

Technologies of Disempowerment

Aaditeshwar Seth
IIT Delhi and Gram Vaani
aseth@gramvaani.org

This note describes how several technological systems for welfare delivery and social security have ended up disempowering many people, while aiming to solve problems for them. It highlights several recurring mistakes in the design of these systems. Much evidence in support of our arguments is based on voice-reports from Mobile Vaani [18], a voice-based participatory media platform that is operated by the social enterprise [Gram Vaani](#). These voice-reports are hyperlinked in the document below.

Badly designed technologies

Biometric fingerprint failure is the single biggest source of errors in the Aadhaar based authentication process for both PDS [1] as well as [cash withdrawals](#). The reasons have been well documented, from machine failures to [illegible fingerprints](#) and also changes with age of the people. Proposals are now being discussed to replace fingerprints with iris scans, yielding even more expenses for the state and in turn higher revenues for companies in this business. What is the reason though to have biometrics at all? We need to go back to the history of the Aadhaar project where biometrics were deemed essential so that nobody could have more than one Aadhaar card. Do we know how many studies have been published about the efficacy of fingerprint biometrics for de-duplication? The answer is zero studies by UIDAI, and just [one study by CIS](#) which claims a high false rejection rate if biometric de-duplication is indeed implemented [2]. If biometrics are not helping with de-duplication then there is no need for them, or for OTPs either, simple smartcard-based solutions are just fine in case digitized transaction logs are required. Errors arising from biometric failures have led to [starvation deaths](#) and large-scale unfair denial of benefits to much needy people, a completely avoidable and unnecessary problem.

One process that is correct though is that the onus for re-registering of biometrics lies with the beneficiary who is the only stakeholder in the mix with a genuine incentive to fix their problem. Re-registration is however not straightforward and we discuss that later. There are however alarming examples of systems where the onus to correct data entry errors lies with stakeholders who do not benefit at all from doing so. Why would they fix these problems then? The provident fund IT system is one such example. Correcting errors in the [spelling of names](#), even marking the gender, date of birth, date of joining, Aadhaar details, mobile phone number, etc, all rest with the employers, including ex-employers. Countless workers are unable to withdraw funds from their PF accounts because of such mismatches. Former employers are hardly responsive because they clearly have no reason to respond. It also does not help that many workers do not even know that their [PF is being deducted](#), or [what is their PF account](#), or the [procedures to withdraw funds](#). How hard is it to conceive of a setup where the workers are well informed of these deductions through SMS messages, the PF account number is mentioned on their payslips, and a user-facing system is provided so that workers can fix the errors, or take help to fix them, rather than rely on employers who have no incentive to pay attention?

Technologies with misplaced objectives

The MNREGA Management Information System (MIS) is highly impressive, housing details of each job card and works done, attendance, payment status, etc, all in almost real-time. Who is it meant for though? The people doing MNREGA work are clearly not savvy with using online systems to check their accounts. They rely on help from others [3]. The MIS is thereby serving a purely accounting function, to keep track of various works and payments, and is therefore a system for the administration rather than the worker [4]. This is not entirely useless, it is much needed, and according to our reports the [wage payments](#) are quite [timely now](#), but it does not fulfil the transparency claim that the MIS was originally envisaged to fulfil. The workers remain disenfranchised without any SMS or IVR or app based interfaces to access their own work history or payments, even though such systems are straightforward to implement [5, 6]. Is it not a rightful enhancement that should be made for the workers so that they can check if the work being done by them is being correctly logged and they are getting their due wages accordingly?

Aadhaar itself is another example of misplaced objectives. It was clearly conceived as a system to reduce inclusion errors in welfare schemes, ie. deny welfare benefits to those who don't deserve them, and marketed likewise as a [means to plug leakages](#). Such leakages of unauthorized access to welfare benefits are however a minuscule fraction of leakages by the ration dealers on [quantity fraud](#) where they do not give the [due quantity of provisions](#) to the people and sell the rest in black. Aadhaar can do nothing to plug these leakages. Nor can it do anything to reduce exclusions errors for the benefits to reach those who need them. On the contrary, the fragility of the Aadhaar technology has led to [unfair denial of benefits for many people](#). With morphing from an optional identity system to a mandatory authentication system, and even an identification system as has been [suggested by many](#), the scope creep of Aadhaar has indeed been quite insidious.

Technologies that creates power inequalities

Who understands and wields a technology is a key driver to determine whom the technology empowers and whom it disempowers. Banking correspondents walk around with Aadhaar enabled biometric authentication machines so that banking services can be delivered to people at their doorstep, a much needed service. However it is also easy for the banking correspondents to [underreport to customers](#) the amount of cash that has been withdrawn from their accounts, by making false verbal claims that an [inactive-account fees was applied](#), for example. Customer service points of banks have reportedly gone further, by telling customers that their [bank account has been deactivated](#) while all the time the accounts were functional and being used for black money transactions. Better designed technology of the POS machines could have improved at least some degree of consumer awareness. Audio enabled POS machines which speak out each and every transaction, explain the error codes in simple terms, and suggest appropriate actions in the case of failure, can go a long way in levelling the power imbalance between the banking agents and consumers.

The same principle is applicable even with ration shops, where the dealer clearly has more power in explaining any authentication issues to the beneficiaries. The dealer can project failures in different ways, including by falsely [claiming a shortfall in stock](#) and not giving full units of food to the people. The beneficiaries have no way to check and have to go with [whatever the dealer says](#). By placing technology in the hands of the dealer – technology that

the beneficiaries do not understand – the inherent power differential between them gets sharper and can manifest itself in other dealings between them. Technology should rather be designed to create power equality among stakeholders [7, 8]. If the ration dealer wants to claim a shortfall then the technology should mandate that they record an oral testimony right there at the point of service to confirm the shortfall and also raise a complaint upstream in the PDS system which can be audited by the food supply department.

The argument extends to technology induced power inequalities that have arisen between consumers and administrative officials too. Aadhaar based authentication for PDS and cash withdrawal may fail for any of [over 150 reasons](#), but only an incomprehensible error code is [thrown up on the POS machines](#). Biometric failure is the largest reason, and can only be fixed by having the consumer make trips to the bank or Aadhaar enrolment centres. This is not straightforward or even easily affordable by everybody, and even worse it sharpens the power differential between the beneficiary and officials. An alternate design would be to examine the logs to identify consumers who have had frequent biometric errors, and commission a door-to-door re-registration exercise for the people. Until then, beneficiaries should be allowed access through social trust mechanisms, where somebody else in the community can vouch for them against their Aadhaar.

Further, entirely different technologies can be envisioned that would rather empower the weak and plug PDS quantity fraud. Technologies that inform people through SMS or IVR or other means about stock deliveries that have happened at their ration shops [9], about the correct number of units due to them, about grievance redressal mechanisms to raise complaints, and resolve them, can go a long way in this direction of empowering the weak. Even non-technological solutions of having the ration shops operated by the panchayats, with [support from SHG networks](#), have gone a long way.

Technologies that alienate

How many Muslims or returned migrant workers will eagerly embrace Aarogya Setu? One argument, albeit misplaced to quite an extent yet advanced by many vigilantes and even technocrats, is that such people are at higher risk of contracting the corona virus, and therefore for their own safety they will use it. Another argument however is that since there has been such [widespread discrimination](#) against them they will not use the app for [fear that if they do](#) come out as at-risk or infected then they could be carried away to [badly run isolation centres](#) or the entire household could be confined from movement and their families too would face discrimination in the community. They will figure out mechanisms to evade proper use of the technology so that they do not come out as at-risk. Which argument ends up being correct will only reveal itself in due course. The point however is to realize that technology does not operate in a vacuum, it is used by people situated in particular contexts and the use is shaped by perceptions of trust among people with one another and with the technology. If this environment has trust cleavages and the technology has the potential to enhance these cleavages then it may [alienate people from the technology](#) and also from one another. Even worse, it could be used as a tool by malicious actors to deepen the cleavages and mistrust. Appropriate communication and alternate designs that remove chances of misuse, can foster greater trust and ultimately better usefulness. The arguments about ambiguous data privacy policies and laws, and the usefulness and accuracy of Bluetooth-based tracing mechanisms, as highlighted by many [10], further outlines additional pathways

through which trust is disrupted when there are chances for misuse of data or for technology failures to go uncorrected and cause undue inconvenience.

What drives technology adoption?

These reasons of poorly thought through technology design, contrived problem statements, and inappropriate management of the socio-technological interface with mishandling of failure cases and wider public communication [8, 11], are seen recurring again and again. The latest wave unleashed is of AI-inspired technologies in areas such as assessing of credit-worthiness of low-income people using mobile call-data-records, risk-scoring for criminal recidivism, performance assessment of human resources across a large range of industry sectors, etc [12]. These are all enthusiastically embraced by many governments, but all such applications are fraught with the same risks and may end up disempowering the weak.

This clearly raises the question that with such grave issues in vast technological systems, how come disempowering technologies are being widely adopted by the state? Why are these technologies not fixed to minimize harm? Several theories can explain this, one being that governments have a strong belief in high-modernism, of technology having the potential to control and make legible its citizens which can aid in national security, targeting of benefits, tax collection, etc [13]. Another theory is around capitalism's need for constant technological innovation [14], which seeks out new markets, including marketing technologies to the state, with strong influence exercised by capital in the uptake of these technologies [15]. In India, the government's desire for technology that facilitates centralization has been cleverly serviced by capital's ingenuity to provide such technology [16], but both have failed to conceive of technologies that can be not-disempowering yet satisfy the state's misguided obsession with centralized control. It has been as much of capital's failure to come up with alternatives, as the citizens' failure to not reject the flawed mindset of their elected governments in wholesale adoption of disempowering technologies. While the clock cannot be set back, the task ahead for us as citizens is clear – to understand the broader ramifications of technologies of disempowerment and to be critical in rejecting them, and in fact for technologists to not even design them in the first place [17].

References

- [1] Siddharth Sekhar Singh, et al. 2018. *Aadhaar Authentication Failure in the Public Distribution System of Andhra Pradesh*. Technical report, Indian School of Business.
- [2] Hans Verghese Mathews. 2016. *Flaws in the UIDAI Process*. In *Economic and Political Weekly*.
- [3] Dipanjan Chakraborty, et al. 2017. *Findings from a Civil Society Mediated and Technology Assisted Grievance Redressal Model in Rural India*. In *Information and Communication Technologies and Development*.
- [4] Rajesh Veeraraghavan. 2013. *Dealing with the Digital Panopticon: The Use and Subversion of ICT in an Indian Bureaucracy*. In *International Conference on Information and Communication Technologies and Development*.
- [5] Dipanjan Chakraborty, et al. 2015. *Building Citizen Engagement into the Implementation of Welfare Schemes in Rural India*. In *International Conference on Information and Communication Technologies and Development*.

- [6] Vivek Srinivasan, et al. 2013. *Airavat: An Automated System to Increase Transparency and Accountability in Social Welfare Schemes in India*. In Information and Communications Technologies and Development.
- [7] Duquenoy, P and Thimbley, H. 1999. *Justice and Design*. In Human-Computer Interaction INTERACT.
- [8] Aaditeshwar Seth. 2019. *A New Paradigm to Accommodate Ethical Foundations in the Design and Management of Digital Platforms*. Working Paper.
- [9] Jean Drèze. 2017. *Sense and Solidarity: Jholawala Economics for Everyone*. Permanent Black.
- [10] Subhashis Banerjee, et al. 2020. *Apps for COVID: to do or not to do*.
<http://www.cse.iitd.ac.in/~suban/reports/apps.pdf>
- [11] Aaditeshwar Seth. 2020. *The Limits of Design in Ensuring Responsible Outcomes from Technology*. In Information and Communication Technologies and Development.
- [12] Cathy O’Neil. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown USA.
- [13] James C Scott. 1998. *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.
- [14] Harvey, D. 2003. *The Fetish of Technology: Causes and Consequences*. Macalester International, 13(7).
- [15] Joseph E Stiglitz. 2012. *The price of inequality: How today’s divided society endangers our future*. WW Norton & Company.
- [16] Anirban Sen, et al. 2019. *An Attempt at Using Mass Media Data to Analyze the Political Economy Around Some Key ICTD Policies in India*. In Information and Communication Technologies and Development.
- [17] Aaditeshwar Seth. 2019. *A Call to Technologists*.
<http://www.cse.iitd.ernet.in/~aseth/call-to-technologists-2019.pdf>
- [18] Aparna Moitra, et al. 2016. *Design Lessons from Creating a Mobile-based Community Media Platform in Rural India*. In Information and Communication Technologies and Development.