June 11, 2018
To,

1. Shri R.S. Sharma
   Chairman
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

2. Shri SK Gupta
   Secretary
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

3. Shri Asit Kadayan
   Advisor (QoS)
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

Re: Response to Draft Telecom Commercial Communications Customer Preference Regulations, 2018

About us

Koan Advisory Group is a New Delhi based policy advisory firm, which combines thorough domain knowledge across multiple technology oriented sectors with continuous engagement of decision makers in industry and government. We have previously engaged with various regulatory arms, including TRAI on issues related to telecommunications such as consumer privacy and net neutrality, and future policy making.

Submission

We laud this initiative of the TRAI to onboard public comments to address the issue of unsolicited commercial communications, or spam. We note the forward-looking nature of the Draft Telecom Commercial Communications Customer Preference Regulations, 2018 ("Draft Regulations") congratulate the TRAI for conceptualizing the technology-based co-regulatory framework for addressing the issue of UCC in India.

Indeed, the issue of UCC is a multi-faceted one, requiring the active engagement of telemarketing agencies, telecom service providers and business entities, and corresponding regulatory arms of the government. Specifically, the Draft Regulations have been framed keeping in mind the role of telecom service providers in curbing the issue of unregistered telemarketers and the need for registering user consent and preferences in the telecommunication sector. However, it is important to note here that the regulatory response to the issue recognize the intrinsic nature of consumer data and underpin responses in a technologically neutral manner. Regulatory responses to the question around the world

have therefore enacted comprehensive regulations in this regard, often based in the definition of the scope of user consent to providing data and receiving marketing and promotion information.
An overview of some best practices in this regard has been tabulated below:

Country	**Relevant Legislation and Provisions**	**Summary of provision**
Estonia	Electronic Communications Act: Sections 102, 103, 103 (1), 107	For any exchange of information, a prior consent needs to be acquired from the consumer. The Act also specifically refrains from according preference to any specific technology.
United States of America	Telemarketing Sales Rules: *The Requirement that Pre-recorded Telemarketing Messages Include an Automated Interactive Opt-Out Mechanism*	The opt-out mechanism must: • be available for call-recipients to use at any time during the message; • when invoked, automatically add the call recipient's number to the seller's entity-specific Do Not Call list; and • after the call recipient's number has been added to the seller's internal Do Not Call list, immediately disconnect the call. By contrast, if it's possible that a prerecorded telemarketing call may be picked up by an answering machine or voice mail service, the message must disclose at the outset a toll-free number that, when called, connects the caller directly to the same type of voice-or-keypress-activated interactive opt-out mechanism that will add the number called to the seller's Do Not Call list. The opt-out mechanism provided must: • be accessible at any time throughout the telemarketing campaign, including non-business hours; • automatically add the call recipient's number to the seller's entity-specific Do Not Call list; and • Immediately thereafter disconnect the call.
United Kingdom	The Privacy and Electronic Communications (EC Directive) Regulations 2003	User consent must be taken at the time of collection of consumer details as to whether they'd like to receive promotional messages, and if their information can be shared with other organisations. Users must consent to being contacted via fax, phone, post or email and be given a chance to object. **Email marketing and text messages** Marketing emails to individual customers can only be sent if they have permitted the same. Emails or text messages must clearly indicate: • the identity of the caller • that you're selling something • what the promotions are, and any conditions

Australia	Spam Act and the Privacy Act: 16, 17, 18, 19	Prior consent is required, and accurate sender information is required to be provided. They must also contain an unsubscribe facility.
Singapore	*Do Not Call ("DNC") Provisions* in Part IX of the *Provisions Personal Data Protection Act 2012* and *Spam Control Act ("SCA")*	A Do Not Call Registry (DNCR) is set up and operated under the Personal Data Protection Commission (PDPC) for individuals to register telephone numbers and organisations to check and ensure they do not send marketing messages to telephone numbers registered in the DNCR. **Currently, the Singapore PDPC is undertaking a consultation process on the review of the DNC provisions under the PDPA and the SCA to enable holistic application across technologies.**

Comparably, the Draft Regulations remain limited to services such as calls and SMSs sent over the telecom network, and fail to address the problem in a comprehensive manner. Here, it will be necessary to engage the relevant government authorities such as the Ministry of Electronics and Information Technology (MeitY), which has already initiated the process of reviewing the extant laws on data protection in India. Notably, the TRAI's *Consultation on Privacy, Security and Ownership of Data in the Telecom Sector* should further enable a robust understanding of the issue in the telecom sector specifically, and should feed into a comprehensive legislative process.

The following additional comments are made for your consideration:

LEGISLATIVE CHALLENGES

Regulation 34 falls outside TRAI's jurisdictional mandate

TRAI will need to address the jurisdictional challenges that abound with respect to Regulation 34. The Draft Regulations have been framed under Section 36 read with Sections 11 (1)(b)(v) and 11(1)(c). Specifically, sub-clause (v) provides TRAI the authority to frame regulations regarding the standards of quality of service, and clause (c) deals with regulations on levying of fees and rates for services covered under the TRAI's jurisdiction. Both these provisions specifically refer to telecommunication services, which do not cover devices and operating systems.

While the Draft Regulations on the whole deal with improving quality of service and safeguarding consumer interest vis-à-vis telecommunication services, Regulation 34, owing to its extension over device manufacturers falls outside the scope of these provisions. Even though the obligations envisioned under Regulation 34 apply to licensed telecom service providers, the implementation results in the creation of regulatory consequences for device manufacturers and operating systems as well. As has been held by the Delhi High Court, "*the power to issue regulations cannot be used to subvert the provisions of the said Act and to assume powers and functions not conferred by the said Act" (MTNL v. TRAI* AIR 2000 Delhi 208). It should be pertinent to note here that the TRAI, in its consultation process regarding *Privacy, Security and Ownership of Data in the Telecom Sector* has recognized the lack of

jurisdiction over devices and browsers. It is therefore necessary in the interests of regulatory certainty and coherence in the sector to ensure strict adherence to the jurisdictional scope prescribed and maintained by the TRAI previously.

The jurisdiction over devices and operating system in fact lies with the Ministry of Electronics and Information Technology (MeitY) as per the Allocation of Business Rules, 1961. At the same time, the Telecommunication Engineering Centre (TEC) under the Department of Telecommunications (DoT) is tasked with developing standards for the sector.

Regulation 34 is overbroad and fails the three-part test

Regardless of jurisdictional challenges, the Regulation also suffers from being vague and overbroad.

The device manufacturers' ability to re-configure App permissions has a direct bearing on the consumers' right to privacy. Here, any Regulation that restricts the same will have to adhere to the three-part test prescribed under the *KS Puttaswamy* judgment. Under the three-part test, for a restriction on a recognized fundamental right to be reasonable, it needs to be prescribed by law, and be necessary and proportionate. As per the current draft, the precise scope of permissions that will be sought by the Apps referred to has not been defined. As such, the scope of non-conformity with the Draft Regulations remains unclear.

Furthermore, given the framing of Regulation 34, the Regulator will need to clarify its application to phones that do not support third party app functionality. For instance, feature phones do not carry the functionality to host apps that are installed as per the user's discretion. This needs to be contextualized within the composition of the cellular mobile market: while India currently has over 300 million smart-phone users, the total number of wireless subscribers in India is 1,167 million.

INFORMATION SECURITY AND PRIVACY CONSIDERATIONS

Respecting security and privacy by design

Information security and privacy scholars have recognized the importance of technological solutions such as security and privacy by design, such that data handlers are encouraged to create applications whereby the design is privacy and security respecting from in its inception. This has been further recognized by the EU GDPR under Article 25, mandating entities to *"implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed*". In India, the MeitY Committee of Experts under the Chairmanship of Justice BN Srikrishna has also recognized the importance of security and privacy by design principles, wherein data minimization has been identified as a key principle of a future data protection framework. Privacy by design has also been acknowledged as a relevant principle by TRAI in its Consultation on Consultation on Security, Privacy and Ownership of Data in the Telecom Sector.

In this regard, it is necessary for the TRAI to develop Apps requiring permissions that respect the design principles of devices and operating systems, so that such technological measures are not defeated by vaguely framed Regulations. In this regard, it is important to recognize that operating systems on smart-phones are configured variably wherein operating system permissions may restrict access to information such as call logs and user information. For instance, the system design for ensuring device security often restricts the data that third-party trusted applications may access, and instead create secure enclaves within the device that store specific types of data only locally on the device.