To,
Justice Srikrishna Committee of Experts on Data Protection
C/O Shri Rakesh Maheshwari,
Scientist G & Group Co-ordinator, Cyber Laws
Ministry of Electronics and Information Technology (MeitY)
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003

Dated : Jan. 31, 2018

Dear sir,

Re: Submission of comments to the Justice Srikrishna Committee of Experts on Data Protection

The Internet Freedom Foundation (IFF) is a non-profit organisation created by members of the SaveTheInternet.in movement for net neutrality. Over one million of our fellow citizens wrote to the TRAI in April 2015 as part of the consultation paper on OTT services using the SaveTheInternet.in platform, and continued to engage the TRAI and the Dept of Telecommunications on subsequent consultative exercises in this area. IFF aims to promote the rights of Indian Internet users — freedom of speech, privacy, net neutrality and freedom to innovate - before policymakers, regulators, the courts, and the wider public sphere.

Our public advocacy and work on informational privacy and protecting the rights of Indian citizens vis-a-vis their data includes:

1) **Advocating for a comprehensive rights based data protection law:** Requests to pass a comprehensive data protection bill to protect privacy of users coming shortly after the historic right to privacy judgement by the Hon'ble Supreme Court of India [link]. IFF has aided Indian lawmakers in their efforts to advance proposals to create comprehensive laws to further provide for the protection of informational privacy and data.

2) **Accountability for the collection and transfer of data by private companies and large platforms:** IFF was granted permission by the Hon'ble Supreme Court to be added as an intervening party in the Whatsapp-Facebook data sharing case where we have pleaded for further disclosure of corporate data collection and transfer practices as well as called for interim orders to protect the interests of our fellow citizens [link].

3) **Regulatory caution to protect user privacy:** Participation in past TRAI consultations where we have highlighted the urgent need to protect user privacy, including:
    a) Submissions to the TRAI Consultation on Data Ownership [link]
    b) Inputs to the WiFi Consultation highlighting various concerns [link]
    c) Response to the Free Data Consultation [link] and our concerns on the recommendations made by the TRAI [link]
    d) Response to the consultation paper on Net Neutrality [link]

As we support privacy, security and the rights of users to control their data, the present submission makes an argument for the most effective form of regulation through a comprehensive data protection law.

To broaden stakeholder comment and inform a larger number of people, we also prepared a 5 page summary of the present white paper at, "Privacy is a Right", to help citizens in understanding the issues at play in this subject and empower them to be better placed if they wish to provide their views to the committee [link].

We are grateful and welcome the movement towards a comprehensive data protection law but have concerns having read the submission by academics and lawyers to this committee dated Jan. 31, 2018 ("Lawyers Submissions"). We adopt these Lawyers Submissions and wish to highlight the following points which are relevant to our stated position and work on securing individual privacy:

1. **Protecting rights and privacy of users should be the objective of the data protection law:** Data not to be construed as property with an individual having ownership over it. This would lower the level of serious protection that data demands as it may be suggested that it be freely traded and even economically exploited. Data needs to be construed as an extension of the individual and part of her circle of privacy, dignity and autonomy. A strong focus on individual at the centre of a data protection law is required, whose interest is paramount especially when weighed against state expectations or commercial interests. (As stated by the Lawyer Submissions, Recommendation No. 1)

2. **Adopt a principle based approach:** The committee should recommend a principle based approach drawing from the Report of the Justice A.P. Shah Committee which recommended nine privacy principles. Also, any exceptions to these principles should be narrowly tailored. (As stated by the Lawyer Submissions, Recommendation No. 2)

3. **Create an empowered, independent regulator to enforce the privacy principles and ensure an effective, citizen friendly adjudicatory system:** The effectiveness of the regulation will depend on the regulator and the enforcement. We adopt recommendations No. 3 and 5 of the Lawyer submissions in this regard.

4. **Aadhaar conflicts with privacy protections and any version of a citizen centric data protection law:** We submit that Aadhaar creates a vast surveillance power in favour of state and private entities and it conflicts with any meaningful standard of privacy and data protection. (Please refer Lawyer Submissions, Recommendation No. 4)

5. **A comprehensive data protection law is incomplete without surveillance reform:** It is relevant to note that despite current provisions applicable to the telecom sector only permitting individualised interception, there are widespread reports of mass surveillance being carried out in that sector. Reports have also indicated the use of invasive technical and commercial tracking technologies by telecom service providers in India, including the use of UIDH tracks or "super-cookies" [link]. We specifically call on the committee to incorporate necessary safeguards in the existing practices and regulations permitting surveillance in India. We request for an in principle recommendation, expressly stating that mass surveillance is illegal and conflicts with data protection. (Please refer Lawyer Submissions, Recommendation No. 6).

In addition to this we further submit some specific concerns:

- **A rule of law framework:** We expressly voice our concern against the deployment of technology frameworks (or, "consent stacks") for consent or privacy protections that undermines consent, purpose limitations and accountability (consent is one of the primary principles of data protection).

- **Big data is personal data:** The focus to fork out, "big data", from the definition of, "personal data" will undermine citizen rights. Aggregated data sets which are based on individual information have tremendous data protection implications. In all measures we recommend at the very least adoption of the Justice A.P. Shah Committee principles along with proportionality and necessity as articulated in the 9 judge bench decision in *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India* [W.P. (Civil) No. 494/2012] [link]. The principles of the 9 judge bench decision are inherent to any recommendation that may be made by a statutory authority.

We urge this committee to adopt the framing of informational privacy and data protection as not merely a property right in which “ownership” vests with a user, but even above and beyond that in which a person has inalienable rights. These rights are horizontally applicable, i.e. available against both state and private entities and are to be enforced by a specialised regulator such as a Privacy Commissioner and through a system of adjudication in which users can make complaints. We hope the this committee considers our submissions and drafts a citizen centric privacy and data protection law.

Sincerely,

Team Internet Freedom Foundation (IFF)
@internetfreedom