



Task Force 2:
**Our Common Digital Future: Affordable, Accessible
and Inclusive Digital Public Infrastructure**



INDIA 2023



भारत 2023 INDIA

A GOVERNANCE FRAMEWORK FOR DIGITAL PUBLIC INFRASTRUCTURE: LEARNING FROM THE INDIAN EXPERIENCE

July 2023

Aaditeshwar Seth, Professor, Indian Institute of Technology Delhi, and Co-founder, Gram Vaani, India

Luís Fernando Vitagliano, Professor, State University of Campinas, Brazil

Nachiket Udupa, Member, Mazdoor Kisan Shakti Sangathan, India

Parminder Jeet Singh, Executive Director, IT for Change, India

Rakshita Swamy, Co-founder, Social Accountability Forum for Action and Research, India

Subrata Singh, Programme Director, Foundation for Ecological Security, India


Vineetha Venugopal, Researcher, Digital Empowerment Foundation, India

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE



Abstract




Digital public infrastructures (DPIs) are said to follow or enable principles such as ‘open-source’, ‘open APIs’, ‘interoperability’, ‘privacy by design’, ‘inclusive design’, and ‘universal access,’ implying that crucial ethical values are baked into the technology itself. However, prior experience with DPIs in India has revealed shortcomings with this simplistic view. Many of these stated principles may not be enacted in practice, and even if they are, they are not sufficient to avoid possible harm or unfair outcomes from DPIs. Additionally, a key principle is often missed—of DPIs to be accountable towards the public, not just in their impact but also their conceptualisation and design. This brief argues that a strong participatory governance framework aligned with democratic principles should be created to bridge these gaps. Institutionalised and statutory mechanisms must exist for the ‘public’ to have a central role


in deciding the purpose of DPIs and validating assumptions on impact pathways behind how envisioned DPIs can meet these ends. It also is imperative that DPIs should not compromise any rights. Accountability mechanisms to safeguard against such violations and to resolve them should be easily accessible by anybody and governed by a legal framework. It should also be required for legislation to be passed for such issues to be highlighted by a representative body and be transparently disclosed and mandatorily addressed. Without strong structures of accountability built into DPI operations, DPIs may harm especially marginalised groups and weaken the citizen-State interface—and thereby grassroots democracy—by distancing the State from the people. As more and more G20 countries move towards DPIs, India’s experience highlights the need for such governance structures.



The Challenge



1




India is a frontrunner in developing and scaling digital public infrastructures (DPIs). Its digital identity system, Aadhaar, a part of the India Stack,^{a,1} provides a population-scale biometric-based authentication service that is the foundation for people to access government welfare schemes. A linked gateway infrastructure provides the ability to map a person's Aadhaar ID with a bank account, enabling government departments to operate direct benefit transfer (DBT) schemes to initiate cash transfers directly to a people's bank accounts. Another DPI, the Unified Payments Interface (UPI), also part of the India Stack, enables inter-bank transactions through an instant process without having customers enter recipient account details each time. Similar architectures centered on digital identities and 'open' interfaces have been proposed, and are being

implemented, in other domains such as health,² agriculture,³ and e-commerce.⁴ Citing the merits of interoperability, open-source, universal access, easier digitalisation, and privacy by design principles through secure data storage and consent mechanisms, such DPIs are claimed to enable rapid socio-economic development by making it easier for government departments and entrepreneurs to innovate and scale new digital applications and services.⁵

However, the process of institutionalising and implementing such DPIs has witnessed many gaps that have violated the fundamental rights of citizens, especially those from marginalised and vulnerable contexts.^{6,7} This includes cases of unfair exclusion from welfare benefits, exploitation through fraudulent transactions, ambiguity in placing accountability, and unreliability in grievance redressal, among others.^{b,8} Concerns have also been raised about

-
- a India Stack is composed of Aadhaar, a nationwide digital-ID infrastructure as a base layer, on which components such as an authentication service, a payment service, an electronic know your customer (e-KYC) service, and a financial transactions standard called Unified Payments Interface (UPI), are layered. India Stack was conceptualised by iSpirit, a network of volunteers largely comprised of veterans from the Indian IT industry, with close ties to the government.
- b A survey of Aadhaar-linked exclusions in welfare services indicated a plausible exclusion of over 10 million people from the public distribution system (PDS), which uses Aadhaar-based authentication, and a similar number for welfare schemes on rural employment and pension that use Aadhaar-linked enrolment and cash transfers.



corporate-government interlocks that influenced the purpose identification, conceptualisation, and development of many DPIs. This policy brief draws attention to DPI governance mechanisms that are crucial to prevent such issues. It proposes a governance framework that should regulate DPIs at three stages—the conceptualisation and purpose identification of DPIs, their design process, and subsequent ethical management of deployed DPIs. Such a governance framework is not only important for India, but also underscores the need for other G20 countries to study the Indian experience and recognize the need to have a just governance framework for DPIs.

Case study of DPIs in India


Through a case-study of Aadhaar-based authentication, DBT schemes, and UPI in the context of rural communities in India, this brief outlines various problems that have surfaced in DPI implementation.

Appropriateness of technology design

Aadhaar provides a biometric (fingerprint)-based authentication framework used in two settings: for the disbursement of subsidised food grains from the network of fair-price shops that operate through the Public Distribution System,^c and for cash withdrawal from people's bank accounts via point-of-sale (PoS) machines operated by banking correspondents to provide cash-in-cash-out services in remote locations.^d People's biometric fingerprints are recorded in a secure centralised database while registering for Aadhaar, following which users can authenticate themselves using their fingerprint at PoS machines for cash withdrawal or claiming their food entitlements. While the biometric-based authentication system was believed to be appropriate for use by less-literate and low-income people, without the need for them to remember passwords or use

c India runs a subsidised food programme called the Public Distribution System mandated as part of the National Food Security Act (NFSA) to ensure food security for its citizens. In 2017, Aadhaar based biometric authentication was made mandatory for people to claim their food entitlements: PDS shop owners were given Point of Sale (PoS) machines through which to authenticate beneficiaries.

d Given the sparse infrastructure of bank branches in rural areas, a banking correspondent model is provided by specialised firms through human agents who provide cash-in-cash-out services to rural customers. The agents use the Aadhaar Enabled Payment System through biometric authentication on PoS machines to provide this service.



phone-based one-time passwords, in practice, failures can arise due to poor network connectivity in rural areas or smudged fingerprints of many people such as elderly citizens, labourers, and farmers.^{9,10} This can impede the ability to claim food entitlements, which is a rights violation, and has reportedly even led to starvation deaths. Similarly, the opaque manner in which this system can be used by the PoS machine operators has led to fraud by them.¹¹ People have also been fraudulently enrolled in insurance schemes by banking correspondents.¹²


In the case of DBT, issues have typically arisen because of data entry errors by government officials.¹³ This results in failed transactions or even cash transfers to incorrect accounts. Diagnosis of the source of error is hard for citizens because the DBT pipeline spans Aadhaar, the concerned government department, banks, and the Aadhaar-bank account mapping gateway, and there are no standardised methods to obtain clarity about where in this pipeline the failure may have occurred. Citizens invariably fall back upon social workers or rent-seeking intermediaries who can help them

navigate such a complex technology landscape.

Such examples show that DPI infrastructures may not always be inclusive or designed in a citizen-centered manner, work reliably, or be appropriate to the context of use, and highlight the need to carefully pilot-test them before scaling, make alternatives available, and ensure accountability to promptly acknowledge and rectify any errors.

Purpose identification

The need for Aadhaar was justified to prevent identity fraud in welfare schemes and deduplication through biometrics was assumed to help ensure uniqueness of identity for each person. Both these claims have been challenged. In the case of distribution of subsidised food, for example, identity fraud is not the primary or even significant cause of leakages; rather, quantity fraud wherein fair price shop owners may not give the entitled quota of food grains to beneficiaries, is the main cause and Aadhaar cannot address that problem.^{14,15} Even whether the use of fingerprint-based biometrics can achieve deduplication is unclear.



No studies have been published, and in fact, a theoretical analysis indicates a high chance of deduplication failure.^{e,16,17}


Similar concerns of the validity of the claimed purpose prevail with e-KYC^f and with the development of the UPI infrastructure. Both services were justified to improve process efficiencies and have been rapidly scaled through State support. However, whether these efficiencies were indeed required, the attention placed on building guardrails to prevent misuse, and the preparedness of the population to handle the services, raises doubts on the intention behind these initiatives. Studies on India's rural employment guarantee scheme (MGNREGA) show that most registered households already had bank accounts;¹⁸ yet e-KYC was used to bridge a purported gap in financial inclusion by opening millions of bank accounts under the Jan Dhan Yojana in 2014, often even without people knowing that bank accounts had been opened in their names. Many of these bank accounts lay unused,

and only resurrected to some extent during the COVID-19 lockdown when the government made relief cash transfers to these accounts.¹⁹ The need and readiness of the people for digital financial services built on e-KYC and UPI is also debatable. For example, almost 50 percent of retail financial fraud arises from UPI.²⁰ The ease of offering financial services such as loans has also led to predatory lending to vulnerable people.²¹ Several studies show that the push in India towards the digitalization of financial services is neither universally supported due to issue of privacy, security, trust, and access, nor are questions on sustaining the basic costs of digital operations fully answered.²²

The lack of robust grievance resolution mechanisms in this space of financial services, inadequate safety guardrails to protect people from fraud, and the low readiness of people before they are financially literate enough to not fall for fraud, yet the hurry in ushering rapid digital financial inclusion of low-income populations without clear pathways

e An audit of the Aadhaar authority institution in 2021 also highlighted gaps in the de-duplication process.

f An electronic 'know your customer' (e-KYC) service enabled through Aadhaar allows agencies to query the address or other demographics of a person.



of how it will impact them, raises concerns about whose interest were such DPIs meant to serve. Similarly, with Aadhaar, the doubtfulness about its stated purpose illustrates the need for extensive prior debate before any DPIs are built and deployed.

Perpetuation of power-based inequalities

The various DPIs examined in this brief have made less digitally literate citizens, such as the poor and elderly, dependent on new kinds of intermediaries to help secure their entitlements, aggravated their vulnerability to fraud, made it hard to place accountability to seek redressal, and increased the distance between citizens and the State to hold the State accountable. Citizens have thus lost power to other stakeholders and bureaucrats, which has resulted in the perpetuation of power-based inequalities. Feedback loops to counter this concentration of power through grievance redressal are essential, but field experience indicates that the complexity of diagnosis of faults and the lack of adequate accountability mechanisms to ensure prompt and correct redressal is not able to reverse this, and results in a violation of citizen rights.²³ Technology tends to amplify

inequalities in the absence of effective guardrails or misguided purposes, and we see the same dynamics having played out in India with DPIs imposed without due multi-stakeholder consultation.


On the other hand, technologies that are designed and deployed in consultation with direct and indirect stakeholders, with the goal of using technologies to empower the weak, invariably tend to be more appropriate to the context, help build the capability of local stakeholders to manage the technologies towards responsible outcomes, and lead to greater power-based equality.²⁴ Systems built with this mindset, such as to prevent quantity fraud in food distribution by informing communities of stock availability,²⁵ or enable communities to escalate complaints against fraudulent fair price shop owners,²⁶ have been shown to empower communities and are alternative examples of technologies that should be scaled as DPIs. These examples highlight the need for underlying principles of democracy to conceptualise the purpose and design of digital public goods, and accountability in managing them, and forms the basis for the recommendations presented in this brief.



The G20's Role

2





DPIs characterised by a uniform architecture and implemented nationwide can provide a foundational building block that can enable new services to be built in a plug-and-play manner. Gaps can arise in this process, however, and violate citizen rights when the DPI technology may not be appropriate to the context, or processes for its use may not be clearly defined and followed, and which in turn can lead to the amplification of power-based inequalities. This highlights the need for stronger governance structures. As more and more G20 countries, including India, move towards DPIs, it is imperative that the principles of democracy and accountability form the foundations of these governance structures:


- Ensure that DPIs are conceptualised to solve valid problems that are framed by participatory citizen bodies.
- Do not scale DPIs without prior evaluations through pilot studies.
- Put responsive management structures into place to react to emergent issues with use and scaling of DPIs.
- Build a multi-level governance body to ensure that DPIs adhere to these above principles.
- Ensure transparency and public scrutiny at all steps.



Recommendations to the G20

3





Based on the underlying principles of democracy and accountability, this brief outlines a governance framework for DPIs at three stages: purpose identification for the conceptualisation of DPIs, appropriate design of the DPIs, and ongoing management of deployed DPIs. Finally, it outlines the need for a nodal regulatory body to implement these processes and ensure that democratic and accountable practices are followed at all the three stages.

Democratic purpose identification

The problem that any DPI is meant to solve should emerge through democratic consensus from the citizens. This implies that needs and observations articulated through institutionalised participatory mechanisms such as the *gram sabhas*^g should be collated, analysed through research studies, and discussed in multistakeholder consultations to arrive

at DPI proposals. This will help ensure that valid felt needs by citizens are given priority in defining the purpose of a DPI, rather than misguided or profit-driven agendas.


The need for bottom-up participatory methods to collect citizen inputs also highlights the need for meta-DPIs^h (DPIs that are essential for fair functioning of other DPIs) to gather and curate insights from the gram sabhas and other citizen forums. Federated public spheres such as the Indymedia network successfully demonstrated protocols to run global-scale deliberation on international economic policies,²⁷ and similar methods could be adopted through authorised networked community forums.

Participatory and evaluative approach for appropriate design

Once the purpose has been precisely identified, the DPI design should also be conceptualised

g Gram sabhas are village-level citizen meetings meant to serve as a participatory forum to discuss local issues and identify solutions that can be actioned by local governance bodies.

h The term meta-DPIs is used in the same context as the term ‘meta-social good technology projects’ introduced in A. Seth’s *Technology and (Dis)Empowerment*, as wider infrastructures needed to uphold governance standards in other infrastructures, for example, the role that media plays in a democracy, or that regulatory institutions play in markets.



through participatory methods with communities so that essential features to ensure accessibility, fault diagnosis, process integration, grievance redressal, transparency, and accountability are all built from the outset. Similar to the concept of privacy by design, principles of accountability by design and power-based equality by design should guide this technology and process design.

The DPI should then be piloted extensively in diverse settings, with a monitoring, learning, and evaluation study commissioned for each pilot. These study reports should be made publicly available and consultation processes should be followed to refine the design based on these pilots. Such efforts to pilot, validate, and then scale will help prevent making grossly incorrect assumptions to do with network coverage, technology literacy of citizens, and affordances that can lead to fraud, among others.

Federated management

No matter how appropriate and comprehensive the design, emergent issues of inconsistent adherence to prescribed processes, gaps in performance monitoring, and cases

of misuse may still arise at the socio-technical interface when DPIs are deployed.²⁸ A federated approach to deployment management can ensure that the capacity of local stakeholders is built to responsibly manage the DPIs and handle these issues, while ensuring that principles of accountability and power-based equality are not compromised any time. Local governance institutions starting with village-level governance bodies should be nodal agencies for this purpose, to flag emergent issues that need to be addressed. Citizen-interest groups such as trade unions and other forms of collectives representing the interests of many groups of citizens can also serve as additional nodal agencies.

Regulatory body

Governance at different stages of the DPI conceptualisation, design, and ongoing management will require a regulatory body to coordinate processes at multiple levels (local, state, and centre). Precedent already exists in India with the Right to Information (RTI) and Anti-Corruption (Lokayukta) Acts that set up ombudsmen and nodal officers in a multilevel framework to guide the implementation of the Acts both horizontally at the local level and vertically for wider

coordination.ⁱ In a similar way, a DPI regulatory body should be established with representatives drawn from amongst government officials, domain experts, civil society organisations, and citizen representatives, who can oversee DPI operations at the state and center levels.^{j,29}

This body can serve to examine all proposals for new DPIs, their design and evaluation reports, and establish the proposed federated management structure for new and existing DPIs. It will release regular reports about its activities and findings, hold public consultations, and produce literature for further global guidance of DPI production and use.

The body must have executive rights so that its recommendations are enforced.


Since the implementation and use of DPIs will span across multiple government departments, it should be answerable either to a permanent standing committee of the parliament or exist as an independent statutory commission appointed by the President as in the case of RTI.

Commons-based approach

We want to add that underlying our proposed approach, and as evidence of its fitment, community-based governance structures of the commons provide an important learning ground. Societal-scale use of DPIs that touch crucial livelihood aspects of citizens' lives positions DPIs as a commons resource that should be governed by the citizens. Local governance structures such as community forest rights,³⁰ water governance,³¹ and, more recently, calls to govern the Internet and societal-scale web-based platforms

i The Right to Information (RTI) Act in India is implemented in a multilevel fashion, at the states and the center. State Information Commissions manage the appointment of RTI officers in all state government departments and monitor prompt action on RTI queries. A Central Information Commission similarly integrates into all central government departments. The Central Information Commission (CIC) and all the state commissions are independent bodies, with the CIC operating directly under the President of India. The Lokayukta Acts in various states similarly enable a post of an ombudsman at the state level to whom citizens can report incidences of corruption against any government official or political representative.

j A UK think tank, Doteveryone, has proposed a similar framework for responsible technology, by setting up an independent regulatory body composed of civil society representations and other stakeholders, which examines incidences of technology misuse and failure, and makes recommendations to technology companies and governments to build appropriate safeguards.




as a commons³² have developed similar principles centered on accountability, observability, autonomy, decentralization, and subsidiarity. Technologies that are governed by such structures, and which support these

structures, empower citizens, rather than a top-down approach which uses technology as a means of social control for safety and security. DPs similarly need a citizen-empowering approach.

Attribution: Aaditeshwar Seth et al., "A Governance Framework for Digital Public Infrastructure: Learning from the Indian Experience," *T20 Policy Brief*, July 2023.

Endnotes

- 1 Regina Mihindukulasuriya, “ ‘All about helping Rajni’ - tech gurus at iSPIRT quietly power India’s digital revolution,” *The Print*, June 25, 2022, <https://theprint.in/india/all-about-helping-rajni-tech-gurus-at-ispirt-quietly-power-indias-digital-revolution/1007652/>.
- 2 Ministry of Health and Family Welfare, Government of India, “National Digital Health Blueprint,” April 2019, https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf.
- 3 Department of Agriculture, Cooperation and Farmer Welfare, Government of India, “Consultation Paper on IDEA: India Digital Ecosystem of Agriculture,” June 2021, https://agricoop.nic.in/sites/default/files/IDEA%20Concept%20Paper_mod01062021_1.pdf.
- 4 Internet Freedom Foundation, “Open Network for Digital Commerce (ONDC): An Explainer,” (2023), <https://internetfreedom.in/ondc-an-explainer/>.
- 5 Cristian Alonso et al., “Stacking up the Benefits: Lessons from India’s Digital Journey,” *IMF Working Paper* 2023/078 (2023), <https://www.imf.org/en/Publications/WP/Issues/2023/03/31/Stacking-up-the-Benefits-Lessons-from-Indias-Digital-Journey-531692>.
- 6 Aaditeshwar Seth, *Technology and (Dis)Empowerment: A Call to Technologists* (Leeds: Emerald Publishing, 2022), <https://www.cse.iitd.ernet.in/~aseth/act.html>.
- 7 Reetika Khera (Ed.), *Dissent on Aadhaar: Big Data Meets Big Brother* (Hyderabad: Orient Blackswan, 2019), <https://orientblackswan.com/details?id=9789352875429>.
- 8 “Home,” State of Aadhaar, <https://stateofaadhaar.in/>.
- 9 Hartej Singh Hundal, Janani A P, and Bidisha Chaudhuri, “A Conundrum of Efficiency and Inclusion: Aadhaar and Fair Price Shops,” *EPW*, April 3, 2020, <https://www.epw.in/engage/article/conundrum-efficiency-and-inclusion-aadhaar-and>.
- 10 Mukesh Ranjan, “Social economist Jean Dreze blames Aadhaar based authentication in PDS for seven starvation deaths in Jharkhand,” *Indian Express*, June 22, 2018, <https://www.newindianexpress.com/nation/2018/jun/22/social-economist-jean-dreze-blames-aadhaar-based-authentication-in-pds-for-seven-starvation-deaths-i-1831924.html>.
- 11 Aarushi Gupta et al., “Delivery of Social Protection Entitlements in India: Unpacking Exclusion, Grievance Redress, and the Relevance of Citizen-Assistance Mechanisms,” *APU COVID-19 Research Funding Programme* (March 2021), <https://www.cse.iitd.ernet.in/~aseth/Delivery-of-Social-Protection-Entitlements-in-India.pdf>.
- 12 Hemant Gairola, “How An Aadhaar Fraud Forces The Poor Into Paying For Welfare Schemes They Do Not Want,” *Article 14* (Feb 2023), <https://article-14.com/post/how-an-aadhaar-fraud-forces-the-poor-into-paying-for-welfare-schemes-they-do-not-want-63f57eb9e8d15>.

- 
- 13 Gairola, “How An Aadhaar Fraud Forces The Poor Into Paying For Welfare Schemes They Do Not Want”; Aarushi Gupta et al., “Delivery of Social Protection Entitlements in India”
 - 14 Jean Drèze and Reetika Khera, “Understanding Leakages in the Public Distribution System,” *EPW*, February 14, 2015, <https://www.epw.in/journal/2015/7/insight/understanding-leakages-public-distribution-system.html>.
 - 15 Reetika Khera, “Impact of Aadhaar in Welfare Programmes,” *EPW*, December 16, 2017, <https://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html>.
 - 16 Hans Varghese Mathews, “Flaws in the UIDAI Process,” *EPW*, February 27, 2016, <https://www.epw.in/journal/2016/9/special-articles/flaws-uidai-process.html>.
 - 17 Ministry of Electronics and Information Technology, Government of India, “CAG’s Audit Report No. 24 of 2021”, https://cag.gov.in/uploads/download_audit_report/2021/exe-sum-0624d8136c68021.65880617.pdf
 - 18 Deepanwita Gita Niyogi, “Is Jharkhand’s Ambitious Aadhaar Linkage Derailing MGNREGA?,” *Down to Earth*, August 31, 2017, <https://www.downtoearth.org.in/news/governance/welfare-interrupted-58472>.
 - 19 Aaran Patel, Pragyna Divakar, and Rajatha Prabhakar, “40% Of Jan Dhan Account Holders Could Not Access Govt’s COVID-19 Relief: Survey,” *IndiaSpend*, June 29, 2020, <https://www.indiaspend.com/40-of-jan-dhan-account-holders-could-not-access-govts-covid-19-relief-survey/>.
 - 20 Arundhati Ramanathan, “The UPI frauds undermining India’s payments fairytale,” *The Ken*, January 4, 2022, <https://the-ken.com/story/the-upi-frauds-undermining-indias-payments-fairytale/>.
 - 21 Devesh K. Pandey, “ED Attaches 86.65 Crore in Micro-loans Fraud Case,” *The Hindu*, July 6, 2022, <https://www.thehindu.com/news/national/ed-attaches-8665-crore-in-micro-loans-fraud-case/article65608038.ece>.
 - 22 Masudul Hasan Adil and Neeraj R. Hatekar, “Demonetization, Banking and Trust in “Bricks” or “Clicks”,” *South Asia Research*, 40(2), April 2020, <https://journals.sagepub.com/doi/10.1177/0262728020915566>.
 - 23 Adil and Hatekar, “Demonetization, Banking and Trust in “Bricks” or “Clicks””; Seth, *Technology and (Dis)Empowerment*
 - 24 Aaditeshwar Seth, “Bringing back the ‘Public’ in Digital Public Goods,” *The India Forum*, November 29, 2022, <https://www.theindiaforum.in/forum/bringing-back-public-digital-public-goods>.
 - 25 Sriniketh Nagavarapu and Sheetal Sekhri, “Plugging PDS Pilferage: A Study of an SMS-based Monitoring Project,” *EPW*, March 29, 2014, <https://pubmed.ncbi.nlm.nih.gov/25810558/>.
 - 26 Dipanjan Chakraborty et al., “Findings from a Civil Society Mediated and Technology Assisted Grievance Redressal Model in Rural India,” *ICTD*, November 2017, <https://dl.acm.org/doi/10.1145/3136560.3136574>.

- 
- 27 Dorothy Kidd, "The Global Independent Media Center Network," In *Be the Media*, ed. David Mathison (San Francisco: Natural E Creative, 2009), pp. 413-422, <https://repository.usfca.edu/cgi/viewcontent.cgi?article=1006&context=ms>.
 - 28 Aaditeshwar Seth, "The Limits of Design in Ensuring Responsible Outcomes from Technology," *ICTD*, June 2020, <https://dl.acm.org/doi/10.1145/3392561.3394631>.
 - 29 Doteveryone, "Regulating for Responsible Technology," 2018, <https://doteveryone.org.uk/wp-content/uploads/2018/10/Doteveryone-Regulating-for-Responsible-Tech-Report.pdf>.
 - 30 Foundation for Ecological Security, *Commoning the Commons*, https://fes.org.in/resources/sourcebooks,manuals,atlases-&-ecoprofiles/manuals/strengthening_governance_and_management_of_water_as_commons.pdf.
 - 31 Elinor Ostrom, *Governing the Commons* (Cambridge: Cambridge University Press, 1990), <https://www.cambridge.org/core/books/governing-the-commons/7AB7AE11BADA84409C34815CC288CD79>.
 - 32 Amy A. Hasinoff and Nathan Schneider, "From Scalability to Subsidiarity in Addressing Online Harm," *Social Media + Society*, September 2022, <https://journals.sagepub.com/doi/10.1177/20563051221126041>.



वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE