

September 8, 2017

Telecom Regulatory Authority of India  
Mahanagar Doorsanchar Bhawan,  
Jawahar Lal Nehru Marg,  
New Delhi-110002

RE: *Comments of ACT | The App Association Regarding the Telecom Regulatory Authority of India's Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector*

ACT | The App Association (App Association) submits the following recommendations to the Telecom Regulatory Authority of India (TRAI) in its request for comment concerning its Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector (Consultation).<sup>1</sup>

#### I. Introduction and Statement of Interest

The App Association represents more than 5,000 small- and medium-sized app development companies and technology firms across the world, including Indian startups such as iCoderz Solutions Pvt. Ltd. of Gujarat, and Exousia Tech of Chandigarh. As the world has quickly embraced mobile technology, the hyper-competitive app ecosystem continues to produce more innovative and more efficient solutions that leverage mobile technologies to drive the global digital economy across modalities and segments, augmenting consumer interactions and experiences throughout their personal and work lives.

The app industry has been in existence less than a decade, and serves as the driving force behind the rise of smartphones and an ever-increasing number of internet-enabled devices. As we detail in our annually-released *State of the App Economy* report, the app economy is a \$143 billion ecosystem today, the clear majority of which are startups or small businesses.

---

<sup>1</sup>[http://www.trai.gov.in/sites/default/files/Consultation\\_Paper%20\\_on\\_Privacy\\_Security\\_ownership\\_of\\_data\\_09082017.pdf](http://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf).

Innovators in the app economy highly value end-user privacy and trust, and regard these as principles that must be upheld to compete in the marketplace. While the TRAI's Consultation appears to be a precursor to the promulgation of a sweeping privacy regime. We appreciate the TRAI's development of its paper and for seeking public consultation on its contents, including through asking the specific questions it poses. We urge the TRAI to take heed of the lessons learned from near-draconian regulatory measures, such as the United States (U.S.) Federal Communications Commission's (FCC's) Broadband Privacy Rules that TRAI cites. Legal and regulatory consistency and certainty are integral to the continued success of the app economy that has flourished in the U.S. under the Federal Trade Commission's (FTC's) approach to the use and protection of personal data. We encourage the TRAI to emulate the FTC's approach to digital privacy when drafting its own privacy regulations in order to create an environment in which Indian app developers may prosper.

The App Association supports the TRAI goal to provide Indian consumers with more transparency, choice, and security when it comes to data privacy—goals our membership fully supports as a whole. However, we urge the TRAI to carefully consider its rules' potentially harmful downstream effects of overbroad and one-size-fits-all requirements that ignore the need for flexibility and scalability in data protection approaches as well as Indian consumers' ability to give informed consent to various uses of their data.

Through our experience with our membership, we understand that the digital economy is dynamically evolving and that a heavy-handed approach would produce far more harm to a business's ability in this space to adapt to market changes, particularly for downstream small business software app developers. For example, the rules' restrictions as they are currently written could potentially foreclose on a telecom service provider's (TSP's) ability to use its data to better assist consumers in a broad spectrum of ways, such as lending its data to advance increasing breakthroughs in artificial intelligence. We strongly urge that the TRAI's privacy rules, should they move forward, strike a balance between the benefits of additional use of data and the risk of privacy harms. To ensure the most informed path forward, we strongly urge the TRAI to initiate public consultations of draft rules and carefully consider the views of all stakeholders before moving forward and finalizing any requirements on companies doing business in India.

Further, we strongly urge for the TRAI to exempt small businesses from adherence to any such privacy regime to ensure that these key innovators are not driven out of business by the cost of compliance.

## II. The App Association Strongly Discourages the TRAI's Use of Invalidated U.S. Privacy Law as a Guideline in Structuring Its Potential Privacy Regime

The Consultation requests comment on how the TRAI should approach the definition of personally identifiable information (PII) and whether more laws should be added to India's existing telecom legal framework to ensure consumer privacy. Further, in Chapter IV of the Consultation, the TRAI referred to the FCC's privacy rules as "instructive," while recognizing that such rules have been repealed and are no longer in effect. The App Association has engaged with the FCC on this exact rulemaking and privacy issues extensively as the voice of small business software developers and innovators; and we further support the repeal of the FCC's broadband privacy rules. If it is the TRAI's intention to adopt the FCC's invalidated approach to privacy regulation, then it should be aware of its potential harmful effects which we have discussed extensively in filings before the FCC.<sup>2</sup>

For example, the App Association was particularly concerned with the FCC's interpretation of Section 222 of the Communications Act of 1934 (the Communications Act) and its potential to restrict an internet and TSP's ability to innovatively use its data to assist small business app companies further down the proverbial totem. In its rulemaking, the FCC did not adequately reconcile the fact that Congress never used the term PII in Section 222 of the Communications Act, or its definition of "subscriber list information."<sup>3</sup> This decision to include PII could have significantly tamper with the symbiotic relationship that exists between small business app companies and TSPs because of the sheer amount of data shared between them. If the TRAI follows the FCC's framework by placing too many regulatory burdens on data maintenance at the TSP level, then it will directly limit TSP's ability to share data that are predominately used by app developers, ultimately and unnecessarily damming up the stream that replenishes the lake of innovation for many of these small businesses. This does not bode well for small businesses, or the consumers they serve.

Additionally, the FCC's Broadband Privacy Order was based on an erroneous assumption that that TSPs have heightened access to broadband customer information over others in the internet ecosystem. This is especially unnerving when one considers the significant implication of the rules' ability to stifle the necessary sharing of data on which app developers rely to increase their apps' utility to millions of American consumers. We believe that the record demonstrated that the FCC's assumption was, at best, objectively disputed and, at worst, conjecture;<sup>4</sup> and we strongly

---

<sup>2</sup>

<https://ecfsapi.fcc.gov/file/10317038881692/031517%20ACT%20Reply%20to%20Oppositions%20for%20Recon%2016-106%20final.pdf>

<sup>3</sup> 47 U.S.C. § 222(h).

<sup>4</sup> See Oracle Petition at 3-7.

urge the TRAI to engage in a data-driven analysis rooted in realistic economic study to ensure that its rules accommodate the ever-growing and diverse app economy.

The App Association has consistently advocated for clarity and consistency in approaches to regulation, particularly in the areas of data security and privacy. As adopted, the Broadband Privacy Order introduces confusion and inconsistencies into the calculation that stakeholders must make when ensuring compliance with laws and regulations concerning the protection of consumer privacy. Therefore, it should fall out of the purview of the TRAI's consideration when constructing its privacy regime.

### **III. If the TRAI Is to Promulgate Privacy Rules, It Should Provide a “Reasonable Measures Standard” to Mirror the FTC’s Data Security Framework Basing Enforcement Actions on Proven Consumer Harm**

Should the TRAI move forward in adopting broadband privacy rules, the App Association strongly urges that the TRAI adopt rules aligned with the approach of the FTC. As an enforcement agency, the FTC has the authority to stop “unfair or deceptive” acts or practices in commerce. This gives the agency the flexibility to stop privacy practices where they diverge from consumer expectations. TSPs in the U.S. have long enjoyed and relied on established privacy principles consistent with the FTC’s long-standing framework.<sup>5</sup> These “ISP Privacy Principles” are a commitment on behalf of the ISPs to take reasonable measures from “unauthorized use, disclosure, or access...”<sup>6</sup> This is preferable, because the principles take a myriad of considerations into account, which allow them to meet market demands much more efficiently than the FCC’s current rules permit. The considerations to which the Privacy Principles adhere are “the nature and scope of [TSPs’] activities, the sensitivity of data, the size of the [T]SP, and technical feasibility.”<sup>7</sup> The App Association supports the FTC’s approach over the FCC’s Broadband Privacy Order because it provides more scalability and dexterity to stakeholders to accommodate the ever-changing market this data-sharing ecosystem experiences.

---

<sup>5</sup> See Joint Petition of American Cable Association et al. (Petitioners) for Stay, WC Docket No. 16-106 at 32 (filed Jan. 27, 2017).

<sup>6</sup> See Order at para. 5.

<sup>7</sup> See *id.*

Even as the FCC adopted its ill-fated privacy rules, then-FCC Commissioner Pai and Commissioner O’Rielly rightly agreed with this position in their respective dissents to the Broadband Privacy Order in noting that the privacy rules would inequitably and overly regulate certain market participants, while not fully demonstrating that such overregulation was warranted to advance its policy goals,<sup>8</sup> thus making this regulatory distinction seemingly arbitrary. Moreover, the FCC itself correctly asserted at the time that considerable ambiguity existed as to the scope and overall breath of its rules, which could vary dependent upon what Commission leadership presides over it in succession.<sup>9</sup>

We also strongly discourage the TRAI from implementing privacy laws that would emulate aspects of the European Union’s (EU’s) General Data Protection Regulation (GDPR) widely regarded as unduly imposing compliance obligations without a corresponding benefit to the public and/or are technically infeasible. For example, the GDPR is framed as extraterritorial (i.e. applying to organizations regardless of their legal or physical connection to the EU), when such requirements are massive disincentives to the free flow of data, and threaten needed legal certainty that companies need – both within and outside of India – in order to undertake research and development and create jobs; further, it is not feasible to apply to EU law to countries with no legitimate connection to the EU, presenting implementation issues that will impede the EU’s public policy goals.

Furthermore, it is crucial that the TRAI’s rules, if they move forward, be based on *proven* consumer harms, and not hypotheticals or academic theories. If the TRAI does not institute such a requirement, then its rules could provide unbridled authority to regulators and, thusly, permit government agencies to subject TSPs to enforcement actions unjustifiably. The stakes are just too high to gamble the growth of the Indian digital economy on unproven and speculative concerns, particularly given the broader, downstream implications to small business app developers.

---

<sup>8</sup> See *2016 Privacy Order*, 31 FCC Rcd at 14121, 14129.

<sup>9</sup> See *Broadband Privacy Order* at para. 16 (writing “[t]he weighting of “data security requirements under HIPA, GLBA, and other relevant statutory frameworks” and other indicia of reasonable data security required by the *Order* would be resource-intensive, and providers could not be sure that they would weigh the factors in the same manner as this or any future Commission.”).

### **III. The TRAI's Privacy Rules Should Allow for Stakeholders' Ability to Use Strong Encryption Techniques to Protect End User Security and Privacy**

The App Association notes that strong technical protection mechanisms, such as end-to-end encryption techniques, are required by TSPs and other downstream market participants to keep users safe from cyber-based harms, such as identity theft. Despite this reality, some government interests persist in demanding that “backdoors” be built into encryption for the purposes of government access. Such policies would degrade the safety and security of data as well as the trust of end users by creating known vulnerabilities that unauthorized parties can exploit. The viability of a small app development company's product from a security and privacy standpoint depends on its end users' trust.

### **IV. TRAI's Rules Should Facilitate Cross-Border Data Flows**

The seamless flow of data is essential to the functioning of the global economy. To support businesses' growth in international markets, app developers must be able to rely on unfettered data flows. Therefore, TRAI's privacy rules should unambiguously preserve this ability.

Increasingly, tech companies doing business overseas face regulatory pressure to build and/or use local data infrastructures. Data localization requirements hurt Indian exports and international competitiveness, and ultimately result in less choice in the consumer marketplace with higher prices. Further, small business app developers do not have the resources to build or maintain unique infrastructure in every country in which they do business. For these reasons, any further rules developed related to privacy protection in India must prohibit on data localization policies.

### **V. Any TRAI Privacy Rules Should Include an Exemption for Small Businesses**

Should the TRAI move forward with the adoption of a privacy rulemaking, we strongly urge that small businesses be made exempt from the rules' requirements. While our innovative members drive the growth of the digital economy, they do not have unlimited resources that larger companies do to address legal and compliance matters. Further, our members already face market effects that would cause significant harm to their business – and may even put them out of business – should they experience a data breach.

Therefore, we strongly urge for the TRAI to exempt small businesses from adherence to any such privacy regime to ensure that these key innovators are not driven out of business by the cost of compliance.

## VI. Conclusion

We hope the TRAI takes these proposals into its consideration as it moves forward to promulgate a privacy regime.

Sincerely,



Brian Scarpelli  
Senior Policy Counsel

Joel Thayer  
Associate Policy Counsel

Brad Simonich  
Associate

ACT | The App Association  
1401 K St NW (Suite 501)  
Washington, District of Columbia 20005