julia Clark, *Identification for Development: The Biometrics Revolution*, SSRN J., 2013, http://www.ssrn.com/abstract=2226594.

[22] *See supra* note 3.

[23] Biometrics must be evaluated in conjunction with related algorithms, data sets, and institutional arrangements, sometimes called the 'biometric assemblage'. *See* Mirca Madianou, *The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies*, 20 Television & New Media 581–599, 2019, https://doi.org/10.1177/1527476419857682.

[24] *See generally*, Mizue Aizeki & Rashida Richardson, eds., *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"*, Dec. 2021, https://www.immigrantdefenseproject.org/wp-content/uploads/smart-city-digital-id-products.pdf.

[25] Sally Weale, *ICO to Step in After Schools use Facial Recognition to Speed up Lunch Queue*, Guardian, Oct. 18, 2021, https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk.

[26] *See, e.g.*, Center for Human Rights and Global Justice [CHRGJ] et al., *Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons,* 2021, https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf; Karthik Muralidharan et al., *Identity Verification Standards in Welfare Programs: Experimental Evidence from India,* NBER Working Paper Series 26744, 2020, http://www.nber.org/papers/w26744.pdf.; Jean Drèze, *There is an urgent need for safeguards against unfair discontinuation of social benefits*, Indian Express, Apr. 20, 2021, https://indianexpress.com/article/opinion/columns/aadhaar-linking-public-welfare-schemes-pds-system-7280621/; Reetika Khera, ed., *Dissent on Aadhaar: Big Data Meets Big Brother,* 2018.

Exclusion can be caused by innate problems with biometric technology. While much recent critique has focused on facial recognition and mass surveillance, the difficulties of mitigating the harmful effects of "lower-tech" solutions[27] such as fingerprinting, should be both a warning and opportunity for learning as "novel," more advanced technologies emerge. As with most biometrics, specific notions of "normality" are built into fingerprinting systems; "hand scanners have particular sizes and shapes, with designated places to put the fingers," and anyone falling outside of this "norm" will struggle to authenticate.[28] Failure rates are significantly higher among people of color as systems are "infrastructurally calibrated to whiteness."[29] Further, as biometric systems are probabilistic and are often designed to tolerate significant exclusion errors, relying on them to definitively identify or verify will inevitably lead to exclusion.[30]

Moreover, while laboratory-based testing of biometric technologies might show relatively high success rates, as was shown in a challenge to a nationwide digital ID system reliant on fingerprint authentication in Kenya, "the real-world data is very different."[31] Environmental conditions, including humidity, temperature, and light exposure, impact the quality of biometric data capture.[32] Biometrics are not immutable, as they can alter over time and degrade with age. Capture and authentication often depend on fragile, expensive hardware, as well as quality internet and electricity. Thus, digital divides—which map onto other disadvantages—can be exacerbated through AI-enabled biometrics.[33]

Consequently, when biometrics are yoked to essential services such as social security or health care, marginalization and exclusion may arise. This in turn results in decreased access to numerous fundamental entitlements, damaging physical and mental health, and impacting dignity. This has been extensively documented in India, home to the world's largest biometric identification system, Aadhaar.[34] Persistent failures to authenticate fingerprints through Aadhaar at the point of service for welfare programs, including food rations depended on by four-fifths of Indian families, has resulted in numerous deaths by starvation, families cut off from rations for weeks, and a system that increasingly punishes the poor.[35] In Uganda, card readers were unable to read older persons' fingerprints or match their biometric profile to an accurate birth date in the national ID database. Although eligible to access certain social protection programs, such as cash transfers, older persons were consistently denied access to life-saving grants because of their inability to identify and authenticate biometrically.[36]

Even where such technologies operate as intended, their use can facilitate other forms of indirect discrimination. They can sit atop existing barriers, while introducing further requirements, and access

[27] Shoshana Amielle Magnet, *Criminalizing Poverty: Adding Biometrics to Welfare*, When Biometrics Fail: Gender, Race, and the Technology of Identity 23, 2011.

[28] Sanneke Kloppenburg & Irma van der Ploeg, *Securing Identities: Biometric Technologies and the Enactment of Human Bodily Difference*, 29(1) Sci. as Culture 57, 62, 2020, https://www.tandfonline.com/doi/full/10.1080/09505431.2018.1519534.

[29] *See* Shoshana Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity*, 2011, at 49, https://www.dukeupress.edu/when-biometrics-fail; Simone Brown, *Dark Matter: On the Surveillance of Blackness*, 2015, https://read.dukeupress.edu/books/book/147/Dark-MattersOn-the-Surveillance-of-Blackness; Grother et. al, *supra* note 7.

[30] Jeremy Wickins, *The Ethics of Biometrics: the Risk of Social Exclusion from the Widespread use of Electronic Identification*, 13 Sci & Engineering Ethics 45–54, 2007, http://link.springer.com/10.1007/s11948-007-9003-z.

[31] Nubian Rights Forum & 2 others v. Attorney General & 6 others, 2020, eKLR 37 [Kenya], at para. 37, http://kenyalaw.org/caselaw/cases/view/189189/.

[32] *See e.g.*, United Kingdom Government Office for Science, Biometrics: A Guide, June 15, 2018: https://www.gov.uk/government/publications/biometrics-a-guide; Ann Livingston et al., *Upholding the Rights of Children: Special Considerations on the Use of Biometrics in Identity Systems*, 2019, https://www.id4africa.com/2019/almanac/UNICEF-Ann-Livingston-Kristen-Wenz-Nicola-Richards.pdf.

[33] Silvia Masiero, *Biometric Infrastructures and the Indian Public Distribution System*, S. Asia Multidisciplinary Acad. J. 11 (2020), https://journals.openedition.org/samaj/6459.This remains a significant issue in the United States, see Emily A. Vogels, *Digital Divide Persists Even As Americans With Lower Incomes Make Gains In Tech Adoption*, 2021, https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/.

[34] Over 1.2 billion people have enrolled in the Aadhaar system. Swetha Totapelly et al., *State of Aadhaar Report*, 2019, https://stateofaadhaar.in/download-reports.php.

[35] *See, e.g.*, Reetika Khera, *These digital IDs have cost people their privacy — and their lives*, Wash. Post, Aug. 9, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/, last visited Jan. 14, 2022; *India's High-Tech Governance Risks Leaving Behind its Poorest Citizens*, Economist, Oct. 16 2021, https://www.economist.com/asia/2021/10/16/indias-high-tech-governance-risks-leaving-behind-its-poorest-citizens; Ursula Rao, *Biometric Bodies, Or How to Make Electronic Fingerprinting Work in India*, 24 Body & Soc. 68–94, 2018, https://doi.org/10.1177/1357034X18780983.

[36] CHRGJ et al., *supra* note 26, at 31–33.

becomes contingent on digital literacy, specific forms of personal identification,[37] reliable access to basic ICT services, or fees related to travel, administration, and lost time spent navigating the system. For instance, in India, the use of Aadhaar in public services requires networks of data operators who continuously collect and verify biometric data. Without oversight, such operators become bureaucratic bottlenecks, sites of harassment and intimidation, and an insurmountable barrier to accessing services.[38]

B. Civil death and other cumulative, systemic impacts of biometric systems

Taken individually, instances of exclusion may already constitute indirect discrimination. But the persistence of biometric information also means that the effects of exclusion replicate quickly, locking individuals out of multiple services. In Kenya, the United Nations High Commissioner for Refugees (UNHCR) collected biometric information to distribute food aid during a period of famine. Consequently, many Kenyans who were registered as children are victims of 'double registration': since their biometric data appears in a refugee database, the government denies them national ID cards, restricting access to services including employment, health care, and social security.[39] In Ireland, the Public Services Card (PSC), which includes collection of biometric data, rapidly expanded beyond its original role in the welfare system, with other government agencies requiring it as the sole form of ID.[40] This expansion was introduced without transparency, democratic debate, or adequate review of its necessity and proportionality. The use of biometrics can therefore quickly become *de facto* mandatory, even when not formally required.

Any failure to authenticate or ensure that data is consistent across different systems can therefore lead to "civil death,"[41] where an individual is cut off from *all* fundamental services. This is the case in Pakistan, where the government has unilaterally blocked certain individuals' biometric digital IDs, forcing them into a vetting process to 'prove' aspects of their identity such as citizenship or gender.[42] In Assam, India, the government recently conducted a mass citizenship verification process,[43] placing approximately 2.7 million people on a 'doubtful list' of those whose citizenship is called into question. Many on this list have had their biometric profiles frozen; this means that they cannot use their Aadhaar record to receive health care, access food rations, get a drivers' license, or register a SIM card.[44]

This civil death phenomenon is especially concerning since use of biometric technologies can coincide with entrenchment of structural racism and discrimination. While the broad use of these technologies in public service delivery will ultimately affect everyone, at present harms disproportionately impact already marginalized communities; across many biometric systems, those unable to identify and verify are often those in poor, rural communities, ethnic and religious minorities, women, and older persons.[45] Widespread deployment may thus exacerbate and deepen structural and institutional patterns of harm.[46]

[37] *See* Vivek Maru et al., *Digital IDs Make Systemic Bias Worse*, WIRED, Feb. 5, 2020, https://www.wired.com/story/opinion-digital-ids-make-systemic-bias-worse/.

[38] Vyom Anil & Jean Drèze, *Without Aadhaar, Without Identity*, INDIAN EXPRESS, July 5, 2021, https://indianexpress.com/article/opinion/columns/flaw-in-aadhaar-architecture-uidai-card-enrolment-7389133/.

[39] Haki na Sheria Initiative, *Biometric Purgatory: How the Double Registration of Vulnerable Kenyan Citizens in the UNHCR Database Left Them at Risk of Statelessness*, 2021, http://citizenshiprightsafrica.org/wp-content/uploads/2021/11/Haki-na-Sheria_Double-Registration_Nov2021.pdf.

[40] *DPC welcomes resolution of proceedings relating to the Public Services Card*, Dec. 10, 2021, https://www.dataprotection.ie/news-media/latest-news/dpc-welcomes-resolution-proceedings-relating-public-services-card.

[41] Usha Ramanathan, *Aadhaar is Like Drone Warfare Versus Hand to Hand Combat, Profiling Becomes All That More Easier*, BUSINESS STANDARD, Apr. 1, 2016, https://www.business-standard.com/article/economy-policy/aadhaar-is-like-drone-warfare-versus-hand-to-hand-combat-profiling-becomes-all-that-more-eaiser-usha-ramanathan-116033101394_1.html.

[42] Alizeh Kohari, *Life in Pakistan without a digital ID*, CODA STORY, Nov. 3, 2021, https://www.codastory.com/authoritarian-tech/pakistan-biometrics-stateless/.

[43] Siddhartha Deb, *'They Are Manufacturing Foreigners': How India Disenfranchises Muslims*, N.Y. TIMES, Sept. 15, 2021, https://www.nytimes.com/2021/09/15/magazine/india-assam-muslims.html.

[44] *Two Years Since NRC, Lakhs Still Remain in Limbo*, HINDU, Aug. 31, 2021, https://www.thehindu.com/news/national/two-years-since-nrc-lakhs-still-remain-in-limbo/article36201266.ece.

[45] Totapelly et al., *supra* note 34.

[46] Virginia Eubanks, *Automating Inequality*, 9, 2018.

Beyond exclusion, the extensive use of biometrics can also fundamentally affect democracy, the rule of law, accountability and transparency,[47] while entrenching private sector control over public functions.[48] After alleged election rigging in the 2017 Kenyan presidential election, government officials were unable to comply with judicial orders to grant access to election results data tied to a biometric voter registration system, as the vendor's servers were in France.[49] In South Africa, the introduction of biometric technologies into welfare payment systems resulted in one company's disastrous monopoly while weakening the government's power to maintain any control over the welfare system.[50] Use of biometrics can thus augment powerful market-based interests that do not reflect human rights and democratic principles.[51]

III. Comparative efforts to mitigate the exclusionary impact of biometric identification

While a data protection and privacy framework should be seen as a necessary condition to safeguard human rights in the context of biometrics, such measures are not sufficient to combat broader effects. Regulatory efforts that fail to include specific remedies for exclusion nor accessible accountability mechanisms render it extremely difficult to safeguard rights. For instance, India's Aadhaar Act stipulates that children shall not be denied access to any subsidy, benefit, or service as a result of failed biometric authentication, but does not provide any specific cause of action or remedy.[52] Most efforts to regulate the use of biometrics—and AI more broadly—have also failed to adequately engage affected communities in a meaningful, continuous way.[53] In Ireland, this was a core complaint about the expansion of the PSC's scope.

Blocked by the lack of remedies, civil society organizations have resorted to litigation to challenge biometric identification systems. A series of such court cases highlights impacts on equality, dignity, autonomy, health, and social security, and demonstrates some ways in which legal frameworks and norms can be applied to biometric technologies.[54] However, litigation is not an ideal mechanism, and challenges within litigation reflect broader difficulties regulating AI.[55] For instance, biometric identification projects often involve proprietary technology and are implemented quickly and with little transparency; litigants therefore face significant barriers to accessing information necessary to challenge these systems. Judicial timelines also mean that harms may continue, and often replicate and deepen, while awaiting review.

Pushback from civil society and affected communities has also demonstrated the limitations of a purely individual rights framework that does not sufficiently recognize disparate impact; many of the impacts of biometric technology are structural, dispersed, and affect groups collectively. For instance, the legal challenge to the national ID system in Kenya required individual plaintiffs to show that they, as a member of a particular *group*, had been directly disadvantaged through the disparate impacts of biometric

[47] *See* Séverine Awenengo Dalberto & Richard Banégas (eds.), *Identification and Citizenship in Africa: Biometrics, the Documentary State and Bureaucratic Writings of the Self*, https://www.taylorfrancis.com/books/9781000380033.

[48] *See generally* Linnet Taylor, *Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector*, PHIL. & TECH. (2021), https://doi.org/10.1007/s13347-020-00441-4; Julie Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, 2019.

[49] Ken Flottman, *Kenya's IEBC announced 18 months ago that it would finally open its vote tally servers to public, but has failed to do so*, AFRICOMMONS, Aug. 29, 2020, https://africommons.com/tag/france/; Duncan Miriri, *Kenyan opposition leader targets Safaricom staff over election*, REUTERS, Sept. 27, 2017, https://www.reuters.com/article/kenya-election-safaricom-idUSL8N1M81HK; Dalberto & Banegas (eds.), *supra* note 52.

[50] *See e.g.*, Keith Breckenridge, *The Global Ambitions of the Biometric Anti-Bank: Net1, Lockin and the Technologies of African Financialisation*, 33 INT'L REV. OF APP. ECON. 93–118, 2019, https://wiser.wits.ac.za/content/global-ambitions-biometric-anti-bank-net1-lockin-and-technologies-african-financialization; Robyn Foley & Mark Swilling, *How One Word Can Change the Game: Case Study of State Capture and the South African Social Security Agency, Stellenbosch: State Capacity Research Project*, 2018, https://www0.sun.ac.za/cst/publication/how-one-word-can-change-the-game-a-case-study-of-state-capture-and-the-south-african-social-security-agency-sassa/;

[51] Amba Kak, ed., *Regulating Biometrics: Global Approaches and Urgent Questions*, 2020, https://ainowinstitute.org/regulatingbiometrics.html.

[52] *Id.*

[53] Christopher Wilson, *Public Engagement and AI: A Values Analysis of National Strategies*, GOV'T INFO. Q. 101652, 2021, https://linkinghub.elsevier.com/retrieve/pii/S0740624X21000885.

[54] *See* Nubian Rights Forum, *supra* note 31; *Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors. Writ Petition (Civil) No. 494 of 2012 and Connected Matters* [India] (26 September 2018); Press Release: Civil Society Drags Government to Court Over Requirement to Have National ID Card Before Receiving Covid-19 Vaccine (2021), https://iser-uganda.org/images/downloads/COVID19_vaccine_and_IDs-ISER_Press_Briefing.pdf

[55] *See, e.g.*, Reetika Khera, "The poor are left to themselves," THE HINDU, Sept. 28, 2018, https://www.thehindu.com/opinion/lead/the-poor-are-left-to-themselves/article25074493.ece, last visited Jan. 14, 2022.

technologies.[56] Similar issues have emerged in the United States,[57] where victims of biased surveillance systems are left without constitutional protections.[58] Thus, it is crucial to establish definitions of group harms and indirect discrimination, as well as evidentiary standards for demonstrating disparate impact.

Each application of biometric technology deserves its own legal assessment of harm, as well as of its legitimacy, necessity, and proportionality. However, some have concluded that, on the evidence, such technologies pose such serious risks to human rights and democracy that the potential benefits are outweighed, necessitating a ban on the sale and use of these technologies.[59] Any steps taken by the U.S. government should seriously consider the gravity of these concerns.

IV. An international and comparative perspective is also necessary to reflect the global environment in which such technologies are being developed, used, and regulated

The United States plays a major role in the development and uptake of biometric technologies globally, through foreign investment, foreign policy, and development aid, as well as the activities of U.S. companies. The U.S. government has participated in *mandating* creation of biometric identification systems, such as through UN Security Council Resolution 2396, requiring states to "implement systems to collect biometric data" in order to "properly identify terrorists."[60] USAID provides active support for foreign governments' collection of biometric data, while the World Bank finances the development of biometric systems in dozens of countries.[61] U.S. government actors and companies influence critical decisions in standard setting bodies about specifications for biometric data collection devices and biometric data analysis.[62] Further, the Taliban's seizure of U.S. military biometric devices and data in Afghanistan demonstrates the immense ramifications of U.S. actions abroad.[63] The widespread use of biometric recognition at entry points at the Mexico border[64] further influences other governments around the world to follow suit.[65]

Meanwhile, the United States is one of the largest exporters of biometric surveillance technologies.[66] U.S. company L1 Identity Solutions was instrumental in the introduction of India's Aadhaar system, for

[56] Amnesty International, *Ban the Scan NYC*, https://banthescan.amnesty.org/nyc/, last visited Jan 13, 2022. *See also* Section II.

[57] Mutale Nkonde, *Automated Anti-Blackness: Facial Recognition in Brooklyn, New York*, Harv. Kennedy Sch. J. Afr. Amer. Pol., 2019–20. https://pacscenter.stanford.edu/wp-content/uploads/2020/12/mutalenkonde.pdf; Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. Times, Sept. 24, 2019, https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html.

[58] *United States v. Tuggle*, 4 F. 4th 505, 513 (7th Cir. 2021).

[59] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, Sept. 13, 2021, A/HRC/48/31, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.doc; *Amnesty International and more than 170 organisations call for a ban on biometric surveillance*, June 7, 2021, https://www.amnesty.org/en/latest/news/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.

[60] United Nations Security Council (UNSC) Res. 2396, Dec. 21, 2017, UN Doc S/RES/2396, https://undocs.org/S/RES/2396(2017). *See also* Krisztina Huszti-Orbán & Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* 2020, https://law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf.

[61] US Agency for International Development (USAID), *Introducing Biometric Data at Refugee Settlements in Uganda*, 2019, https://www.usaid.gov/news-information/videos/introducing-biometric-data-refugee-settlements-uganda; USAID, *Good Governance & Public Administration Strengthening Project (GGPAS)*, 2021, https://www.usaid.gov/kyrgyz-republic/fact-sheets/good-governance-public-administration-strengthening-project-ggpas; *USAID pilots biometrics to track youth health in Kenya*, Identity Week 2015, https://identityweek.net/usaid-pilots-biometrics-to-track-youth-health-in-kenya/.

[62] Joseph N. Pato and Lynette I. Millett, *The Biometrics Standards Landscape*, (National Research Council (US) Whither Biometrics Committee, 2010, https://www.ncbi.nlm.nih.gov/books/NBK219888/.

[63] Ken Klippenstein & Sara Sirota, *The Taliban Have Seized U.S. Military Biometrics Devices*, Intercept, Aug. 18, 2021, https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/; Eileen Guo & Hikmat Noori, *This is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban*, MIT Technology Review, Aug. 30, 2021, https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/; Verónica Arroyo & Donna Wentworth, *We Need to Talk About Digital ID: Why the World Bank Must Recognize the Harm in Afghanistan and Beyond,* Access Now, Oct. 14, 2021, https://www.accessnow.org/digital-id-world-bank/.

[64] *See, e.g.*, UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial and Xenophobic Discrimination, Emerging Digital Technologies, and Border and Immigration Enforcement*, 2020, UN Doc A/75/590, para. 47, https://antiracismsr.org/wp-content/uploads/2020/11/A_75_590_Advance-Unedited-Version.pdf. Immigrant Defense Project et al., *Factsheet: Freeze Expansion of the Hart Defense*, Apr. 2021, https://justfutureslaw.org/wp-content/uploads/2021/04/HART-Appropriations-2022.pdf; Todd Miller, *More than a Wall*, 2, 2019, https://www.tni.org/files/publication-downloads/more-than-a-wall-report.pdf.

[65] Petra Molnar, *Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up*, 2020.

[66] Steve Feldstein, *The Global Expansion of AI Surveillance*, 2019, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf; Valentin Weber and Vasilis Ververis, *China's Surveillance State: A Global Project*, 2021, https://www.nspirement.com/2021/09/01/chinas-digital-surveillance.html; Liza Lin & Josh Chin, *U.S. Tech Companies Prop Up China's Vast Surveillance Network*, Wall St. J., Nov. 26, 2019, https://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846;

example;[67] and U.S. companies such as Apple have also normalized the everyday use of biometric authentication.[68] These companies have been largely unfettered by legal or regulatory constraints in their experimentation with biometrics.[69] In large part, such initiatives have been paused only after public backlash and coordinated advocacy have forced companies to change course.[70] Meta's recent decision to shut down its facial recognition system and delete facial templates was explicitly driven by "societal concerns,"[71] but this came after Meta had been unconstrained in creating a database of over one billion faces; the company retains its DeepFace software and can resume use at any point.[72] Further, existing models of self-regulation are insufficient and do not provide meaningful constraints on the development and deployment of biometric technologies.[73]

Reticence in constraining U.S. technology companies' advancements has been driven by a dominant narrative of an "AI arms race" with China.[74] The National Security Commission on Artificial Intelligence (NSCAI) notes that China is setting a "chilling precedent."[75] Indeed, shocking reports detail the Chinese State's use of biometrics to facilitate surveillance and persecution of Uyghurs in Xinjiang.[76]

Yet U.S. government officials lament that technology companies in China can develop AI aided by unconstrained biometric data collection, claiming it is "not a level playing field."[77] This furthers the idea that "global AI leadership" requires low regulation, private sector access to troves of personal data, and expansive security use.[78] The NSCAI urges that the United States "must win the AI competition"[79] and identifies, somewhat uncritically, "surveillance," "clearing of regulatory barriers," and "enormous government stores of data" as factors enabling China "to leap ahead."[80] Viewing the development of AI-enabled biometric technologies through this competitive, national security paradigm risks that law, regulation, and human rights are sacrificed in efforts to "win."[81] The U.S. government must not allow a perceived AI arms race to dictate its approach to regulating biometric technologies.

Further, an arms race narrative simplifies complex realities around regulation in China itself.[82] Growing public controversy around facial recognition, combined with tensions with Chinese Big Tech companies, have led the Chinese government to introduce regulations, including regarding the use of biometric

[67] Unique Identification Authority of India, *Device Drivers,* https://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189

[68] *Face Biometrics Month: The Apple Effect and the Mainstreaming of Face Authentication*, FindBiometrics, 2019, https://findbiometrics.com/face-biometrics-month-the-mainstreaming-of-face-authentication-611140/.

[69] Kate Crawford et al., *AI Now 2019 Report*, 2019, https://ainowinstitute.org/AI_Now_2019_Report.html.

[70] *See* Rebecca Heilweil, *Big tech companies back away from selling facial recognition to police. That's progress.*, VOX, June 10, 2020, https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police.

[71] Jerome Pesenti, *An Update On Our Use of Face Recognition*, META, Nov. 2021, https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/.

[72] Rebecca Heilweil, *Facebook is backing away from facial recognition. Meta isn't*. Vox, Nov. 3, 2021, https://www.vox.com/recode/22761598/facebook-facial-recognition-meta.

[73] *See* Ben Wagner, *Ethics As An Escape From Regulation: From "Ethics-Washing" To Ethics-Stopping*? in Emre Bayamlioğlu et al. (eds.), *Being Profiled: Cogitas Ergo Sum: 10 years of Profiling the European Citizen*, 2018, https://www.cohubicol.com/assets/uploads/being-profiled-cogitas-ergo-sum.pdf.

[74] *See* Crawford et al., *supra* note 69; Daniel F. Runde, Romina Bandura, & Sundar Ramanujam, *The United States Has an Opportunity to Lead in Digital Development*, 2021, https://www.csis.org/analysis/united-states-has-opportunity-lead-digital-development; Amanda Macias & Kayla Tausche, *U.S. Needs to Work with Europe to Slow China's Innovation rate, Raimondo says*, CNBC, Sept. 28, 2021, https://www.cnbc.com/2021/09/28/us-needs-to-work-with-europe-to-slow-chinas-innovation-rate-raimondo-says.html.

[75] National Security Commission on Artificial Intelligence [NSCAI], *Final Report*, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[76] *See* Maya Wang, *The Robots Are Watching Us, Human Rights Watch*, 2020, https://www.hrw.org/news/2020/04/06/robots-are-watching-us; Olivia Shen, *AI Dreams and Authoritarian Nightmares*, in Jane Golley et al. (eds.), *China Story Yearbook: China Dreams*, 2020.

[77] *See* Macias & Tausche, *supra* note 74 .

[78] Crawford et al., *supra* note 69.

[79] NSCAI, *supra* note 75.

[80] National Security Commission on Artificial Intelligence [NSCAI], *Chinese Tech Landscape Overview: NSCAI Presentation*, May 2019, https://epic.org/wp-content/uploads/foia/epic-v-ai-commission/EPIC-19-09-11-NSCAI-FOIA-20200331-3rd-Production-pt9.pdf. *See also* Ryan Fedasiuk, *Chinese Perspectives on AI and Future Military Capabilities*, (Center for Security and Emerging Technology, 2020).

[81] Crawford et al., *supra* note 69; Kelsey Piper, *Why an AI Arms Race with China Would be Bad for Humanity*, VOX, Aug. 10, 2019, https://www.vox.com/future-perfect/2019/8/10/20757495/peter-thiel-ai-arms-race-china.

[82] Maya Wang, *China's Techno-Authoritarianism Has Gone Global*, FOREIGN AFFAIRS, Apr. 8 2021, https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global.

technologies.[83] The Supreme People's Court of China has issued regulations requiring companies to obtain consent before collecting and processing facial biometric data.[84] China's recent Personal Information Protection Law mandates data minimization and user consent across the private sector when processing "sensitive personal information" including biometric data. China appears to be taking seriously the need to regulate biometric technologies.

Meanwhile, the European Union (EU) is claiming a leadership role in regulating biometric technologies and protecting human rights. For instance, the EU seeks to prohibit outright some uses of mass biometric surveillance by law enforcement.[85]

The United States should view such attempts not as a ceiling, but rather a challenge to set standards even higher. Indeed, the EU's proposed AI Act has been critiqued for its overly-broad exceptions; unnecessarily restricting prohibition of remote biometric identification to law enforcement; and applying prohibitions only to "real-time" uses rather than continuing or post-hoc uses.[86] Further, the EU's proposed Act gives providers significant discretion to assess the risks of their own technologies;[87] it also fails to confer individual rights to those impacted by AI systems, or to provide for effective remedies where harms occur.[88] We encourage OSTP to look to these parallel efforts and strive to go further still.

The U.S. government must also take account of the far-reaching impacts that its decisions and regulation of U.S. companies already have worldwide: the extraterritorial application of technologies developed, produced, sold, and promoted by U.S. government agencies and U.S. corporations must come into the remit of the AI Bill of Rights.

V. Recommendations

The outcome of this RFI and the AI Bill of Rights should be a comprehensive governance framework, including relevant laws, policies, and plans for implementation, which emphasizes human rights, regulatory oversight, and effective enforcement. In order to achieve this, OSTP should therefore work towards the following recommendations:

1. **Impose an immediate moratorium for critical sectors**: Define, classify, and enact a moratorium on the use of mandatory AI-enabled biometric identification technology.[89] Such identification systems should never be mandatory in critical sectors such as education, welfare benefits programs, and health care, so as to preserve access to fundamental services.

2. **Invoke legal action to address the indirect and disparate impact of biometrics**: Propose and enact legislation that unequivocally applies the disparate impact doctrine, at a minimum in federal equal protection claims regarding the design and use of AI-enabled biometric identification technologies,

[83] *China Rebukes 43 Apps including Tencent's WeChat for Breaking Data Transfer Rules*, REUTERS, Aug. 18, 2021, https://www.reuters.com/business/retail-consumer/china-ministry-targets-43-apps-including-tencents-wechat-2021-08-18/; Josh Horwitz, *China Steps up Tech Scrutiny with Rules over Unfair Competition, Critical Data*, REUTERS, Aug. 17, 2021, https://www.reuters.com/business/media-telecom/china-issues-draft-rules-banning-unfair-competition-internet-sector-2021-08-17

[84] Supreme People's Court of China, Provisions on Relevant Issues on the Application of Laws in Hearing Civil Cases Related to the Application of Facial Recognition Technology in Processing Personal Information, July 28, 2021. *See also* Ananaya Agrawal, *China Supreme Court Issues Regulations Against Misuse of Facial Recognition Technology*, JURIST, Aug. 2021, https://www.jurist.org/news/2021/08/china-supreme-court-issues-regulations-against-misuse-of-facial-recognition-technology/.

[85] EU Member States are also taking steps to curb biometric technologies. *See* Koalitionsvertrag Zwischen SPD, Bündnis 90/Die Grüne, und FDP, Mehr Fortschritt Wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 2021, https://cms.gruene.de/uploads/documents/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf.

[86] *See An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement*, Nov. 30, 2021, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf [Hereinafter EU Civil Society Statement]; Nathalie A. Smuha et al., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act* (2021), https://papers.ssrn.com/abstract=3899991; Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act.* 22 COMP. L. REV. INT., 2021, 97, https://ssrn.com/abstract=3896852.

[87] Smuha et al., *Id*.

[88] *See* EU Civil Society Statement, *supra* note 86*;* Smuha et al., *supra* note 86.

[89] Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong., 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2052?q=%7B%22search%22%3A%5B%22Facial+Recognition+and+Biometric+Technology+Moratorium+Act+of+2021%22%5D%7D&s=1&r=1.

encompassing their implementation in administering access to public and private services. Such legislation should be designated implementing legislation in line with the ratification of the CERD, affording a private right of action for racially discriminatory effects of the deployment of AI-enabled technologies.

3. **Engage in further review of the human rights impact of biometrics and the components of different legal and regulatory approaches. This should include, *inter alia*:**
    a. Conduct and make public a comprehensive mapping of all federal systems currently or prospectively using biometric identification, including (1) the kinds of information collected, (2) the legal authority for collection and retention, (3) the purposes for which information is used, (4) how the information flows within public agencies, and (5) the impact of collection, retention, and sharing on rights.
    b. Conduct a comprehensive analysis of other countries' and regional bodies' efforts to develop binding legal frameworks to regulate AI-enabled biometric technologies. Distilling key lessons, the U.S. government should go beyond minimal standards to progress the field towards greater recognition and protection of human rights.

4. **Build a comprehensive legal and regulatory approach that addresses the complex, systemic concerns raised by AI-enabled biometric identification technologies, including:**
    a. Commit to adoption of AI-enabled biometrics within administrative agency operations only to the extent that adoption demonstrably furthers the justification for delegated authority. Subject such adoption and use to regular oversight and review.
    b. Establish clear safeguards for experimentation with these technologies, including but not limited to mandating rights-based impact assessments before a biometric technology can be piloted by the government or the private sector, and requiring a high level of justification, as well as suitable precautions, when such technologies are deployed first on marginalized groups such as migrants or welfare benefit recipients.
    c. Address both (and distinguish between) public and private use, individual and group rights, and domestic and international use and data-sharing.
    d. Place meaningful constraints on actions taken abroad. This includes U.S. companies' operations abroad with regard to marketing, sale, or transfer of biometric data and technologies, as well as the U.S. government's actions in spheres including, but not limited to, international development, counterterrorism, defense, and migration.

5. **Ensure that any new laws, regulations, and policies are subject to a democratic, transparent, and open process.** This should include, *inter alia:*
    a. Hold further consultations, proactive outreach to affected communities, and engagement outside of the United States.
    b. Ensure that public education materials and any laws, regulations and policies should be described and written in clear, non-technical, and easily accessible language.