



GSM Association  
Level 1, Red Fort Capital  
Parsvnath Tower,  
Bhai Veer Singh Marg, Gole Market  
New Delhi-110001, India  
Tel: +91 (011) 66782420  
Fax: +91 (011) 66782403  
Web: [www.gsma.com](http://www.gsma.com)

21 November 2017

Mr R S Sharma  
The Chairman  
Telecom Regulatory Authority of India  
Mahanagar Doorsanchar Bhawan  
JLN Marg, New Delhi – 110002

Dear Mr Sharma

**Re: Privacy, Security and Ownership of the Data in the Telecom Sector**

The GSMA thanks the Authority for the opportunity granted to submit our further feedback. Having gone through responses of various stakeholders, it seems that a significant number of respondents tend to converge towards a more principles-based, horizontal approach to privacy. The GSMA welcomes some of the similar points made by other respondents (see a few footnotes quoted below). Therefore, we reiterate and request the following:

**A horizontal approach to privacy / data protection is needed:**

Compartmentalising digital services, or telecoms services serves no purpose. A more principles-based, horizontal approach<sup>1</sup> that applies to all processing of all personal information should be followed, and any additional requirements to address specificities be kept to a minimum.

**Differentiate among Personal Data, Sensitive Data and Metadata (Anonymised data)<sup>2</sup>:**

Not all personal data is of a higher sensitive nature (Sensitive Personal Data or SPI), and the level of protection required for SPI is higher than the level of protection afforded to less sensitive data. Thus, a clear distinction between the two must be brought out.

Increasingly important is to explicitly recognise that anonymous data **is not** personal data and that pseudonymisation can provide genuine safeguards without the need for consent.

**Follow same service same rule<sup>3</sup> in the digital ecosystem:**

To the extent that any obligations currently imposed on the Telecom Service Providers are to be retained because otherwise there would be harm to consumers, then all communications service providers should also be subjected to the same rules (e.g. about lawful surveillance and law enforcement) as those applied on telecom service providers under the principles of 'same service, same rules'. If there is a risk of harm to consumers, then arguably they should be applicable across the board.

---

<sup>1</sup> See e.g. USIPF, USIBC, IAMAI, ISPAI, etc. on need for a horizontal or technology/platform neutral approach

<sup>2</sup> See e.g. USIBC, ISPAI, IAMAI, COAI etc. on need to have distinction between Personal, Sensitive, Meta/Anonymised data

<sup>3</sup> See e.g. COAI, ISPAI, CUTS International etc.



### **Strike a balance between stimulating competition, protecting consumer privacy, and providing incentives to innovate and invest<sup>4</sup>:**

It is important to distinguish a situation where cases are considered on a case-by-case approach (ex post, after something has been alleged to have a negative impact on competition and consumers) from a situation where an authority is given the right to regulate ex ante (in the absence of any specifically alleged consumer harm). Regulation of data protection that results in an authority having to approve data protection schemes would likely result in a bottleneck of requests. The GSMA believes that ex post rules encourage accountable organisations to adopt effective compliance programmes so that they can not only comply, but can also demonstrate how they comply. This strikes the right balance between allowing authorities to check adherence to the rules and allowing organisations operate and innovate flexibly within the rules.

### **International flow of data is important:**

Cross border data<sup>5</sup> (CBD) flows are integral to a flourishing digital economy, socio-economic development, innovation, and competition. The APEC's Cross-Border Privacy Rules are a good example of international cooperation. Therefore:

- Restrictions and conditions on international data flows should be kept to a minimum and applied in exceptional circumstances only (such as threats to clearly defined national security issues, to be assessed on a case-by-case basis).
- CBD transfer rules should be risk-based and support measures to ensure data is handled with appropriate and proportionate safeguards while helping realise potential social and economic benefits
- To the extent that governments need to scrutinise data for official purposes, achieve this through existing lawful means and appropriate intergovernmental mechanisms

Please do not hesitate to contact us if you have any further questions regarding this submission or any other matter in which we might be of help to the TRAI and other stakeholders in India.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Emanuela', is positioned below the text 'Yours sincerely,'.

Emanuela Lecchi  
Head of Public Policy, APAC  
[elecchi@gsma.com](mailto:elecchi@gsma.com)

### **Copy to:**

Sh. Arvind Kumar, Advisor (BB&PA)  
Sh. Bharat Gupta, Joint Advisor (TRAI)

---

<sup>4</sup> See e.g. IAMAI, CUTS International, ITI, USIBC, USIPF etc.

<sup>5</sup> See e.g. CUTS international, USIBC, USIPF, ASSOCHAM, IAMAI, NASSCOM, EBG, etc.