Our counter-comments are based on the comments submitted by some of the largest TSPs and industry bodies. In order to avoid repetition, we have grouped similar submissions for those comments that have been repeated by more than one of the participants whose comments we analyzed in the consultation process. These counter-comments may be viewed as our submission against similar recommendations made by others that have not been named in this document.

Broadband India Forum[1] has submitted that the potential costs of opting-in to collection and processing of personal information are larger than the potential benefits, and that users lack experience with data-centric services and the benefits they provide until after opting in. They recommend implementing a system of implied consent with a mechanism to opt-out of data collection and processing. An opt-in mechanism is more beneficial for the privacy and security of user data than an opt-out mechanism. A user that wants a product or a service will undertake the efforts of opting in for specifically those compromises on their privacy that are necessary in order to receive that product or service. Opt-in mechanisms prevent collection, storage, use and sharing of data that is not necessary for the provision of a product or a service.

iSPIRT[2] has recommended that TRAI must introduce a clear framework on the applicability of Deep Packet Inspection. They recommend allowing it for network management, QoS and security, but not for advertising or malicious purposes. Deep packet inspection should not be applied for any purpose. Deep Packet Inspection reveals not just metadata, but the actual contents of each packet of data. The data that can be gathered from Deep Packet Inspection includes personal and sensitive personal data of all kinds.[3] This technology is too broad and too dangerous to be employed for any reason whatsoever.

iSPIRT states that data controllers may co-create data with users and recommends that data controllers should be allowed to retain a copy of data generated so. It is not clear what iSPIRT means by co-created data. If it is data creating using the metadata, personal data or sensitive personal data of a user,

1 Broadband India Forum's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/BIF_Telecom_Sector_07112017.pdf. Last accessed on 21 November 2017.
2 iSPIRT's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/iSPIRT%27s_Response_07_11_2017.pdf. Last accessed on 21 November 2017.
3 Digging Deeper Into Deep Packet Inspection (DPI), *Jay Klein*, available at http://spi.unob.cz/papers/2007/2007-06.pdf. Last accessed on 21 November 2017.

then our submission is that this request for an exemption for co-created data is an attempt to claim ownership of data created using data supplied by a user. It is also an attempt to bypass the requirement to delete data when a product or service provider would otherwise be required to delete data. Any such co-created data, if it is based on metadata, personal data or sensitive personal data of a user, should not be allowed to be retained by a data controller after a user revokes their consent, requests deletion of data or after the completion of the purpose for collection of data.

Some of the comments recommend some form of self-certification or self-regulation in concert with or in place of data privacy and protection obligations. DSCI,[4] for example, recommends self-certification of privacy policy and practices. IAMAI[5] recommends self-developed privacy programs and self-regulation. USISPF[6] recommends a self regulatory approach backed by co regulation, seals and certifications where necessary. Self-certification and self-regulation are insufficient as a means to protect personal data. The Advertising Standards Council of India publishes a set of principles and guidelines[7] for advertisers. These guidelines are toothless because advertisers are expected to self-regulate without a proper enforcement mechanism. Any self-certification or self-regulation mechanism must be accompanied by a strong data privacy and protection law containing a set of principles to be followed, an audit mechanism for verification of adherence to the principles, and an enforcement mechanism to punish violation of the principles.

ACT,[8] in its submission, asks TRAI to refrain from following FCC's rules and the EU GDPR as ACT believes that they unduly impose compliance obligations without a corresponding benefit to the public and/or are technically infeasible. ACT wants TSPs to be able to freely share data with application developers. ACT believes that these rules are unnecessary and create excessive burdens. ACT has asked TRAI to act only on proven consumer harms and not hypotheticals or academic theories. Since the right to privacy has been recognized as a fundamental right by the Supreme Court of India in the case

4 DSCI's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/DSCI_07_11_2017_0.pdf. Last accessed on 21 November 2017.
5 IAMAI's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/IAMAI_07112017.pdf. Last accessed on 21 November 2017.
6 U.S. India Strategic Partnership Forum (USISPF)'s comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/USISPF__07_11_2017.pdf. Last accessed on 21 November 2017.
7 https://www.ascionline.org/index.php/principles-guidelines.html
8 ACT's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/ACT_App_Assn_07112017_0.pdf. Last accessed on 21 November 2017.

of K.S. Puttaswamy v. Union of India[9], the protection of privacy is a duty of the government. The mere violation of privacy should be actionable without the need to prove other harms that stem from such a violation. The need to prove other harms would be an excessive burden on people. Protection of a fundamental right is more important than promoting the development of an app or a service through unchecked violations of the fundamental right to privacy.

ACT speaks against extra territorial jurisdiction of GDPR as ACT believes that it applies to companies that have no connection to the EU. This position is entirely incorrect as the purpose of GDPR is the protection of the people in Europe from whom the data is taken or on whose data the processing takes place. This is an entirely reasonable step to take to protect the data of the residents of Europe. India should follow in the footsteps of GDPR to protect the data and rights of Indians.

ACT also recommends a blanket exemption for small businesses from India's data privacy and protection requirements due to the cost of compliance. While small businesses may be exempted from a requirement to have a data protection officer along the lines of GDPR, it would be imprudent to exempt them from all data privacy and protection requirements. The privacy and security risks faced by data are not impacted in the slightest by the scale of data controllers or processors involved. As data protection laws are meant above all else to safeguard user data, exempting small businesses from their purview would put the data of Indians at risk of collection, storage, processing and sharing without the need to follow notice, informed and meaningful consent, collection limitation, purpose limitation, deletion of data after purpose completion or revocation of consent and other principles that form a bedrock of privacy protection, and would also invariably create gaps in data security measures that would further endanger user privacy. Any such exemption would undermine the very existence of any attempt to protect user privacy.

Some of the participants in the consultation process have asked for exceptions for collection, use or transfer of anonymized or aggregated data. Vodafone[10] recommends exceptions for metadata,

9 W.P.(C) 494/2012

10 Vodafone's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/Vodafone__07_11_2017.pdf. Last accessed on 21 November 2017.

anonymized data, and personal and sensitive personal data if the data does not identify a user. ISPAI,[11] COAI,[12] iSPIRT, Bharti Airtel Limited,[13] Reliance Jio Infocomm Limited[14] and Reliance Communications Limited[15] are some of participants that have asked for an exception for anonymized data. The principle of notice should be followed, and informed and meaningful consent should be taken before collecting, using or sharing any personal or sensitive personal data without any exceptions. Other privacy principles such as collection limitation and purpose limitation also cannot be ignored for metadata, anonymized data and aggregated data. There is no way to completely anonymize a data set. Multiple data sets can often be combined to identify a user when the same data by itself would have been insufficient to identify the user. Metadata often contains identifying information that can lead to revealing a user's identity and behaviour patterns even if at first glance it appears to be innocent data free from any identity information. Any exceptions for the use of anonymized or aggregated data, such as use for law enforcement purposes, must be narrowly defined with sufficient safeguards to prevent abuse of the safeguards.

Vodafone has asked for a removal of the privacy requirements in licensing agreements, and has recommended that only the requirements under the Information Technology Act, 2000 and its Rules, or a new privacy, security and data protection law, should be applicable to telecom providers. Removing the requirements under licensing agreements before India has a strong data protection law would be premature and would result in tangible harms for consumers. Telecommunications is a modern day utility; it is an essential and core part of modern life. Telecom providers have the unique position of gathering personal data, such as location data from cell towers, that users cannot opt out of by simply removing an app or disabling a permission from their device. As such, it is paramount to protect the data gathered by telecom providers. Privacy requirements under licensing agreements should not be

11 Internet Service Providers Association of India (ISPAI)'s comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/ISPAI_07_11_2017.pdf. Last accessed on 21 November 2017.
12 Cellular Operators Association of India (COAI)'s comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/COAI_07_11_2017.pdf. Last accessed on 21 November 2017.
13 Bharti Airtel Limited's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/Airtel_07112017_0.pdf. Last accessed on 21 November 2017.
14 Reliance Jio Infocomm Limited's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/Airtel_07112017_0.pdf. Last accessed on 21 November 2017.
15 Reliance Communication Limited's comments on the Consultation Paper, available at http://trai.gov.in/sites/default/files/RCOM_07112017.pdf. Last accessed on 21 November 2017.

removed until India has a strong data protection law in place for all data controllers and data processors.

Some of the participants such as Reliance Jio Infocomm Limited and Reliance Communications Limited have stated that TRAI can regulate OTT applications and services to ensure that they obey the same standards of privacy and data protection as the licensed entities. Reliance Communications Limited recommended imposition of penalties on data controllers, similar to TSPs, for any breach of privacy of the user. As mentioned in our own comments, TRAI does not have the power to regulate most data controllers including OTT applications and services. The issue of regulating OTT services and applications has already been dealt with by TRAI in its Consultation Paper on Regulation of OTT Services. TRAI's powers to regulate data controllers are limited to regulation of the telecommunications industry and do not extend to regulation of OTT applications and services. While OTT applications and services do not need to comply with the licensing requirements imposed upon TSPs, they are not entirely unregulated. In addition to the requirements under Information Technology Act, 2000 (mentioned below), OTT applications also have to comply with the Consumer Protection Act, 1986, Payment and Settlement Systems Act, 2007, Indian Copyright Act, 1957, Income Tax Act, 1961, Customs Act, 1962, Central Excise Act, 1944, Foreign Exchange Managements Act, 1999, Prevention of Money Laundering Act, 2002, among others. Like all other data controllers, they have to obey the requirements under The Information Technology (Reasonable security practices for sensitive personal information) Rules, 2011 made under Section 43A read with Section 87(2)(ob) of the Information Technology Act, 2000. As mentioned in our comments, the 2011 Rules formed under Section 43A are insufficient to protect the rights of users as they are limited to sensitive personal data or information only. India requires a data privacy and protection law to regulate collection, use and transfer of personal and sensitive personal data by all players in the digital ecosystem, not just OTT applications and services.

Reliance Communications Limited has recommended that TRAI should be empowered to order blocking of content violating data privacy and protection norms. This is a dangerous route to go down. Blocking any content is a violation of the freedom of speech and expression guaranteed under Article 19 of the Constitution of India. Data blocking should take place in only extreme cases, and only

through lawful court orders after proper examination of the necessity and proportionality of blocking content in view of the harm caused by not blocking the content. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 under Section 69A of the Information Technology Act, 2000 is the only legislative instrument that grants the power to block content in India. TRAI does not have the power to block content and should not be authorized to undertake content blocking on its own.

While Reliance Communications Limited is correct in their assessment that the encryption norms in India are outdated and regressive, their recommended encryption strength is insufficient and outdated. DES 56 bit was developed in 1974 and adopted as a standard in 1977. As of 2001, 56 bit key lengths were considered to be obsolete for security against attacks in the world of encryption.[16] In 2004, the US based National Institute for Standards and Technology (NIST) declared DES obsolete.[17] RFC4772[18] discusses security implications of using DES as of 2006. 3DES 128 bit, recommended by Reliance Communications Limited, does not exist. The actual standard is 3DES 168 bit, which has an effective security of 112 bits.[19] 256 bit key length should be the bare minimum standard of encryption for any semblance of security of data and communications today. There should be no maximum limit on the encryption strength in use because computers evolve faster than laws, as a result of which any upper limit on the strength of encryption would only serve as an eventual return to the current state of insecure communications due to an easily breakable encryption.

Reliance Communications Limited has also recommended mandatorily depositing encryption keys with the CMS (Central Monitoring System) deployed by the government to facilitate real time monitoring by LEA's. There should be no requirement to deposit encryption keys, and there should be no requirement to introduce backdoors in an encrypted product or service. A requirement to deposit encryption keys or to provide backdoors in the security of a product would weaken the security and

16 The Day DES Died, *Paul Van De Zande*, available at https://www.sans.org/reading-room/whitepapers/vpns/day-des-died-722. Last accessed on 20 November 2017.
17 Federal Register, July 26, 2004, 69(142), 44509-44510, available at https://www.gpo.gov/fdsys/pkg/FR-2004-07-26/html/04-16894.htm. Last accessed on 21 November 2017.
18 Available at https://www.rfc-editor.org/rfc/rfc4772.txt
19 Barker, Elaine (January 2016). "NIST Special Publication 800-57: Recommendation for Key Management Part 1: General" (4 ed.). NIST, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf. Last accessed on 21 November 2017.

reliability of the entire internet infrastructure. It would (1) hamper innovation; (2) prevent service providers based in other countries from providing their services to residents of India as depositing their keys with Indian authorities would weaken the security of their product or service for residents of other countries, making it harder for them to justify the privacy and security of their products or services if they offered their product or service in India; and (3) stifle the growth of Indian products and services as they would be unable to find a market outside India due to a trust-deficit in their privacy and security. A hands-off approach should be taken for encryption, with only a minimum defined encryption strength and no maximum encryption strength in order to promote innovation and protect privacy and security of all stakeholders in the digital ecosystem.

Some of the comments submitted to TRAI, such as those submitted by Reliance Communications Limited, ask for data localization – storing personal and sensitive personal data within the geographical boundary of India. While it is important to protect sensitive personal data with higher standards than personal data, a requirement to store all personal data within the geographical boundary of India would prove counter productive. Localization requirements impose an excessive financial burden on product and service providers to install a server in each country that requires data localization. If all countries introduce laws requiring data localization, innovation would be effectively killed as start-ups and small data controllers would be required to undertake the financial burden of installing and maintaining a server in each country of the world. The need of the hour is not to have data localization, but to protect personal and sensitive personal data no matter where it is located. This can be achieved by making laws that meet the privacy and security standards being followed in the laws of other countries so that free flow of data is allowed to India from those countries, and requiring a similar level of protection for privacy and data security in other countries before allowing data transfer to another country. Ensuring that data is transferred to only those countries that protect the data of Indians would allow innovation to take place while protecting the privacy and security of Indians without creating any additional burden on product or service providers.