Observations on

WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA

Rahul Tongia, Ph.D.
rtongia[at]brookingsindia[decimal]org

This note is in a personal capacity only.

Relevant PERSONAL BACKGROUND:

I am a scholar/researcher/professor on issues of technology and policy, and am presently a Fellow at Brookings India, a not-for-profit Think Tank based in New Delhi.

I have been a long-time faculty member at Carnegie Mellon University (CMU) (where I remain an Adjunct Professor), including in the Depts. of Engineering & Public Policy and School of Computer Science. I have spent decades working on issues of ICT and human development, digital divide, etc., including having served as the Vice-Chair of the UN ICT Task Force on Low-cost connectivity / Enabling Environment. I have also co-taught classes on privacy and other policy issues in ICT at CMU, working with some of the world's authorities on privacy.

I am active in issues of Smart Grids, having set up the Government of India's Smart Grid Task Force (as its Advisor), and am also the Founding Advisor of the India Smart Grid Forum.

I presently am leading a study on precisely similar issues of data ownership/rights/access/privacy for the power sector. Even without a smart meter, utilities, at the least, can figure out when someone is home or not (with digital meters that record time of day data). This is a personal security risk. As things get "smarter" there is scope for energy efficiency, but also much more profiling, e.g., figuring out if a consumer is BPL or APL.

Brookings India hosted a workshop jointly with the National Smart Grid Mission (NSGM), Govt. of India, on Consumer data and its rights. The report, FYI, is at:

https://www.brookings.edu/research/power-sector-data-and-frameworks-thinking-ahead-for-data-usage-access-and-rights/

Summary and Key Issues/Suggestions

1) [Kudos on a strong intro]:

   "*—Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state.*"

   However, this assumes a clear distinction between state and non-state actors. However, many aspects of life in India involve state-owned enterprises, or government departments offering (effectively) commercial services, including electricity, transportation, etc. How are these to be

handled. Calling things "State", even if linked to taxpayer money at the back end, is a slippery slope that should explicitly bounded. There is also the known issue that many "public services"(including electricity, transportation, etc.) are either governmental or outsourced to private operators, franchisees, consultants, etc.

2) The draft has a lot of great information, and asks virtually all the right questions. But the issue isn't just asking the questions, but stepping back from the details to the big picture. What are guiding principles that help us overcome conflicts or trade-offs? There are 7 principles listed, but these may not be enough.

   One of the major frameworks that can be applied is the *precautionary principle*. Drawing from lessons in other spheres, waiting to see damage or harm and then regulating it may be too late. In the data world, it's very hard to put the genie back in the bottle.

   A possible set of guiding frameworks could include [portions in RED overlap with the existing seven principles as given]:

   i) *When in doubt, err on the side of personal privacy/data protection.* The norm should be opt-in for data sharing as opposed to opt-out.
   ii) *Consent is a necessary but not always sufficient condition for data access/usage/etc*. Consent is useful but limited, due to issues of complexity, bundling, implicit consent, and unstructured consent (including ambiguity/interpretation). This can be improved by having discrete consent norms instead of blanket consent norms. One should not be able to consent away one's fundamental rights or future recourse.
   iii) *Ambiguity and uncertainty should be minimized, and there should be mechanisms to test/check any norms or practices against the law*. This will then enable things like Safe Harbour. Naturally, this will not be perfect, and may need to be iterated upon. Just like there are Information Commissioners, one may want a body of Data Protection Commissioners, to help educate, interpret, and enforce data protection rules. [For example, Canada has a Privacy Commissioner – data protection commissioners can do even more.]
   iv) *Legitimate data access in national needs such as law-and-order or national security need a bounded, explicit, and controlled framework, including oversight and recourse.*
   v) *There should be no differences in rules for public versus private creators/users/etc. of data,* keeping in mind point (ii) above.
   vi) *There should be a layered approach to privacy/data protection*, with some aspects inviolate, some voluntary, and a large segment in between which will evolve based on the market, case law, etc.

3) How does one treat electricity companies? [This example isn't just because it's one I'm active in, but it is a strawman for similar issues outside the direct IT sector.] Electricity companies are corporates but mostly state owned. Electricity is a public utility, and one with public good, but at the same time commercial. When dealing with consumer data, there are few issues of grid-level or National Security (those are mostly higher up in the system, especially with

transmission). It would be easy for any utility to claim national interests, but we have to prevent overreach of such claims.

Responding specifically to the Qs listed in the draft [not all topics are addressed, and there can be overlap in topics, hence these are best identified by name instead of number]:

1) Territoriality

This is a tricky question made harder by the "flattening of the earth" thanks to the Internet and cyber-communications.

One can make Indian law mandatory for all services aimed for Indians, but we wouldn't want to make rules only for India else it may restrict global participation in innovation.

Suggestions

a) India should join forces for global harmonization for minimum and necessary global conformity that matches the majority of the world – a few censorship oriented regimes may not participate.
b) There should be an elastic framework that sets a minimum set of laws/regulations applicable for any data of Indian consumers, combined with an ability to escalate this to a tighter framework as when where deemed necessary on a case-by-case basis.

A generic framework could be:

Level 1 – minimum rules applicable for all cyber-transactions and presence in India

Level 2 – Minimum rules for entities or transactions based in India or tailored for India (tighter than level 1)

Level 3 – Minimum rules for entities or transactions that meet well-defined criteria for necessitating higher levels of compliance (combined with burden of proof of compliance, failing which penalties). E.g., a healthcare data provider in India. Implications of a possible breach combined with size of the entity (including its ecosystem – not just shell/holding companies) can be criteria (larger companies are more able to comply).

2) Scope

It is NOT necessary to have separate laws for public versus private. For starters, public sector in India is often dominant, and often commercial YET governmental. Second, other than direct national security issues, which anyways would have waivers or separate norms, other datasets/collection/storage/processing should have tighter norms. E.g., the census. This is tightly protected, else people will not divulge true answers.

I cannot think of a single case where a government entity can ask – we need looser rules. Even for things like epidemic detection using healthcare data – there is enough anonymization and aggregation possible to still allow analytics to work (e.g., via k-same anononymity frameworks).

Where you have to find specific individuals, just like with the law, waivers or permissions should be possible.

A compliance timeframe is reasonable, but it should be realistic, without continued roll-overs, stays, litigations, etc. Witness how Environmental norms for power plants, by MoEFCC, are ignored by power plants, ultimately resulting in a delayed rollout – in part this is due to a lack of a realistic roadmap for implementation.

3) Sensitive and Personal Data

It may be helpful to separate "personal" from "sensitive". Personal relates to identifiable, even if to a profile instead of a physical person (e.g., the resident at flat 123, house 6, road B, etc.). Data vs. information can be a red herring – we should use the broader of the two terms, and then clarify it encompasses both. Information can mean data plus inferred information, and thus information is broader. Importantly, information spans not just data but includes meta-data.

There is a simple reason to separate personal from sensitive. Sensitive can be non-personally identifying as well. E.g., knowing voting patterns at a neighborhood level. Based on public data of donations made to respective parties. Alternatively, some personally identifiable data may not be sensitive, but worth protecting. Thus, personal can be aggregated and anonmized/pseud-anonymized and then used more freely, but sensitive data should be allowed the same.

Data about not an individual but a profile is also data worthy of protection. This profile that a company makes is both valuable and also important since it creates linkages or impressions that can be important. E.g., if one particular flat orders some types of medicines – doesn't matter who exactly (often the ordering can be by the breadwinner of the family, but now someone else knows SOME person there suffers from X. Hence, any company is free to make a profile about me (e.g., spend-thrift vs. heavy-spender), but as soon as they do so, they have created a persona or avatar for me, and hence come under the rules.

4) Sensitive personal information/data

This absolutely should be treated with higher norms, and the scope should expand to include all the terms/issues as per EU's GDPR.

Websites visited should be sensitive information, even if these are not individually identifiable. If someone visits "how to beat skin cancer" or "how to quit a job early" that's their business. The ISP is responsible ensuring these data aren't tied back to any individual per se. One may argue that Google/Microsoft always do so – if they build a persona, they can, but they then have to treat such a thing as per regulations (e.g., cannot disclose or sell that information, except without a warrant). NOTE, the content of a website isn't the issue – even the title/address is enough!

5) Processing

Manual and automated/digital should be treated the same. If one says one can allow looser laws for manual since one cannot do analytics easily on manual data, either (i) that is not true; or (ii) it may be true, in which case asking for equal restrictions is easy since they would comply by default.

The only case where a distinction helps is in terms of obligations and liability. A controller who is "in charge of " (e.g., "owns") the data is the one who should be careful in the terms they set for their partners who may be processors. If there is a failure or breach by a processor, it would behoove both entities to help resolve the issues (ranging from informing, rectifying, paying penalties, etc. as applicable).

6) Processor and Controller

It is arbitrary and loose to allow a distinction – the same norms should apply to both. Rather, to all entities in the chain of data (collection, storage, processing, usage, etc.)

7) Exemptions

"Fair use" type exemptions (as borrowed from copyright laws) give exemptions for personal/household use and articstic/literary use. Scholarly use should not get an exemption as they can utilize aggregation/anonymization for their purposes. National security should have separate norms for limited, governmental, and restricted uses, with their own oversight mechanisms. "National security" should not be blanket permission for a fishing expedition with data. On the other hand, there are reasonable and helpful law-enforcement and security needs for accessing data.

Linked to "national security is "preventing a crime". Instead of generic data-driven analysis, ***specific*** queries and limited analysis can be allowed, with a framework and oversight. E.g., if one suspects something is amiss, an authorized investigator then queries data – this is no different from getting a warrant to check.

Regarding taxes, there can be 2 ways to look at this. First, if one wants to do broad analysis of complies, the total data sets can be used to see if there is a mismatch. E.g., if only 1% of the population pays income tax above threshold of (say) 10 lakhs, yet there are Y crore luxury vehicles sold annually, something is amiss. This points to the need for new laws and enforcement. This is not personal. To become personal, one would need a warrant. OR one needs a law (which may exist) which is to have digital transactions and/or use of a PAN card for any high-value transactions.

8) cross-border flows

These are necessary in the modern world, and an adequacy framework should be a starting ground for norms. One can always apply stricter norms (see the tiered approach suggested above, and points on incentives for reducing cross-border flows at the end).

There can be 2 major means for cross-border flows. First is a company with a presence in India links to its global system. Second is a company outside India that a consumer/citizen in India chooses to

voluntarily deal with from India. Often, the latter can be samller and/or there is no direct transaction with them (financial).

One solution can be that as soon as one has a financial dealing, then Indian laws apply (even if they are stricter than adequacy laws). It is not clear if this is enforceable, and we may have to evolve norms. E.g., the App Store or Play store. One may find many apps for 50 or 100 rupees, affordable to many Indians. The App developer may be outside India, but the Play Store/App Store (Android/Apple) has a presence in India. It's not clear if one can make the stores liable (even if they are respectively compliant).

Maybe one method is to evolve a "certified for India" mechanism that applies to apps, websites, etc. that have India *dealings*. That will give both consistency and confidence. If one doesn't have that, then the consumers are taking a risk of less recourse, but the developers are also taking a risk they may be held to a higher standard, even if through individual actions.

9) Data localization

(see above, which links to this)

One should *encourage* data localization. If one is taking data offshore for convenience reasons (e.g., scale of processing) then that is distinct from taking it offshore for legal liability protection reasons. Since we cannot distinguish, we should remove the loophole that data elsewhere has less protections per se, with a minimum set of rules applicable to any entity that *transacts* in India.

It may be difficult to separate personal from sensitive personal data. It's easy to make a list of what is sensitive (common sense) but what else becomes sensitive? May need an evolving list. One that also discourages gathering of sensitive data, regardless of where it sits. Thus, one only gathers sensitive data for a good reason, and has a compliance cost to do so.

10) CONSENT

"Informed Consent" – this sounds appealing, and is necessary, but it may not be sufficient without secondary checks and balances. Is "informing" sufficient? Numerous studies have shown that legalese in "terms and conditions" are often confusing, and often not read. But one regularly checks off "I agree" just to proceed further. In a famous test, a bank once wrote to a large test sample, buried in the terms, something to the effect" write to us with this line/phrase, and we'll credit your account $100. Not a single person did so.

Even otherwise, many times one has no choice but to consent, else they cannot transact. To make claims of "you have a choice" may be naïve – many things are either dealing with monopolies or de-facto monopolies.

Most importantly, one shouldn't be able to consent away ones rights, or allow unreasonable terms. Many terms state things like you shall not publicly criticize, or sue us, etc. Those remedies must always be allowed.

One goal should be to have layered consent, e.g., if I want to use an App that asks for permission to, say, access my camera, storage, contacts, etc., I should be allowed to use the app without saying yes to all

the permissions. This may mean I lose *some* functionality, but developers should then layer their offering accordingly. NOTE, this is not something easy to mandate or worthy of regulation but one where new frameworks and positive encouragement towards these can help. E.g., if a company does so, then they benefit from safe harbor norms (see discussion on safe harbor).

CHILDREN

We can and should enable children-specific rules and norms that allow for more restrictions. The benefit is lower risks to children, and parents also have lower fears. While this can help, one cannot ensure that kids don't bypass this and sign up for "regular" services. E.g., YouTube Kids app – doesn't show some mid-level search results due to sometimes overly-strict filtering (erroring on the side of caution).

This is a cat-and-mouse problem in general. One solution or need may be to focus rules on key entry/exit points for data services. One can list the handful of service providers (Apple/Facebook/Google [alphabet[/Microsoft) etc. which control most transactions. They should come up with compliant and innovative solutions. Specifically, one would need:

1) Appropriate offerings
2) Voluntary opt-in by parents (and kids)
3) Compliance and enforcement

If a company doesn't have such offerings, they would face increased risks/liability for any failures, and have higher burdens for ensuring no negative outcomes/happenings. It may be easier to create a restricted environment that has no marketing/tracking/etc.

18 is normally an age of consent, but one may want a mid-grade level of access, say, above 14 or 15, at the risk of the individual. BELOW this age, one needs parental opt-in. BUT one cannot and should not rely on a strict number per say (hence the "opt" part). This is because for any age chosen, one can find people older who are not ready, and younger who may be ready. This applies for many things ranging from driving/dating/drinking/etc.

Suggestion – staggered norms:

1) Younger – very strict rules; no purchases, etc.
2) Mid- more freedoms, but some limits as designed by providers (and maybe mandatory notification/access) to a parent or guardian.
3) Full (adult) freedoms

PURPOSE SPECIFICATION AND USE LIMITATION

This is very tricky as *some* things can be known up front, but others may emerge over time. Alternative, a broad placeholder may allow many things, e.g., "to help improve the quality and efficiency of the service(s) delivered" – that could allow almost anything.

Declaring a specification is still helpful since this forces the data user/owner/etc. to think hard about what they want to do. Then, there would be grounds for them to be challenged down the road.

Can use limitation be considered without tight purpose specification? Perhaps, if we consider this to mean TYPES of uses and relationships. We can differentiate between "self-use" and "third-party use". The latter will more easily trigger regulations. If they want to do it internally, then it becomes both more limited and easier to ensure compliance since they anyways have compliance norms.

Sectoral regulators, who have domain expertise, may help.

SENSITIVE PERSONAL DATA

As discussed above, these should be segregated, and have higher norms, at the very least, as high as the combination of sensitive and personal data, but rather higher.

STORING DATA AND QUALITY

A dual of quality is right-to-access and also repudiation. We have been suggesting that an examination of data ownership frameworks can allow a consumer/citizen to access their own data, and also question its accuracy. This is easily understood for things like public utilities (electricity, water, etc.) or commercial transactions (mobiles, TV, etc.)

INDIDIVUAL RIGHTS

(see other points)

This links to the issues of who owns the data.

There are some data that consumers have created. E.g., how many GB of data do I consumer per day on my mobile? High usage may indicate travel (so no WiFi) or watching a movie. Naturally, the service provide will know this. What should be regulated is what they can do with this – they cannot share this, nor "tailor" offerings for me in a discriminatory manner.

Any such data, e.g., related to billing and commercial terms of service, should be accessible to a consumer for free. If large quanta of data are required, then a nominal and marginal cost fee may be charged. E.g., in the power sector domain, residential users (homes) should get free access, but larger (HT) commercial users should pay a nominal fee to get their full data – this should cover the costs of making such data available – a win-win situation.

Right to be forgotten is tricky, but ultimately, one that is akin to mandated censorship. If someone commits fraud, it is in the public interest to know that a person was so (or, e.g., was a child molester). On the other hand, the worry was if one has false claims against them. A better solution is where a verdict was in someone's favor—that should also be made public and easily found. This "right" is mainly used by the elite who have the means to get some parts of their online presence modified. Instead of trying to only get a specific version online, even if that may be trying for the "truth", a better framework may be for all aspects to be accessible online, warts and all.

REGULATION AND ENFORCEMENT

Co-regulation is not just a middle ground, it can be interpreted tightly or loosely to spread to either end of the spectrum (command and control vs. self-regulation).

There are two different ways to consider regulation. First is a light touch that only responds "when there is a problem". The other extreme is to prevent problems by laying out what can and cannot be done. The problem with the latter is new issues can and will come up for which norms are not yet spelled out.

A reasonable framework is to allow self-regulation that meets the layered approach to privacy, i.e., ensures a minimum level is met, and other levels of privacy are based on choice, the market, etc. This still allows self-regulation to be over-ridden when there are risks to the public or even selected individuals.

ACCOUNTABILITY AND LIABILITY

As we move to a far more granular and "real-time" world, including via IoT, segements of data will need to be seen/used by more and more entities. It may not be practical or even necessary to make all of them equally liable for a breach of norms. If there is a clear "prime" (equivalent to the System Integrator in large IT projects), they are ultimately responsible. They would be free to set up back-to-back agreements with their sub-contrators/partners/etc. If there is no prime, then the liability would be on the entity which led to the breach of privacy.

Mandatory insurance may not be a good solution as this may lead to moral hazard. A bigger issue is the lack of insurance models today for data security and privacy (NOTE – for insurance, privacy is a subset of broader issues of cyber-security). Security is likely a more robust framework from which to consider insurance as well as reporting norms.

If one is hacked versus one is lax in cybersecurity, and this results in the breach of personal data – the end result is the same, and hence penalties/obligations to inform/liability should be similar.

BREACHES AND NOTIFICATIONS

It's not clear if a single criteria is enough to justify inclusion or exclusion from notification. E.g., say we use 500 people as the cut-off; is this to say that 499 people isn't roughly as bad?

Just like with disease burdens (exposure, impact, remediation), we can have multiple criteria help guide where disclosure is required (number of people impacted; severity of possible damage; need for action.

If there is a breach, and due to the breach an individual(s) faces identify theft or other negative implications, the costs of both monitoring solutions as well as clearing up one's "digital identity" or equivalent should be borne by the party/parties at fault.

CATEGORIZATION OF DATA CONTROLLERS

It is helpful to have segmentation of responsibilities based on criteria such as size of the company, to limit the burden and also delineate required effort levels. HOWEVER, it is not clear that turnover (revenues) is a sufficient criteria. Doesn't a small healthcare data informatics startup need greater privacy compliance/efforts/statutory rules/etc. than a medium-sized steel manufacturer?

Based on the sizes and other norms, companies may need audits/data privacy officers/etc. This is something that should evolve via best-practices as well. Mandating a "data officer" or "data privacy officer" shouldn't become a perfunctory "check box" to be ticked. Hence, a 3rd party audit is far more

important than an internal officer. The latter may become chosen by the entity to help them comply (and also pass the external audit).

Suggestions:

1) Segment based on a combination of not just turnover but domain space.
2) Sync levels with GST norms, to make it easier to know who is or isn't to be covered.
3) Focus on external audits over internal audits

DATA PROTECTION AUTHORITY

There should be an authority for this functionality. This should not be mixed with the CIC/RTI officers, whose mandate is different. Here, this entity should be charged with:

1) Education
2) Enforcement
3) Interpretation of existing rules.

They should NOT also be setting up the rules. This is akin to the difference between legislation and regulation. E.g., in the US, the Clean Air Act only gave congress the power to "regulate pollutants harmful to human health". It did NOT specify what levels of sulfur emissions were or weren't allowed by (say) power plants. That job fell to the Environmental Protection Agency.

ADJUDICATION

Sitting above the Data Protection Authority should be a different body that can be used equivalent to an appeals court.

This body should have adjudication officers who are not just versed in IT rules, but also domain specific knowledge (e.g., specialists for finance, healthcare, etc.).

Caps on penalties (e.g., Rs. 5 crores) aren't necessarily appropriate. If 100 million people have their identities stolen, and have a liability or headache/cost that is even if small, in aggregate this is a big sum. There should only be a clarification that penalties are meant to be reasonable and commensurate with the failure, and penal clauses are to be separately disclosed.

Class Action suits are appropriate – and need to be strengthened in Consumer Law as well!

REMEDIES

It is difficult to specify the limits/minimums/etc, but remedies need not ONLY be financial. These can also result in cancellation of license(s), break-up of companies, etc.

COMPENSATION

Mitigation for breaches/failures can include the following:

1) The entity was following best practices AND
2) The failure was due to a problem that affected the entire industry/sub-industry (e.g., a new day-zero vulnerability).

OFFENCES

Yes, some breaches should be viewed as criminal, and not just civil.

OTHER ISSUES (not covered in the summary questions)

1) Data protection can actually mean cyber-security, in which case privacy is a subset of the issues. Data protection versus privacy should be clarified. This entire white paper focuses on privacy. That is also data protection, but data protection can actually go further.

2) Time-frames
   There should not be pre-determined restrictions on length of data retention per se but obligations must continue, making it "expensive" for data to be held unnecessarily long. E.g., in the EU, there are restrictions on how long, e.g., an electricity company can keep a particular consumer data (sometimes 3 years) – this is restriction as electricity planning often needs decadal data. Same for planning infrastructure like housing, transport, etc.

3) Opt–in vs. opt-out
   The default should be consumers have to opt-in to allow their data to be used by others.

4) Creating incentives for stronger compliance
   While outside the scope of these norms, through other complementary means, one can incentivize greater within-India storage of data. E.g., there is limited data which can be sent outside the country, but if one is based within the country, one has higher compliance requirements BUT is also allowed to collect more granular if not personal data.

5) How do these laws apply in the world of AI, IoT, bots, etc.?
   We have to anticipate such things, and evolve norms that could range from shutting problems down after they emerge to pre-empting issues by setting up rules to be followed up front.

6) How do we translate these laws into actionable frameworks?
   Power utilities are woefully unprepared for this task. They don't have a CIO, let alone a CISO. One useful step is for consistent thoughts on who "owns" the consumer data? Is it the consumer? Or the utility, which is the custodian only? If the utility is the custodian, they still have data protection obligations, and they cannot claim a consumer gave them blanket rights to "use the data".

7) Safe harbor
   The concept of safe harbor and limiting liability can be useful, if an entity is doing the best it can, and someone else (3rd party) does something wrong. Of course, this should apply to the IT Act, where, e.g.,. a buying-selling website should not be immediately liable if a seller lists forsale something illegal. Of course, they are obligated to take down such an item once reported.

8) Awareness and Human Capacity are bottlenecks
   We may need funding and programs for these, both for end-citizens, as well as service/solution/content providers. The default for many questionnaires/data gathering should

include “don’t know/n.a./unsure/choose not to answer”, e.g., if someone asks about “have you ever had a surgery, and if so, for what?”

If I find a question online for a service that I don’t like, I should have the ability to flag this, just like we have ombudsmen, RTI officers, etc. 3rd party firms should also be geared up to do audits of entities, like required for financial systems/services.

Canada has a **Privacy Commissioner** – we may need a similar function in India, whose job is not merely to catch offenders but rather empower and enable compliance and mindset change.

9) Make this stuff easy, consistent, and transparent
   A lot of this stuff is evolving, has nuances, and perhaps trade-offs. If we consider 2 types of firms, simplified as “big” and “small”. “Big” can invest to comply. “small” need to be told exactly what they can and cannot do, and then have solutions that enable compliance.

10) 3rd party access to data – non-discriminatory
    There are many tricky areas. Can third parties demand access to data, at least on a non-discriminatory basis? Say an electricity company gets good data on its consumers. They can’t directly use it for more revenues. Say they want to monetize it (in a legal and compliant manner, of course)? Is that to be encouraged? If they raise revenues, like railways is look at hoadings/advertising, won’t that help lower electricity bills? This is true in a regulated rate of return world, but what of a competitive space? What about when this is a private provider (like Tata/Reliance instead of government electricity boards/corporations?

11) Undoing past problems, or even upcoming future problems?
    Lots of people have freely shared their Aadhaar card with 3rd parties. Even though is neither required nor encouraged, it has happened. Now what? [Frankly, Aadhaar needs fixing to make sure this isn’t a problem, but today’s framework isn’t set up this way]