2023

Collective Data Rights and Their Possible Abuse

Asaf Lubin
Maurer School of Law - Indiana University, lubina@iu.edu

COLLECTIVE DATA RIGHTS AND THEIR POSSIBLE ABUSE

Asaf Lubin[*]

INTRODUCTION

In her keynote address for this symposium, author and activist Nanjala Nyabola discussed the politics and technologies surrounding border crises. Nyabola masterfully and powerfully illustrated how physical borders have become "a millstone over the necks of foreigners."[1] Central to her thesis was the role that surveillance technologies and digitization have played in compounding and exacerbating the border crisis, further repressing immigrant and refugee communities.[2]

Nanjala Nyabola is not alone. Scholars, thought leaders, and advocates have long been ringing the alarm bells about the adverse effects of datafication, digitization, and automation on marginalized groups and collectives. In *Black Software*, for example, Charlton D. McIlwain describes how "computing technology was built and developed to keep black America docile and in its place."[3] In *Femtechnodystopia*, Leah Fowler and Michael Urlich discuss the role that period and fertility trackers have played in producing what they call a "femtechnodystopic panopticon," increasing reproductive surveillance

---

* Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, Fellow at IU's Center for Applied Cybersecurity Research, Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, Affiliated Fellow at the Information Society Project at Yale Law School, and a Visiting Scholar at the Federmann Cyber Security Center at Hebrew University of Jerusalem. I want to thank participants of the Temple University Institute for Law, Innovation & Technology and Temple Law Review joint symposium: "Sovereign Identity Crisis: State, Self, and Collective in a Digital Age." I further want to thank the editors and staff of the Temple Law Review for their excellent work in supporting this symposium and in putting together this publication. An early and significantly shorter version of these remarks was published in the Proceedings of the 116th Annual Meeting of the American Society of International Law, Seventh Annual Detlev F. Vagts Roundtable on Transnational Law: Transnational Regulation of the Platform Economy, at 125–27 (Apr. 8, 2022), https://doi.org/10.1017/amp.2019.121 [https://perma.cc/5DEX PPVE].

1. Asaf Lubin (@AsafLubin), TWITTER (Nov. 17, 2022, 7:20 AM), https://mobile.twitter.com/AsafLubin/status/1593262884427075585 [https://perma.cc/6HVC-8YXP].

2. *Id.* The UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, noted that:

> many digital border technologies substitute or aid human decision-making processes, sometimes in ways that raise serious human rights concerns. These technologies also expand the power and control that governments and private actors can exert over migrants, refugees, stateless persons and others, while simultaneously shielding this power from legal and judicial constraints. In other words, they magnify the potential for grave human rights abuses, and do so in ways that circumvent substantive and procedural protections that have otherwise been essential in the border enforcement context.

E. Tendayi Achiume (Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance), *Rep. of the Special Rapporteur on Cotemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance*, ¶ 19, U.N. Doc. A/75/590 (Nov. 10, 2020).

3. CHARLTON MCILWAIN, BLACK SOFTWARE: THE INTERNET AND RACIAL JUSTICE, FROM THE AFRONET TO BLACK LIVES MATTER 7 (2020).

and thereby jeopardizing the "privacy, autonomy, and personal sovereignty" of women everywhere.[4] Others have studied the weaponization of queer data on geosocial dating apps[5] and the censorship of queer speech on social media platforms.[6] And there are even more abuses for marginalized communities, as commercial data practices "facilitate voter suppression, digital redlining, discriminatory policing, retail discrimination, digital inequity, the amplification of white supremacy, identity theft, [and] the endangerment of personal safety."[7]

Against this backdrop of unprecedented technologically enabled targeting of marginalized groups, we are witnessing an evolution in human rights discourse. In the past, the premise was that existing human rights law was elastic enough to address these abuses—that applying traditional human rights in online spaces would curtail these abuses[8]—that tenor has now shifted. Scholars are now arguing that "effective protection of human rights in cyberspace cannot be achieved by relying solely on existing international human rights law and that existing rights need to be adapted and complemented by new digital human rights."[9] Civil society organizations have therefore begun to develop new soft law instruments that seek to introduce tailored and emerging rights for the digital age.

One such instrument is the Internet Rights and Principles Coalition's (IRPC) Charter of Human Rights and Principles for the Internet. The IRPC charter, which was launched in 2011, is now in its eighth iteration. The charter aims to become an "authoritative document" that could frame "emerging rights-based norms for the local, national, and global dimensions of internet governance."[10] Among the many new digital rights affirmed by the IRPC charter are the right to digital inclusion, the protection of

4. Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. (forthcoming 2023) (manuscript at 37, 41), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4099764 [https://perma.cc/HQG7-MAWS].

5. *See* ARTICLE 19, APPS, ARRESTS, AND ABUSE IN EGYPT, LEBANON AND IRAN (2018), https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_21.2.pdf [https://perma.cc/Q24H-AHP5].

6. *See* Ari Ezra Waldman, *Disorderly Content*, 97 WASH. L. REV. 101 (2022).

7. BECKY CHAO, ERIC NULL, BRANDI COLLINS-DEXTER & CLAIRE PARK, NEW AM., CENTERING CIVIL RIGHTS IN THE PRIVACY DEBATE 5 (2019), https://d1y8sb8igg2f8e.cloudfront.net/documents/ Centering_Civil_ Rights_in_the_Privacy_Debate_2019-09-17_152828.pdf [https://perma.cc/VZK5-PVFH].

8. *See, e.g.*, Human Rights Council Res. 20/8, ¶ 1 U.N. Doc. A/HRC/RES/20/8 (July 16, 2012) ("Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."); G.A. Res. 69/166, ¶ 3, U.N. Doc. A/RES/69/166 (Feb. 10, 2015) ("Affirms that the same rights that people have offline must also be protected online, including the right to privacy."); Dafna Dror-Shpoliansky and Yuval Shany call this the "normative equivalency paradigm." Dafna Dror-Shpoliansky & Yuval Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology*, 32 EUR. J. INT'L. L. 1249, 1251 (2021).

9. Dror-Shpoliansky & Shany, *supra* note 8, at 1281–82; *see also Rep. of the Special Rapporteur on the Right to Privacy*, ¶ 6, U.N. Doc. A/HRC/37/62, (Oct. 25, 2018) ("When dealing with technologies such as the Internet it is simplistic and naïve to be content with a statement that 'whatever is protected off-line is protected on-line.' That is a hopelessly inadequate approach to the protection of privacy in 2018.").

10. INTERNET RTS. & PRINCIPLES COAL., CHARTER OF HUMAN RIGHTS AND PRINCIPLES FOR THE INTERNET 2 (8th ed. 2022), https://drive.google.com/file/d/1HgsgI1-Irxe_3angb8GJoIdlK9nScaEi/view [https://perma.cc/76MS-ABL6].

virtual personality, the right to digital data protection, rights to net neutrality and net equality, and the right to enjoy secure connections to and on the internet.[11]

This changing human rights discourse does not stop at the formulation of new digital rights, however. It extends towards a third generation of rights, whereby the very categories of right holders and duty bearers may be reconceptualized. As Dafna Dror-Shpoliansky and Yuval Shany write, this wave of categorization rebooting is "required in order to adequately capture new power configurations and social interactions in cyberspace, so as to effectively address new risks to the basic online needs and interests of individuals and groups of individuals."[12]

This short reflection looks at one controversial category reboot in the governance of emerging digital rights, the recent proposals for the establishment of a unique set of new right holders: collectives. In my brief remarks, I wish to direct our attention to this elusive and evolving concept of "collective data rights" and its relationship with sovereignty. In this piece, I wish to highlight the transnational risks associated with formal recognition of communitarian rights over data under international human rights law. While not rejecting the prospects of such an endeavor wholesale, the paper merely calls for greater caution and nuance in the development of such rights. This Essay proceeds in two Sections. Section I maps out current proposals for the formulation of "collective data rights" and the motivations behind them. Section II applies the political science concept of "unjust collectivities" in the context of collective data rights to demonstrate some of the potential risks associated with this emerging discourse. Finally, I conclude by proposing a middle ground for advocates writing in this space.

I. COLLECTIVES IN THE INFORMATION SOCIETY

We have truly entered a new epoch of communitarianism in the regulatory discourse surrounding our digital economy. Everywhere you go the talk of the town is collectivism. Imagine a lively, loud, and vibrant bazaar, like a Turkish spice market with rows of colorful stalls. We may call this grand bazaar "*the marketspace of data governance ideation*."

In it you will find merchants of all shapes and sizes, each trying to sell you on their own particularized version of the future of data protection. One salesman is all in on data

11. *Id.* at 14–29.

12. Dror-Shpoliansky & Shany, *supra* note 8, at 1269.

cooperatives,[13] another is committed to data collaboratives,[14] a third is just convinced the future is in data trusts,[15] and a fourth is so certain the right approach is data stewards that he will bet his house on it.[16] And there are even more merchants out there promoting

13. *See* JONATHAN VAN GENUS & ANA BRANDUSESCU, MOZILLA INSIGHTS, SHIFTING POWER THROUGH DATA GOVERNANCE 9 (2020) [hereinafter MOZILLA INSIGHTS], https://assets.mofoprod.net/network/documents/ShiftingPower.pdf [https://perma.cc/9DM2-VR2L] ("A data cooperative is a legal construct to facilitate the collaborative pooling of data by individuals or organizations for the economic, social, or cultural benefit of the group. The entity that holds the data is often co-owned and democratically controlled by its members. . . . One example is Driver's Seat, a cooperative of on-demand drivers who gather their own combined driving data in an app to gain insights that are usually kept secret by employers like Uber. When Driver's Seat sells mobility data to city agencies they share profits with drivers. In this way, cooperatives can shift power to data subjects, who typically have very few rights in mainstream ventures."); *see also* Thomas Hardjono & Alex Pentland, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, MIT CONNECTION SCIENCE (2019), https://arxiv.org/pdf/1905.08819.pdf [https://perma.cc/N3E3-M88M] ("The notion of a data cooperative refers to the voluntary collaborative pooling by individuals of their personal data for the benefit of the membership of the group or community. The motivation for individuals to get together and pool their data is driven by the need to share common insights across data that would be otherwise siloed or inaccessible. These insights provide the cooperative members as a whole with a better understanding of their current economic, health and social conditions as compared to the other members of the cooperative generally."); Ernst Hafen, Donald Kossmann & Angela Brand, *Health Data Cooperatives – Citizen Empowerment*, 53 METHODS INFO. MED. 82, 86 (2014).

14. *See* MOZILLA INSIGHTS, *supra* note 13, at 12 ("A data collaborative is often what you have when private sector data is combined to help inform public sector decisions. At least this is one aspect. Data in a collaborative could be shared strictly between partners, with an independent third party who manages access to the data, or publicly online."); *see also* Stefaan G. Verhulst & Andrew Young, *The Potential and Practice of Data Collaboratives for Migration*, *in* GUIDE TO MOBILE DATA ANALYTICS IN REFUGEE SCENARIOS: THE 'DATA FOR REFUGEES CHALLENGE' STUDY 465, 470, 473 (Albert Ali Salah, Alex Pentland, Bruno Lepri & Emmanuel Letouzé eds., 2019) ("We use the term [data collaboratives] to refer to an emergent form of public-private partnership that allows for collaboration and information sharing across sectors and actors. This model has now been used in a variety of sectors and geographies, ranging from sharing disease data to accelerate disease treatments to leveraging private bus data to improve urban planning.").

15. *See* MOZILLA INSIGHTS, *supra* note 13, at 13 ("A data trust is a legal relationship where a trustee stewards data rights in the sole interests of a beneficiary or a group of beneficiaries. When a person or group hands over their data to a trustee, it means the trustee has a fiduciary duty to act according to predefined terms and conditions and never in their own self interest. Data can be pooled from different sources, and a trustee can negotiate access by others on behalf of the collective. As a legal framework, trust law only exists in some parts of the world (including, the UK, US, and Canada) but fiduciary duties often still exist outside of trust law jurisdictions, for instance when a legal representative handles the estate of a deceased person on behalf of a group of specific beneficiaries."); *see also* George Zarkadakis, *"Data Trusts" Could Be the Key to Better AI*, HARV. BUS. REV. (Nov. 10, 2020), https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai [https://perma.cc/EVZ6-748S] ("That legal and governance setup obliges the data trust administrators (the 'fiduciaries') to represent and prioritize the rights and benefits of the data providers when negotiating and contracting access to their data for use by data consumers, such as other private companies and organizations."). *But cf.* João Marinotti, *Data Types, Data Trusts, and Data Doubts*, 97 N.Y.U. L. REV. ONLINE 146, 170 (2022) (discussing "unanswered questions that will hinder the adoption of data trusts as a means of private data governance").

16. *See, e.g.*, Anouk Ruhaak & Ashta Kapoor, *What Is Data Stewardship, and How Could It Address Questions of Power Imbalance in the Data Economy?*, HEINRICH BÖLL STIFTUNG (Dec. 30, 2021), https://il.boell.org/en/2021/11/18/data-stewardship [https://perma.cc/E9CV-KG89] ("A data steward is an independent intermediary or agent who acts on behalf of the subjects of the data and/or those affected by its collection and use. For instance, a diabetes patient might wish to make data available to medical researchers hoping to cure diabetes. Instead of individually deciding about which person or organization should receive access to their data, they could hand that decision-making power to a data steward. Stewards are especially useful

novel concepts like data sharing pools,[17] data commons,[18] data altruisms,[19] data fiduciaries,[20] and data marketplaces and unions.[21] Truly it is exhausting just to try to keep abreast of all the banners at the top of each of the different booths.

These collective data governance concepts did not appear out of thin air. They represent broader notions of ownership common in most domestic regimes of property and contract law. But interestingly the discourse around data communitarianism has also permeated upwards and has recently entered the field of public international law. So,

---

in situations where we cannot rely solely on individual consent to decide how data should be collected, accessed, and used. This is the case when data is about more than one person, and particularly when the collection, access and use of data comes with risks and benefits not just to the individual subject, but also to society in general.").

17. *See, e.g.*, Marina Micheli, Marisa Ponti, Max Craglia & Anna Berti Suman, *Emerging Models of Data Governance in the Age of Datafication*, 7 BIG DATA & SOC'Y 1, 7 (2020) ("Different actors join a [Data Sharing Pool] to 'analyse each other's data and help fill knowledge gaps while minimizing duplicative efforts.' By creating these partnerships, they ease the economic need for exclusive rights and obtain limited co-ownership stakes in the resulting data pool. Data is treated and exchanged as a market commodity with the aim of producing data-driven innovation, new services, and economic benefits for all the parties involved. . . . Governance mechanisms for [Data Sharing Pools] include technical architectures, such as data sharing platforms and Application Program Interfaces (APIs), which facilitate a centralised data exchange within business ecosystems." (citations omitted) (quoting Jennifer Shkabatur, *The Global Commons of Data*, 22 STAN. TECH. L. REV. 354, 390 (2019))).

18. *See, e.g.*, MOZILLA INSIGHTS, *supra* note 13, at 10 ("In a data commons, data is pooled and shared as a common resource. This approach can address power imbalances by democratizing access to and availability of data. Often, a data commons is accompanied by a high degree of community ownership and leadership and has a public good cause.").

19. *See, e.g.*, Carina Kruesz & Felix Zopf, *The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU*, 7 EUR. DATA PROT. L. REV. 569, 570 (2021) (citing the European Commission Data Governance Act's definition of data altruism: "[T]he consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services." (internal quotation marks omitted)).

20. *See, e.g.*, MOZILLA INSIGHTS, *supra* note 13, at 15 ("A data fiduciary is an intermediary between individuals and data collectors, which takes many experimental forms. These range from 'information fiduciaries' that focus on use of fiduciary law to require a 'duty of care' toward data subjects, to various intermediary technologies or storage solutions that act as a buffer between people's personal data and any commercial entities or online interactions. . . . The concept of an 'information fiduciary' was explored by Jack M. Balkin and Jonathan Zittrain in 2015/16 sparking continued discourse over the conflicts of interest inherent to a digital surveillance economy and how to generate new pathways for trust. Under the fiduciary umbrella, some scholars would also include advanced tech tools that act as trusted intermediaries (or 'trustmediaries') like personal AIs, identity layers, or personal data pods, and cloudlets. These are all approaches that recognize the significant power asymmetries that occur online between consumers and those who have access and control over personal data.").

21. *Id.* at 18 ("A data marketplace is an approach that enables consumers to sell or trade their personal data for services or other benefits. . . . The questions posed through this approach are multiple. Why shouldn't people be paid for data that big tech profits from? How could you develop interoperable systems to transfer data between platforms? Could it lead to more transparency around processing and algorithms? Critiques of this approach can be scathing, suggesting that data marketplaces incentivize data collection that should not happen in the first place. Bypassing data brokers that operate in the shadows may sound appealing as a business model, but critics argue that it promotes a commodification of personal data that is core to what is already wrong with the surveillance economy. In theory, it is imagined that customers of data marketplaces could pool their data for collective bargaining (similar to credit unions where people pool their finances for the collective benefit of members). Members could own and manage such 'data unions' and at the same time earn profits from aggregated data.").

with apologies, I will have to describe yet another grand, lively, colorful, and vibrant bazaar. One merchant here promotes the idea that self-determination rights of peoples could help fight election interference.[22] Another merchant believes that the collective rights of the civilian population occupied territories could defend against the use of advanced surveillance technologies like facial recognition.[23] A third is committed to the concept of digital cultural rights as a means of responding to internet shutdowns and censorship.[24] And a fourth is an advocate for indigenous data sovereignty as a tool in the toolkit in the fight against colonialism and postcolonialism.[25]

I acknowledge that there are few connecting threads between each of these merchants across these different bazaars. And yet, one thing they all share is a common enemy. All of these norm entrepreneurs repudiate a capitalistic, neoliberal, dignitarian, individual-rights-based, Eurocentric model of data governance.[26] By focusing on the horizontal relations in the digital economy, this epistemic community of social constructivists is hoping to uncover and thereby disturb power structures that undergird our contemporary datasphere.[27] Their goal is to demonstrate how datafication may lead

22. *See* Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1596 (2017) ("The election process is the ultimate expression of a people's sovereign will. By illicit interference, the Russians influenced the election to produce the sovereign will of the Russian people (or its government), rather than the sovereign will of the American people. . . . The interference substituted one sovereign will for the other as an outcome of the election. Doing so violated the right of the American people to self-determination."); *see also* JENS DAVID OHLIN, ELECTION INTERFERENCE: INTERNATIONAL LAW AND THE FUTURE OF DEMOCRACY (2020).

23. *See* Rohan Talbot, *Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory*, 102 INT'L. REV. RED CROSS 823, 849 (2020) ("Where deployed within an Occupying Power's measures of control and security, [facial recognition technologies] sit at the fulcrum of the law of occupation's central balance between the Occupying Power's security interests and the humanitarian interests of protected persons."); *see also* Eian Katz, *Liar's War: Protecting Civilians from Disinformation During Armed Conflict*, 102 INT'L. REV. RED CROSS 659, 682 (2021) (setting a "theoretical foundation for further efforts" in mapping the collective rights of civilian populations to fight against disinformation during times of armed conflict).

24. *See* Ilze Brands Kehris, *Internet Shutdowns*, U.N. OFF. OF THE HIGH COMM'R FOR HUM. RTS. (Sep. 21, 2022), https://www.ohchr.org/en/statements-and-speeches/2022/09/internet-shutdowns [https://perma.cc/2G77-TYLH] ("To deliberately shut down access to the internet – whether through full shutdown, bandwidth throttling, blocking of mobile services or other means – is a powerful tool of control. Control over what kind of information can be accessed or shared, and with far-reaching consequences on a range of human rights, including social, economic and cultural rights.").

25. *See* MOZILLA INSIGHTS, *supra* note 13, at 16 ("Indigenous data governance is about shifting access and control over data away from governments and other institutions and directly to Indigenous Peoples. This includes information about territories, natural resources, and people, as well as about collectively owned knowledge and intellectual property. Considering how often the withholding of information has been used as a vector of subjugation and control worldwide, it's a data governance approach that illustrates how important data sovereignty can be to self-determination and justice.").

26. For a general literature review of core pillars and themes in data justice, see GLOB. P'SHIP ON A.I., ADVANCING DATA JUSTICE RESEARCH AND PRACTICE: AN INTEGRATED LITERATURE REVIEW (2022), https://gpai.ai/projects/data-governance/advancing-data-justice-research-and-practice-literature-review.pdf [https://perma.cc/84F9-UCQJ].

27. *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 613 (2021) ("While horizontal data relations are of primary importance in explaining why data collectors develop infrastructures to collect and monetize data flows, they do not feature much, if at all, in how current data-governance law allocates claims, privileges, and duties among actors in the digital economy.").

to unfair wealth inequality while reproducing and amplifying forms of social hierarchy.[28] Each of their proposals is simply a response, albeit of different magnitudes and kinds, to this underlying economic and political scaffolding.[29] As Julie Cohen has summed up, existing legislation on data collection and processing rely as a "primary mechanism" on property notions of individual rights "with no or only residual provision for ongoing governance at the collective level."[30] Yet, "[a]tomistic, post hoc assertions of individual control rights . . . cannot meaningfully discipline networked processes that operate at scale."[31]

To understand this idea better, consider for example Salomé Vilojen's groundbreaking Yale Law Journal Article *A Relational Theory of Data Governance*.[32] Salomé rejects the now dominant individualistic approach to data governance and replaces it with what she calls a "population-level" analysis.[33] By merely changing the point of view from the individual data subjects to the society they form a part of, Salomé reveals new previously undiscovered sets of pressure points along the complex and interrelated system that makes up the datasphere.[34] This is what leads her to her normative claim, that we need to redesign our institutions so as to appreciate data not as an individual medium but as a democratic medium, which is a medium better suited, in her view, to embody broader societal interests.[35] Collective data governance, as an ideational approach, is thus a form of social resistance as it brings together groups of individuals who otherwise would not realize they are bound together by chains of corporate and governmental digital abuse.[36] Rising up as a community, the theory goes, will empower these groups to unshackle themselves from the merciless markets that profited off their impoverishment.[37]

II. THE RISK OF UNJUST COLLECTIVITIES

We are at an inflection point. This move from individual digital rights to communitarian digital activism is truly the current state of the art. And like any inflection

28. *Id.* at 653.

29. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 362 (2022) (describing how data aggregation and machine learning help identify correlative patterns which are then used probabilistically to make inferences about society and its members in a way that "disempowers individuals about whom inferences are made, yet who have no control over the data sources from which the inferential model is generated").

30. JULIE E. COHEN, HOW (NOT) TO WRITE A PRIVACY LAW, KNIGHT FIRST AMEND. INST. 4 (Mar. 23, 2021), https://s3.amazonaws.com/kfai-documents/documents/306f33954a/3.23.2021-Cohen.pdf [https://perma.cc/9AGG-RP8S].

31. *Id.*

32. Viljoen, *supra* note 27.

33. *Id.* at 580 ("[D]ata's relationality results in widespread population-level interests in data collection and use that are irreducible to individual legal interests within a given data exchange. Contending with the economic realities of data production thus expands the task of data-governance law: from disciplining against forms of interpersonal violation to also structuring the rules of economic production (and social reproduction) in the information economy.").

34. *See id.*

35. *Id.* at 634–53.

36. *See id.*

37. *See id.*

point, it holds great promise but also poses great risk. Writing nearly three decades ago, Michael Freeman wrote one of the most cited defenses to the concept of collective human rights in political theory. In *Are There Collective Human Rights?*, Freeman describes in powerful and passionate language the importance of recognizing collective rights in the international community.[38] Yet, in concluding his Essay even Freeman acknowledges that "[t]he theoretical concept of collective human rights cannot solve the practical problems posed by unjust collectivities," that is "[the] capitulation to collective demands that are unjust."[39] Freeman wrote this but never expanded further. He merely advocated that supporters of individual autonomy and collective solidarity should come together to engage in further dialogue.[40]

Any advocate for collective digital rights should be mindful of the risks of "unjust collectivities," because collective digital rights are particularly susceptible to this form of abuse. It is important to recognize that group identity and population-level identity are to some extent arbitrary, certainly online. Unlike a universal standard that applies uniformly to all people, group rights require a clear delimitation line between members of the *in-group* and members of the *out-group*. Collective rights are thus by design intended to exclude. Indeed, as Brownlie wrote, "[t]he establishment of a definition of membership . . . is a delicate matter."[41] While the original motivation of its promoters might have been to protect minority rights and empower marginalized communities, abusers of the system could use the language of collective identity to exclude these very groups and subject them to even further harm.

Take for example the concept of sovereignty in China as discussed by Maria Carrai.[42] After exploring the genealogy of the concept in Chinese literature going back to 1840, she concludes that "China is attempting to affirm its national identity and preserve its own path to modernity through the idea of cultural sovereignty."[43] In other words, China is using the collective interests rooted in the contested concept of sovereignty to promote its efforts in empire building. The concept is contextually and instrumentally employed to push forward state aspirations at the expense of minority groups, like the Uyghurs. This has manifested in the digital space too.

China has unleashed wholesale monitoring and tracking of Uyghur individuals, including biometric data collection of facial imagery and iris scans and genomic

38. *See* Michael Freeman, *Are There Collective Human Rights?*, 43 POL. STUD. 25, 38–40 (1995) ("Some human-rights theorists argue either that there are no collective human rights or that there are collective human rights but all such rights are derivative from individual human rights. . . . Collective human rights are, however, not reducible to individual human rights. The right to collective self-determination is not reducible to any set of individual human rights, though it may be dependent on and necessary for such rights . . . . Collective human rights are necessary in some situations for justice and peace. . . . The concept of collective human rights, therefore, helps to reconcile the values of liberal universalism and cultural pluralism, and thereby provides a theoretical framework for practical policies that might reconcile justice and peace.").

39. *Id.* at 40.

40. *Id.*

41. Ian Brownlie, *The Rights of Peoples in Modern International Law*, *in* THE RIGHTS OF PEOPLES 1, 7 (James Crawford ed., 1988).

42. MARIA ADELE CARRAI, SOVEREIGNTY IN CHINA: A GENEALOGY OF A CONCEPT SINCE 1840 (1999).

43. *Id.* at 223.

surveillance through mandatory DNA sampling.[44] China is relying on collective right arguments, namely those of absolute sovereignty and nonintervention in domestic affairs, to further crush dissent in the Xinjiang region.[45] Control over data and technology, through the Great Firewall, is thus part of a "collective story" that only further entrenches oppression.[46] In summary, once the language of collectivism becomes part and parcel of digital rights discourse, there is nothing stopping totalitarian regimes from utilizing that very language to advance injustice.

A second concern has to do with the content of collective rights. Since these rights are "culturally specific[] and time-bound,"[47] their exact scope and meaning evades precise capture. Unlike the universal understanding of individual rights, collective rights have a murky place in customary international law. For this reason, the "1948 Universal Declaration of Human Rights, which is the framework of principles underpinning the modern international human rights system, made no explicit references to collective rights."[48] If we are to prioritize the collective over the individual, we are potentially inviting a rejection of a universal minimum baseline of data subject rights. In fact, we might be exchanging this governance system for a far riskier competition between societies, all equally entitled on the horizontal plain to insist that their national data governance model is legitimate, effective, and should indeed control.[49] As countries and companies race to the bottom in their boisterous attempts to commodify data and win the AI arms race, do we really need to legitimize and incentivize this kind of competition?

Consider the expansive internet-balkanizing data localization policies of India and Nigeria,[50] the informational censorship frameworks in the Philippines,[51] or the government data access regimes in Indonesia and Brazil.[52] In a future world where

---

44. Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. To Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/K9JU-JNWA]; Tara Francis Chan, *A Chinese Province Is Collecting DNA and Iris Scans from All Its Residents*, BUS. INSIDER (Dec. 13, 2017), https://www.businessinsider.com/china-collects-dna-fingerprints-biometrics-from-residents-human-rights-watch-2017-12 [https://perma.cc/NR32-8H2Z].

45. *See* Mozur, *supra* note 44; Chan, *supra* note 44.

46. Yaqiu Wang, *In China, the 'Great Firewall' Is Changing a Generation*, POLITICO (Sept. 1, 2020), https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 [https://perma.cc/ED3R-8EYS].

47. AARON RHODES, HERITAGE FOUND., HOW "COLLECTIVE HUMAN RIGHTS" UNDERMINE INDIVIDUAL HUMAN RIGHTS 17 (June 25, 2020), https://www.heritage.org/sites/default/files/2021-06/SR227_0.pdf [https://perma.cc/MY9D-ECS7].

48. *Id.* at 5.

49. *See id.* at 18 ("Collective human rights threaten the idea, and enjoyment, of human rights insofar as they empower assertions that the rights of a group, or the state itself, can be of higher value than the rights of the individual.").

50. *See, e.g.*, Neha Mishra, *Data Localization Laws in a Digital World: Data Protection or Data Protectionism*, 4 PUB. SPHERE 135, 137 (2016).

51. *See, e.g.*, FREEDOM HOUSE, FREEDOM OF THE NET: PHILIPPINES (2021), https://freedomhouse.org/country/philippines/freedom-net/2021 [https://perma.cc/FBC5-VDRP].

52. *See, e.g.*, Bruno Magrani, *Systemic Government Access to Private-Sector Data in Brazil*, *in* BULK COLLECTION: SYSTEMIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 129 (Fred H. Cate & James X. Dempsey eds., 2017); Rainer Heufers, *Less Freedom for Indonesia's Internet*, E. ASIA F. (Nov. 12, 2022),

cultural relativism could become the crux of all digital rights, how can we meaningfully fight against these emerging legal frameworks around the world? Are these data governance regimes not ringing the alarm bells for what could happen if we somehow prioritized collective, relative, and culturally specific approaches to data governance over an individualistic baseline? And what would be the implications on markets and the broader balance of power if we encouraged further great power competition between jurisdictionally encroaching societally motivated data-hungry sovereigns?

Shortly after Russian forces took over Kherson in Ukraine, they ordered internet service providers at gun point to relinquish control over their networks.[53] "Russian authorities then rerouted mobile and internet data from Kherson through Russian networks" thereby blocking access "to Facebook, Instagram and Twitter, as well as to Ukrainian news websites and other sources of independent information. Then they shut off Ukrainian cellular networks, forcing Kherson's residents to use Russian mobile service providers instead."[54] Russia used data control as a form of population manipulation and reengineering in the leadup to the false referendums on the annexation of the territories it occupied.[55] Some have suggested that the Russian rerouting efforts reflect a Russian agenda to weaponize the internet; that its internet occupation seeks to control the minds and mouse clicks of millions of Ukrainians to introduce fake news and Russian propaganda.[56] If national collectives—the polities through their representatives—get to have a final say about how they want data to be governed; if they are granted sole possession and full control over the moderation standards they wish to set for themselves and their peoples; and if they then use that control to promote authoritarian viewpoints on informational privacy, online speech, data protection, internet access, and cybersecurity; what claims could be raised to push back against them in a postcollective data governance world?

---

https://www.eastasiaforum.org/2022/11/12/less-freedom-for-indonesias-internet/ [https://perma.cc/FQ8X-L6PB].

53. Adam Satariano, *How Russia Took Over Ukraine's Internet in Occupied Territories*, N.Y. TIMES (Aug. 9, 2022), https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html [https://perma.cc/ZCX9-YST3].

54. *Id.*; *see also*, Vera Bergengruen, *The Battle for Control Over Ukraine's Internet*, TIME (Oct. 18, 2022), https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/ [https://perma.cc/9TU6-JNLM] ("Russia's attempts to control the flow of information have been extensive. More than 4,000 base stations belonging to Ukrainian telecommunications providers have been seized or destroyed by Russian soldiers since the beginning of the invasion, and more than 60,000 kilometers of fiber-optic lines used for Internet have been captured or damaged, according to Ukraine's Special Communications Service. Russian forces also destroyed 18 broadcasting antennas that provided television and radio signal. In some areas of southern Ukraine, Russia appears to have rerouted Internet traffic through their own providers, exposing it to the Kremlin's vast system of surveillance and censorship.").

55. Matt Burgess, *Russia is Taking Over Ukraine's Internet*, WIRED (June 15, 2022), https://www.wired.com/story/ukraine-russia-internet-takeover/ [https://perma.cc/QHS9-BUZX].

56. *Id.* (citing Liliia Malon, the commissioner of Ukraine's telecom regulator, who noted that "rerouting of the internet in occupied Ukrainian areas . . . has the goal of spreading 'Kremlin propaganda' and making people believe Ukrainian forces have abandoned them.").

CONCLUSION: WHERE SHOULD WE GO FROM HERE?

We are all disenchanted with individual human rights law. Indeed, as Gráinne de Búrca writes, "the language and concepts of human rights were taken up and co-opted by advocates of global capitalism and economic liberalism in an effort to give overwhelming if not exclusive emphasis . . . to the right to property and freedom of contract as justification for their preferred economic and political ideology."[57] It is truly naïve to think there is some universal right to privacy or data protection,[58] and the practice of states in cyberspace demonstrates just how frustrating the tension is between the mythical law in the books and the law in action, especially in the wake of the *lex mercatoria* of contemporary data broker markets.

As João Marinotti wrote, the "rapid expansion of the datasphere . . . cement[s] the need for data governance strategies that successfully balance scientific innovation, economic prosperity, personal privacy, and individual autonomy, among the many other interests at stake currently being discussed in this rapidly evolving field of research."[59] With that in mind, it is certainly not my contention that collective data rights projects be rejected or flat out denounced. No, quite the opposite, they are inspiring, understandable, and laudable projects.[60] Or as Freeman wrote, the fact that collective rights produce "conceptual confusion and political danger" should *not* result in a rejection of communitarian rights but rather in further scrutiny of them towards making them better.[61] We should be cautious in recognizing them and in applying them, but not fight them. The threat that technology now poses to marginalized groups demands of us to develop "more sophisticated understandings of collective harm and obligation, and of the ways that design interventions can protect both individual and collective values."[62]

What worries me is that the current discourse is situated around a zero-sum game. Efforts in identifying new collective rights approaches and regulations seem to be in competition with existing individual rights models. Certain scholars and policy makers are falsely pitting them against each other.[63] You must choose; favor one or the other. Not both. This is a dangerous dichotomy in my view.

---

57. Gráinne de Búrca, Book Review, 16 INT'L J. CONST. L. 1347, 1348 (2018).

58. *See generally* Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 CHI. J. INT'L. L. 502 (2018).

59. Marinotti, *supra* note 15, at 172.

60. Indeed, as Ayelet, Alexandra, and Katrina have written, "the collective, interdependent nature of personal data means that no single individual can decide on their own how much data they want to disclose to platforms, or what data they want to keep private. Therefore, any intervention in the data ecosystem must be grounded in a deep understanding of the strong collective nature of data and the various dependencies that characterize data." Any effort to understand this *collective nature of data* is foundational and crucial. Ayelet Gordon-Tapiero, Alexandra Wood & Katrina Ligett, *The Case for Establishing a Collective Perspective To Address the Harms of Platform Personalization*, VAND. J. ENT. & TECH. L. (forthcoming 2023) (manuscript at 20), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105443 [https://perma.cc/8K3M-39RP].

61. Freeman, *supra* note 38, at 39.

62. Julie E. Cohen, *From Lex Informatica to the Control Revolution*, 36 BERKELEY TECH. L.J. 1017, 1045 (2021).

63. *See e.g.*, Linnet Taylor, *What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally*, 4 BIG DATA & SOC., 2017, at 4, https://doi.org/10.1177/2053951717736335 [https://perma.cc/5VVU-69DP] ("Until now, within the global North freedoms and needs with regard to data technologies have been approached through a fundamental rights framework that includes data protection,

Instead, I would invite anyone who is interested in exploring these arguments of collective data governance to think more about the way such frameworks could supplement and build around our existing individual models rather than replacing them.[64] Such complementarity, I think, offers the best prescriptive solution to the current challenges we face in the datasphere.

framings of informational privacy and the right to free speech and communication. However, this framing presents two problems when applied in relation to the global data market. First, the liberal individual framing of Human Rights requires that abuses are clear and visible so that those injured can respond, and second, it assumes that redress will be sought on the individual level. This is rendered problematic by the invisible and many-to-many nature of 'seeing' through data technologies, but also by the fact that many of the negative impacts of data occur on the group as much as the individual level. Instead of applying a fundamental rights framework whose application demands Identifiable violations, this new situation requires a more multifaceted approach that can address the breadth of actors and possibilities inherent in contemporary data collection and use. By identifying the new ways in which power is inscribed in large-scale digital data, we can better debate what we want and do not want from the information we emit about ourselves.").

64. *See e.g.*, Inge Graef & Bart van dar Sloot, *Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving Beyond Individual Empowerment*, 33 Eur. Bus. L. Rev. 513, 513 (2022) (noting in their abstract that "data protection and competition law can be applied more proactively to address [collective] harms" but that they might be insufficient on their own and thus require supplemental "regulatory interventions" that "target collective, and sometimes competitive, harm from technologies like pervasive advertising, facial recognition, deepfakes, and spyproducts.").