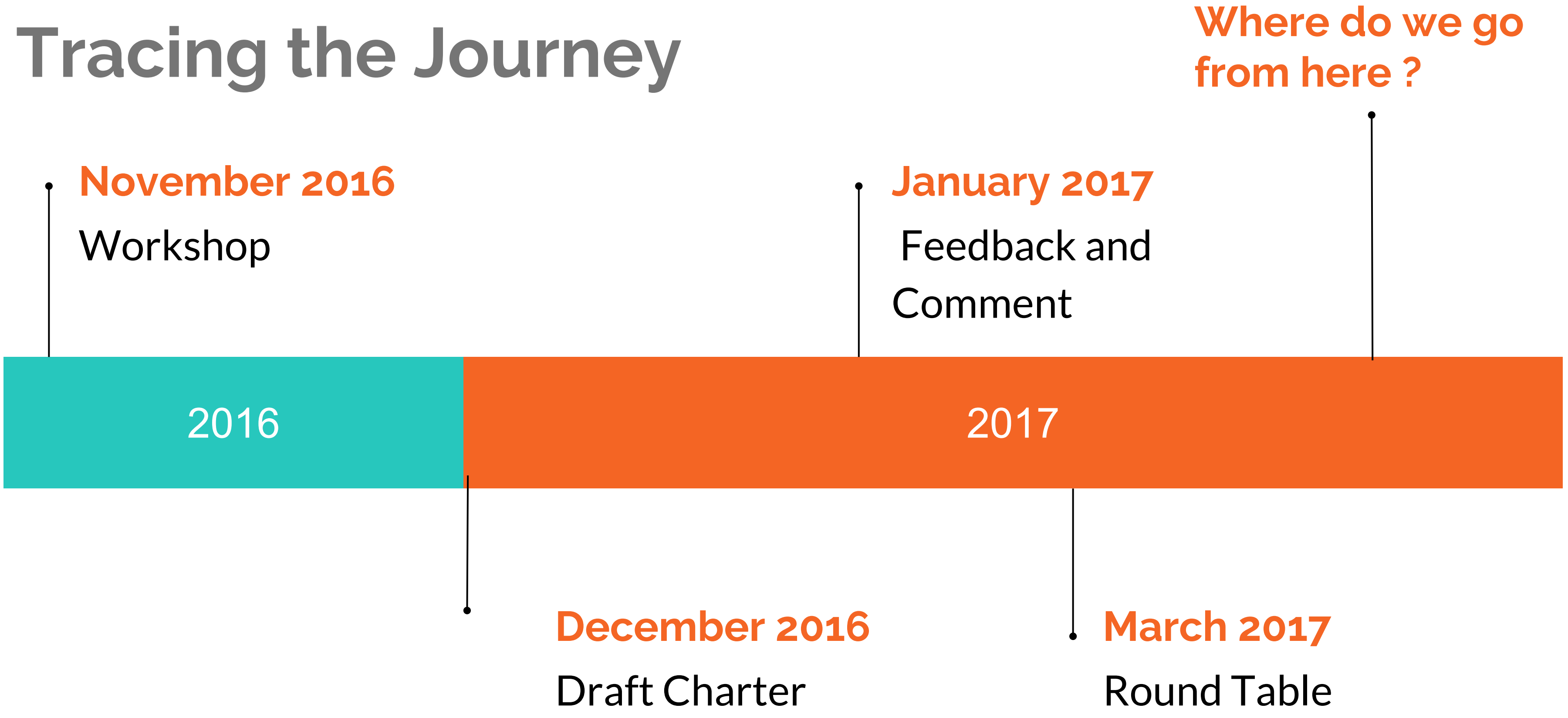
Democratic Accountability: Taking the Dialogue Forward

Round Table - IT for Change, 11 March 2017

Tracing the Journey



November 2016

Workshop

December 2016

Draft Charter

January 2017

Feedback and Comment

March 2017

Round Table

Where do we go from here ?

Charting the emerging landscape of digitalised, datafied governance

A new welfare regime that has destroyed the old social contract

The rise of a

‘Rule-by-data’ regime

State of Play: Welfare

Rupture of the social contract - Social, economic and political citizenship is no more a given, but has to be constantly established.

- Aadhaar is not ‘proof of citizenship.’ Yet, it is increasingly becoming the prerequisite to make any claim on the state(“Ration cards that have not been linked to Aadhaar will be considered bogus” -- U.T.Khader, Karnataka minister)

- The fiction of Aadhaar being an identity card that will help the most marginalised make their claims on the state.

Present but Presenceless? The hyper visibility of the most marginalized does not guarantee the legibility of their claims.

- Biometric authentication failures (UIDAI tender specification is 1,000 times less accurate than it should be to have a reasonable chance of building a truly unique database -- pointed out as early as 2011)
- No redress or compensation for unfair denial of entitlements due to biometric authentication failure, or database seeding errors. (Only a weak provision exists in the Aadhaar Act for UIDAI to set up grievance redress mechanisms if it deems fit)

Inversion of transparency - the citizen shall always be visible, but the state and new private actors in network governance arrangements remain opaque.

- Ubiquitous Aadhaar-based tracking of anything and everything (Eg. payments transactions tracking by National Digital Literacy Mission)

- The a priori correlation between going digital and seeking private involvement in governance.

- Naturalisation of non-accountability by calling upon volunteerism. Take the case of India-Stack. A payment architecture (UPI) is being built through an ad-hoc arrangement, without any regulatory backing.

The intermediary is dead. Long live the intermediary!

- The ‘sales pitch’ for digital governance has been its potential for circumventing corrupt intermediaries at the local level.

- But not only do new intermediaries emerge, new forms of corruption build upon existing client-patron networks -- which work on scale, in a corporatised and decentralised mode. (NREGS in Telangana and the ICICI Business Correspondent)

Digital by default? Not so much

- Manual processing options retained: Advanced democracies such as Netherlands, which have over 95 per cent internet penetration continue to have offline systems in place.

- Convergence seen as automatically permissible because of building a unique identifier that enables database interoperability (contrast of the UID with the Social Security Number)

- Right to audit welfare delivery (in its individualised form, it will be along the lines of the right to explanation; and in its social form -- a much larger idea of auditing new intermediaries, new partnerships in network governance, new technological/data back-ends)

State of Play: Data in governance and data for governance

In data we trust?

- What the Sameer Kochar expose reveals about the yawning gaps in our data regulatory regimes (no data protection guarantees, no penalty for data being compromised, no intimation about data breaches despite Shah Committee recommendation)

Keep calm and leave it to Big Data

- The ideology of data driven governance is pervasive even if India's state led big data capabilities are still nascent. (Interviews with MeiTY, what DoST is embarking on)

- Big Data analytics will lead India's policy efforts - RAS, My Gov, e-taal

- Old exclusions become recoded in this paradigm - predictive policing, DBTs, smart city planning, ITS in transport.

Data convergence: For whom? Towards what?

- Techno-design features that can enable us to maintain balance between
    - Individual privacy and transparency ;
    - local discretion and centralised efficiency
- We may also want to ensure interoperability, while ensuring convergence choices can be made on a case-by-case basis.

To retain or not to retain?

- To create a data ecology that respects and protects constitutional guarantees of citizens, we need to take into account the following considerations:

- Political trade-off: transparency/privacy
  social trade-off : separations of the realms of the private and public (what this means in practice: different modalities of releasing data sets -- personalised, pseudonymised, anonymised)

- Economic trade-off : private innovation/ public accountability wrt data commons

What is data sovereignty again?

‘According to some estimates, the value of European citizens’ personal data has the potential to grow to nearly €1 trillion annually by 2020.
(EU Fact sheet, 2016)

- The Google case in the ECJ showed that re-users of publicly available data can be made responsible under data protection.
- ‘Data controllers must prove that they need to keep the data rather than you having to prove that collecting your data is not necessary. Providers must take account of the principle of ‘data protection by default’ (EU Fact Sheet, 2016)
- Data sovereignty for the global South -- an emerging challenge

So, what can citizens' right to their data look like?

- **Data protection and security (EU GDPR landmark development)**
  - Strengthens the right to be forgotten which is "about making sure that the people themselves – not algorithms – decide what information is available about them online when their name is entered in a search engine."
  - Codifies 'Data protection by design' into big data management and 'data protection by default', which means that the default settings should be those that provide the most privacy.
  - Ensures affirmative consent - citizen will receive clear and understandable information when their personal data is processed.

So, what can citizens' right to their data look like?

- **Data protection and security (EU GDPR landmark development)**
  - Allows access and correction of personal data,
  - Right to object to data processing,
  - Right to be informed when data security is breached
  - Right to data portability
- But what about data as public value resource/ national economic resource?

Do we need a data ombudsman?

- Two separate authorities for transparency and privacy (Canada model -- Information Commissioner and Privacy Commissioner)
- A single authority to take charge of freedom of information and data protection issues (UK model)
- But, In this approach, the issues pertaining to economic governance of the data commons falls between the stools.

Questions

What should a digitalized service delivery model that guarantees democratic accountability look like?

a. Should welfare service data bases be convergent at the back end? (Convergence -- for whom? Towards what?)

b. How can we create tamper-proof records of digital processes that inform the decision-making on a welfare claim? Should there be institutional and techno-measures to ensure that the level of transparency remains the same for state and citizen? Ex- can there be same dashboard view for both administrative and citizen logins? (**See for reference, comment made on section 1.1.3 of draft charter**)

c. What principles – techno-design, last mile implementation, any other? – should be followed for accountability in digitalised service delivery?

d. How should grievance mechanisms be designed in the context of digital mediation of services?

How can legal-institutional systems for data-in-governance and data-for-governance be designed to ensure public interest and the promotion of people's rights?

a. What legal-institutional lacunae relating to the data ecology undermine democratic accountability in the current context?

b. How can techno-design enable a federated data architecture that addresses competing considerations for accountable governance?

- What data should be aggregated and what should be maintained in a localised manner? What considerations should inform choices on data convergence? (keeping in mind need for optimal balance between privacy and transparency; local discretion and centralised control of data veracity etc.)

- What kind of policy do we require on data retention in government databases? (**See for reference, sections 4.2.1 and 4.2.2 of draft charter)**

c. What broad guidelines need to be linked to proactive disclosure and standards for open data? For instance, what should be the procedure for changes in taxonomy - changing 'views' and changing 'fields'?

How can legal-institutional systems for data-in-governance and data-for-governance be designed to ensure public interest and the promotion of people's rights?

d. How can citizen right to audit data-in-governance be imagined? How can it cover audit of open data systems, software, algorithms etc?

e. What kind of legal-institutional framework do we need for governing data in and for governance (including data collected through private parties)?

- When managing data in governance systems, what is the balance we can strike between allowing room for innovation and protection of citizen privacy if and when we allow private/ non state actors to use them? (**See for reference, section 4.1.3 of draft charter)**

- What are considerations to take into account when we articulate a position on privately collected data for public use? **(See for reference, section 4.1.6 of draft charter)**

How can legal-institutional systems for data-in-governance and data-for-governance be designed to ensure public interest and the promotion of people's rights?

f. What institutional mechanisms should be in place to manage data that emerges from state-citizen engagement generated through consultative processes on third party social media platforms? Should these platforms be held liable to comply with specific data requests from the government? **(See for reference, section 4.1.1 of draft charter)**