Draft Charter on Democratic Accountability in the Digital Age

Synthesis from the Workshop on Democratic Accountability in the Digital Age 14-15 November 2016, New Delhi

IT for Change, *Mazdoor Kisan Shakti Sangathan*, Centre for Internet and Society, Digital Empowerment Foundation and National Campaign on People's Right to Information organized a national level workshop between 14 and 15 November 2016, in New Delhi. The primary objective of the workshop was to lay the groundwork for building a charter of principles for democratic accountability in the digital age. This note attempts to bring together and consolidate the principles that emerged out of workshop discussions.

The draft charter begins with a preamble, followed by the principles clustered into specific categories. The principles are elaborated as per the group discussions and plenary presentations, and include remarks made/feedback given by co-participants during the plenary.

Footnotes providing supporting/ supplementary information to the principles wherever required are added. For each principle, a reference in brackets has been added to attribute to the group/s who articulated it. The details of the groups are provided in Annex 1.

We have added points that did not come up in the discussions for the sake of completeness, with the annotation "**added, IT for Change**" in parentheses and welcome your reflections on these.

While reviewing this draft, please consider flagging any additional principles or points, annotating such additions with your name.

We envisage the following steps at this stage:

- Version 1 of the Charter – with comments, notes of agreement, notes of disagreement, suggestions for refinement, alternative language, etc – will be co-created with your inputs and suggestions by December 25, 2016.

- Steps towards a Version 2 and actions to follow from that will be finalized jointly by the collaborating organizations, through a discussion in January 2017.

Draft Charter on Democratic Accountability in the Digital Age

December 2016

Preamble

India is witnessing the rise of a new governance paradigm, characterized by the digitalization of welfare systems and citizen engagement mechanisms. This moment of flux presents new opportunities for inclusive democracy, but also encompasses the real threat of new forms of citizen exclusion. The shrinking room for local accountability in automated service delivery, the replacement of democratic deliberation by data driven participation, and the hollowing out of the state due to the emergence of a networked governance culture in which private actors are taking over core public functions, suggest the need for a critical stocktaking.

There is much to be gained by appropriate digitalization of governance, but an emerging architecture of digital control poses the risk of disempowerment of the majority. A crisis of democratic accountability is evident. In order to protect and promote participatory democracy in the digital age, we need new legal frameworks, policy guidelines, institutional mechanisms and techno-design practices.

This charter puts forward first principles in this regard and may be considered as a work in progress. It was developed through the deliberations at the *Workshop on Democratic Accountability in the Digital Age,* organized by IT for Change, *Mazdoor Kisan Shakti Sangathan*, Centre for Internet and Society, Digital Empowerment Foundation and National Campaign on People's Right to Information, on 14th and 15th November 2016.

Section 1. Digitalized welfare systems

1.1 Digitalized welfare systems must leave no one behind

1.1.1 In the transition to digitalized welfare systems, citizens should not be denied their rightful claims and entitlements, just because they do not have Internet access[1]. Citizens who lack access to connectivity should not be excluded from public services (Group 1).

1.1.2 Digitalization cannot introduce a 'scope creep' into public service delivery through a 'for profit' logic (Group 1). Access to all basic e-services should be zero rated, meaning that these services should be free of data charges when accessed online (added, IT for Change). Citizens cannot be charged for basic e-services by government one stop shops / Common Service Centres (Group 1).

---

[1] The idea that citizenship claims cannot be predicated upon Internet access is important for the inclusion of all citizens in public service delivery. Principle 17 of the Delhi Declaration of the Just Net Coalition, for example, underlines that, *"People must be able to enjoy all their rights and entitlements as citizens, even if they choose not to have Internet access. Access to and use of the Internet should not become a requirement for access to public services".*

1.1.3 The onus of streamlining access to digital services and addressing glitches in roll out must be on the government (Group 1). Government agencies have the responsibility of ensuring that design choice in digitalized service delivery takes into account differences in levels of access and digital capabilities of users, to enable effective citizen uptake (Group 1).

1.2 Digitalized welfare systems must be accompanied by comprehensive legal-institutional frameworks for accountability

1.2.1 The transition to digitalized welfare systems must be backed by a people centred accountability legislation that covers local, state and union government agencies, as well as private parties contracted by government agencies for the discharge of public functions/ provisioning of public services[2] (Group 1, 4). This legislation should:

- Ensure citizen access to information about entitlements.
- Establish a comprehensive grievance redress mechanism, and protect citizens who file complaints/grievances pertaining to service delivery and implementation of welfare schemes.
- Make room for citizen participation at every stage in the design and implementation of digitalized services.
- Provide for social audit mechanisms of techno-governance processes.
- Guarantee timely action from state and private actors involved in service provisioning, both in terms of processing service requests and responding to complaints/grievances[3].

In cases where service requests are denied without due cause, such as authentication failures or technical glitches in digitalized systems, the concerned authorities must be penalized[4] (Group 1).

1.2.2 Any digitalized welfare service must be rolled out only after it is successfully piloted and a satisfactory, independent, third party evaluation is conducted to assess its viability, including cost-benefit analysis, and long term sustainability. The marginalized cannot become guinea pigs for digital experimentation. The same principle should also extend to any future expansion and/or alteration in service design (Group 1).

---

2 The Supreme Court of India, in its judgment in Dr. Janet Jeyapaul v SRM University ruled that writ jurisdiction of the High Court could be extended to private bodies performing public functions, thus opening up a legal gateway for enforcing citizen accountability of private actors in government systems.

3 These points are borrowed from the Bhilwara principles, a five point set of the essential ingredients of a citizen centric accountability legislation as articulated by a group of young people fighting dalit atrocities in their villages in Bhilwara district, Rajasthan. This includes "*jaankari, sunwai,suraksha, bhagidari, karyavahi." See http://www.hindustantimes.com/ht view/citizenship for all our citizens/story UlNTa8vPWm81wVF0srrw4O.html*

4 The *Aadhaar* Act (2016) completely flouts this principle. There is currently no provision in the Act (or any existing legislation on guarantee of services) that penalizes government agencies for unfair denial of services to citizens due to technological glitches. In fact, there is not even a provision pertaining to citizen redress against unfair denial of entitlements.

1.3 Access to digitalized welfare must be by choice and not by default

1.3.1 Access to digitalized welfare services should be a choice that citizens can exercise of their own volition. No one can be forced to switch from non-digitalized to digitalized service delivery mechanisms. Disincentives for offline state-citizen interactions cannot be used as a strategy to make citizens switch over to online/digital modalities (Group 1, 3).

1.3.2 In the transition to digitalization, investment in offline modalities of service delivery must not be abandoned. On the contrary, such investment must be continue till such time that access to, and use of, digital technologies and digitalized services becomes universal (Group 1, 3).

1.3.3 The digital platform or mechanism underlying basic state-citizen transactions should allow citizens the choice to 'opt out'[5] (Group 1, 3). Citizens must have the right to opt out of digitalized welfare services, and continue with manual modes of service delivery[6] (Group 2). No blanket consent may be sought from citizens for including them into digitalized service delivery systems (Group 1).

Section 2. Citizen participation in digitalized governance

2.1 Digitalized governance systems must reinforce and expand citizen right to participation

2.1.1 The design and implementation of digitalized governance must be informed by public consultation.

2.1.2 Existing legal-institutional guarantees pertaining to the Right to Information Act (2005) and the right to democratic participation must be extended to online spaces as part of their very design[7] (Group 3). The technological architecture of online platforms and mechanisms of digitalized service delivery must be in conformity with the provisions of existing laws and policies on the rights to information and democratic participation (added, IT for Change).

---

5 This is currently violated, given that Clause 7 of the *Aadhaar* Act (2016) allows central and state governments the power to make *Aadhaar* identification mandatory for any subsidy/ service/ benefit funded by the Consolidated Fund of India.

6 The importance of the choice to opt out of digitalized governance systems has been acknowledged in New Zealand. The Electronics Transactions Act (2002) adopts the logic of 'opt in', by offering citizens free choice to continue to carry out transactions offline, without incurring any additional disadvantage. See http://www.legislation.govt.nz/act/public/2002/0035/latest/whole.html

7 For instance, the Right to Information Act (2005) explicitly includes data material held in any electronic form in its definition of information. Supplementary rules on RTI, issued by the Department of Personnel and Training (office memo of April, 2013), have extended the application of proactive disclosure provisions to all digital records, multimedia resources and data sets held by public authorities. Similarly, the Prelegislative Consultation Policy framed in 2014, when providing for a clear set of procedures for citizen consultation in enacting legislation, specifically mentions the need for proactive disclosure of proposed legislations on Internet and mass media platforms.

2.1.3 There should be a citizen engagement protocol underpinning e-participation initiatives[8] (Group 3). This should facilitate individual and collective expression of citizen voice, and prescribe a mechanism to enable timely reporting back by government agencies to citizens on the outcomes of e-consultation processes. Collective and deliberative processes should not be sidelined in favour of individualised inputs (added, IT for Change).

2.1.4 Digital platforms for citizen interaction cannot become the privileged mode of mobilizing public opinion for decision making. Offline modalities of citizen engagement and public consultation must be emphasized equally (Group 3).

2.1.5 Universalizing meaningful access to the Internet is an integral component of citizen right to participation[9]. Investment in the creation of accessible public access spaces and information facilitation centres at the last mile[10] and provisioning of a universal data allowance (Group 1) are preconditions to enable citizen appropriation of the empowering possibilities of the Internet, along with the implementation of universal and contextual digital literacy programmes[11] (Group 1, 3).

Section 3. Techno-design for democracy

3.1 Design choices in the creation and maintenance of digitalized governance systems must guard against and proactively tackle exclusion, social bias and inequality

3.1.1 Any technological platform or mechanism introduced in governance should have built-in room for course correction and overhaul, to address citizen exclusion (Group 1). The design of digital systems and platforms must guard against the perpetuation and amplification of existing patterns of exclusion that prevent marginalized individuals and groups from participating in governance and democracy (Group 3). In fact, digital platforms must be used to make public information and service provision more accessible, effective and citizen-friendly (added, IT for Change).

3.1.2 Techno-design choices in the roll out of digitalized governance systems must be driven by the priorities of the concerned government agency, and not by technology vendors, lobbies of technology companies or other vested interests (Group 4). The development of technological platforms and mechanisms must conform to the provisions of the National Policy on Open Standards for e Governance (2008) in order to prevent

---

8 See for instance, https://euparticipation.files.wordpress.com/2015/05/e_participation_guideline_final.pdf

9 The National Telecom Policy (2012) acknowledges broadband connectivity to be a basic necessity like education and health and the importance of working towards reliable and affordable broadband access in rural and remote areas. In fact, it invokes the idea of 'the right to broadband'.

10 Such information and facilitation centres should be funded by the state as part of its investment in furthering proactive disclosure under the Right to Information Act (2005). However, in their everyday functioning, these centres must have management structures that are autonomous.

11 Digital literacy programmes should go beyond mere skills training and focus on enabling individuals use the digital opportunity to expand their citizenship capabilities. The evolution of a set of measurable standards for such a capability set and the establishment of time bound targets for digital capacity building are essential for the success of such efforts.

vendor lock-ins. They must not be bandwidth intensive. Further, wherever possible, Free and Open Source Software should be adopted (added, IT for Change). In making these design choices, the executive must consult citizens and their elected representatives (Group 4).

3.1.3 When government agencies enter into contracts with technology providers for the design and maintenance of digitalized systems, they must guard against the risk of such projects becoming a means for permanent rentiering by third parties, instead of furthering public interest mandates. Such contracts must have clear provisions for technology transfer so that government agencies can internalize the ability to build and manage new digital systems without costly lock-ins, and redesign them if need be to achieve intended outcomes (Group 4).

3.1.4 'Privacy by design' should be a core design principle in digitalized systems/ platforms for state-citizen interaction. In cases where this principle comes into conflict with requirements under the right to information and open data laws and policies, competing considerations of privacy and transparency must be effectively reconciled through appropriate technical safeguards[12] (Group 2).

3.1.5 Algorithmic decision making in governance cannot displace the role of public deliberation to reconcile competing interests towards the common good or violate constitutional rights of non discrimination[13] (Group 3). Citizens must have a right to seek an explanation about the system that was adopted and the steps that were followed in arriving at these decisions, to ensure that automated technologies do not reinforce existing biases and inequalities[14] (Group 2, 3). Therefore, in such automated decision making processes, audit trails must be maintained to establish accountability. Such audit trails must be within the purview of the Right to Information Act (2005) (Group 2). Source code and algorithmic design must be accessible for scrutiny by a designated regulatory authority (added, IT for Change).

Section 4. Data in and for governance

---

[12] Design choices in digitalized governance must not further the 'transparency paradox', a situation where the privacy of the powerful groups and institutions is protected while that of the poor is completely compromised.

[13] Algorithms rely on probabilistic analysis for aiding predictive decision making. They can amplify existing social biases and inequalities in ways that are not evident even to their creators. For example, in the United States, law enforcement agencies make decisions pertaining to parole through algorithmic assessments that assign risk scores to offenders. These risk scores indicate the likelihood of an individual re offending, and are arrived at through a mathematical formula that draws upon information about offenders' education levels, their friends' criminal records, their performance on other psychometric tests, alcoholism in the family and so on. Civil rights groups have flagged that the attributes used by these tools are loaded against blacks – with the result that blacks are more likely to be assigned higher risk scores than white offenders. See https://www.propublica.org/article/machine bias risk assessments in criminal sentencing for more information.

[14] The European Union General Data Protection Regulation, which will come into effect in 2018, allows citizens to seek 'a right to explanation' regarding an algorithmic decision that was made about them under Article 22: Automated individual decision making, including profiling.

4.1 Data in governance should be regulated as a common pool resource

4.1.1 Data generated and contained within governance systems should be treated as a common pool resource and held in trust by the state[15]. This data can include but need not be restricted to;

- Data collected through public information seeking drives and undertakings such as census and official household surveys or land and water surveys
- Data generated for and through process documentation in state administration
- Data and metadata captured through online citizen engagement platforms, websites, portals and other mechanisms

4.1.2 Data systems in governance should primarily be used in public interest for the purpose of democratic governance. While the state can have the right to use data for specified governance functions and informed decision making, it cannot assert ownership over the same for commercial gains, nor engage in sale, or trade of citizen data in a for-profit transaction (Group 2, 4).

4.1.3 Under exceptional circumstances, where commercialization of public data is permitted, it must be accompanied by strict regulation to ensure that such arrangements do not end up exploiting citizens (Group 2).

4.1.4 Citizens should have the right to know what information about them is being collected and maintained by government agencies (Group 2). All information and data systems used in governance must be maintained on public servers and available for audit by citizens. Such systems must disclose data in intelligible and easy-to-understand formats that allow the creation of public interest Application Programming Interfaces (Group 3).

4.1.5 Citizens should have the right to audit data systems in governance at every stage – creation, deployment and updation – to ensure their accuracy and veracity, and that the common good is always upheld (Group 2).

4.1.6 Data generated and/ or collected and synthesized by private parties should be freely available for access and use, in instances where it is essential to the delivery of basic services, has implications for vital sectors, is required for public-policy making and regulatory purposes, or in instances where it is being created through public funds or generated during the implementation of a public programme (Group 2).

---

[15] Article 39(b) of the Constitution of India requires the state to enact policies regarding the material resources of the country, including the rules of their distribution so as to serve the common good. To extend this to the digital context, spectrum is internationally accepted as a scarce, finite and renewable natural resource to which the state has a right of use. While data is admittedly neither organic nor scarce, a case can be made for recognizing it as a valuable common public resource for which a custodian framework can apply. Towards this, a special, statutory, agency with clear separation from the executive can be set up.

4.2 Information and data systems in governance should not violate citizen right to privacy and anonymity

4.2.1 A data protection legislation is non-negotiable for safeguarding anonymity of citizens [16] (added, IT for Change). Government departments must collect personal data of citizens only on a need-to-know and non-retention basis, the limits of which are determined by law. Also, when governance data sets are opened up for public scrutiny as part of right to information obligations, care must be taken to ensure that privacy is not compromised (Group 2). The violation of citizen right to privacy and personal data protection resulting from a breach of security in information and data systems created and maintained by government agencies must be treated as a criminal offence. Culpability should also extend to any private partners involved (Group 4).

4.2.2 Integration of databases for efficiency should be appropriately balanced by limiting access at different levels of government to that which is necessary for discharge of responsibilities (Group 2). Every decision to interlink databases must be separately evaluated for its implications for citizen right to privacy (added, IT for Change).

[16] When public data sets contain personal information, complex de-identification techniques that go beyond aggregation or masking of individual names, such as introducing contingency tables and synthetic data, may be required. See https://cyber.harvard.edu/node/99428 for more information.

Annex 1: Workshop Groups

Group	Topic	Group Members
1	**Ensuring accountability and local responsiveness in digitalized welfare services**	**Coordinators** Nikhil Dey, MKSS Sumandro Chattapadhyay, CIS **Rapporteurs** Eshita Mukherjee, DEF Jeevika Shiv, ANANDI Mukesh Nirvasit, MKSS **Members** Aanchal Mittal, DEF Chatar Singh, MKSS Karuna Muthiah, Pudhu Vaazhvu Project, Government of Tamil Nadu Praavita Kashyap, NCPRI Rajendran Narayanan, Liberation Technology Sanjay Sahni, SPSS Sharada Kerkar, DEF Shivani Lal, DEF
2	**A governance framework for data in governance**	**Coordinators** Parminder Jeet Singh, IT for Change Anupam Saraph, Independent Researcher **Rapporteurs** Inayat Sabhikhi, People's Action for Employment Guarantee, Pension Parishad Amrita Vasudevan, IT for Change **Members** Shankar Singh, MKSS Vineet Bhambu, MKSS Smriti Khera, IT for Change Abu Maroof, DEF Faakirah Irfan, DEF
3	**Rethinking the right to participation in the digital age: Guarantees and institutional safeguards**	**Coordinators** Anjali Bhardwaj, NCPRI Ashish Ranjan, Jan Shakti Jagran **Rapporteurs** Rakshita Swamy, MKSS Deepti Bharthur, IT for Change

		Members Anugrah Abraham, Change Alliance Gurumurthy Kasinathan, IT for Change Nikhil Shenoy, MKSS Patrick Ruether, FES
4	**Managing private actors in digitally mediated governance arrangements**	**Coordinators** Kshithij Urs, Action Aid Usha Ramanathan, Legal Scholar **Rapporteurs** Nandini Chami, IT for Change Seema Vashisht, NCPRI **Members** Col. Mathew Thomas, Retired Army Officer and Civic Activist Gagan, DEF Rajesh John Mathew, DEF Sukarn Singh Maini, SFLC Swapna Sundar, IP Dome Vinay Baindur, Independent Researcher