Disney India

November 6, 2017

VIA E-MAIL SUBMISSION
(BHARATGUPTA.TRAI@GMAIL.COM)

Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi -110 002

Dear Sir,

Re: Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

Disney Broadcasting (India) Limited ("Disney") is pleased to submit these comments in response to the Telecom Regulatory Authority of India's ("TRAI") request for input on the issues related to data protection in the delivery of digital services, as identified in its Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector (the "Consultation Paper"). The Consultation Paper identifies a number of stakeholders inside and outside the telecommunications sector that are involved in the collection and use of consumer data, as well as the fact that technologies and platforms for delivering content to users are evolving at a rapid pace. As a provider of premium entertainment experiences, Disney appreciates the need to adopt responsible business practices that maintain consumer trust in this increasingly complex digital environment.

There is already a strong legal framework in place for data privacy and security under the Information Technology Act, 2000 together with the Rules thereto ("IT Act") and any gaps in the current legal regime should be addressed through frameworks that create incentives for industry to develop best practices and codes of conduct that focus on ensuring robust transparency and control for consumers. TRAI should also be mindful of the different types of services – and the different privacy risks they present. Services that have access to all or most of a user's communication or web browsing are differently situated than services that are primarily designed to deliver video content. Rather than taking a regulatory approach that may have unintended negative consequences for consumers, we believe that an emphasis on self-regulation and industry codes of conduct would result in more innovative and effective solutions for protecting consumers. As discussed in more detail below, a self-regulatory approach would result in more effective transparency and control mechanisms for consumers, more effective audit and enforcement approaches, and would address some of the limitations of the notice and consent model as applied to emerging data and analytics models.

User Control and Consent

As the Consultation Paper points out, online content and services are delivered through a variety of systems, platforms, and devices that are the result of a collaboration among numerous entities, including content providers, Internet-based platforms, telecommunications carriers, device manufacturers, mobile and desktop application developers, and service providers. Although TRAI's primary regulatory focus is on telecom services and other methods for delivery

of digital content, each of these entities plays a role in collecting and processing user data to enable innovative new types of services, features, and accessibility. Data privacy regimes around the world rely on transparency and consent to achieve appropriate protections for consumers. However, given the multitude of entities that collect and process consumers' data, consent requirements can become burdensome for consumers, particularly where they are not calibrated to the sensitivity and the risk of processing the data at issue.

Question 2 of the Consultation Paper asks for input on how consumers can be empowered to take control of their data. Because of the complexity of the data ecosystem, we believe that companies across the value chain should be encouraged to work collaboratively to come up with streamlined, easy-to-use consent mechanisms. For example, a content provider that hosts a portal to third-party content may establish a centralized control mechanism for users that would apply to all content accessed through the portal. Allowing this type of centralized consent relieves consumers of the need to configure multiple, individual controls. Likewise, customers of a platform provider may also benefit from a centralized control mechanism that would allow them to give consent at the platform level for data collection and use that takes place within individual applications on that platform. Instead of focusing on obtaining consent for each individual data processing activity, the focus should be on pushing industry to come up with common tools that will promote effective controls that consumers will actually be able to use. This path would help avoid "consent fatigue," where users simply check "accept" to move through a transaction or signup process without meaningfully reviewing the options. The key to all of these options for meaningful consumer control is a privacy regime that is flexible, allowing for further innovation in consent and control mechanisms as technology continues to evolve.

Question 2 of the Consultation Paper also asks whether users' consent should be obtained before using their data for commercial purposes. Requiring specific user consent is not appropriate in all circumstances – some types of data collection and use are consistent with user expectations, and the context of the transaction should be allowed to proceed without asking for additional user consent. For example, an entity should be able to use third-party vendors to collect or process data on that entity's behalf if the use of the data is well-controlled and otherwise consistent with the consumer's expectations. Likewise, a user should reasonably expect that a content provider from which it has made a purchase may advertise additional related content to that user. In all cases, the question of whether consent should be required should be tied to an examination of the sensitivity of the data at issue.

The IT Act appropriately distinguishes between personal information, which broadly covers any information relating to a natural person that can be used to identify that person, and "sensitive personal data or information" ("SPDI"), which includes highly personal items such as passwords, financial account details, health conditions, and biometric information. This distinction reflects the relative risks of disclosure of the different types of information, with SPDI being subject to a variety of specific heightened controls addressing the collection, use, transfer, disclosure, and retention of that data. The different treatment of personal information and SPDI under India's law demonstrates the principle that the amount of protection or privacy that should be given to any user-related data will necessarily depend on the context of what the information is and how it was obtained. We endorse that approach, which is consistent with other privacy frameworks around the world, and recommend that any expansion of the categories of sensitive personal information under Indian law be calibrated to the risk of harm to the individual, as well as the reasonable expectations of individuals regarding the collection and use of their data.

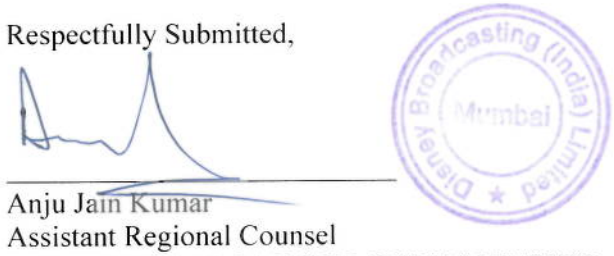
Industry Cooperation and Enforcement

In response to Questions 6 and 7 of the Consultation Paper, Disney does not encourage the government to establish a technology-based architecture or sandbox to attempt to regulate privacy and security practices. With the rapid changes in technology and the ever-increasing flow of data, a technology-based architecture to audit the use of personal data and associated content would prove impractical and likely stifle innovation. Further, it could raise concerns about government oversight over such audits and create a chilling effect on consumers' adoption of new technology. Such an audit system also could give rise to a different set of privacy concerns on the part of consumers about potential unwarranted government surveillance.[1] Creation of a government "sandbox" would present similar practical obstacles and also would likely have a chilling effect on consumers who wish to avoid government scrutiny. Instead of pursuing a technological solution that will quickly become obsolete, Disney suggests that selective, targeted enforcement of existing laws coupled with cooperation with industry would prove a more effective means for improving privacy protections for consumers.

Finally, a focus on industry codes of conduct and best practices would be the most effective way to address the challenges of big data and analytics. As the Consultation Paper points out, the notice and consent model may not be adequate to address data protection challenges brought about by the rapid rise in volume and velocity of data processing. A self-regulatory approach strikes the right balance between encouraging beneficial innovation in this area while also encouraging the development of appropriate governance mechanisms to protect consumers without imposing an overly burdensome notice and consent regime. These governance mechanisms should include investment in anonymization and de-identification technologies, as well as common standards for anonymization across industries.

Disney appreciates TRAI's solicitation for comment regarding how best to protect the privacy and security of consumers' data in the delivery of digital content and services and looks forward to further participation with TRAI on these important issues.

Respectfully Submitted,



Anju Jain Kumar
Assistant Regional Counsel
DISNEY BROADCASTING (INDIA) LIMITED

---

1 *For example, a recent poll in the United States found that 74 percent of citizens lack confidence in government's ability to keep their data private and secure. See Accenture Citizen Survey on Cybersecurity conducted by Market Strategy Group (Apr. 10, 2017).*