S.No.	Document Clause/Reference	Question/Comment
1	Consent Registry	In case of Mobile Number Portability and Reissue of same Mobile number to a new customer: - How will the consumer preference and consent registered in DLT be applicable? - How will Access provider provide such information as the Consumer in such cases may not be forthcoming in providing information or validating the same Access provider should have tht provision to deactivate the consumer preference or consent and bypass the user authentication requirement. alternatively: consumer should validate the preference once in a given period to make it continue. In the absense of the same, the consumer preference should get deleted/inactive
2	COMMUNICATIONS CUSTOMER PREFERENCE REGULATION – Page 4	More insight on Pre-checks and post-checks? It needs to be clearly highlight the pre-checks and post checks done by Access Providers. In an event the message is sent to an Access Provider and it is Off-net i.e. meant for another TAP. In this case what all checks will be done by TAP and OAP. This is critical to avoid duplication of work and also increased latency
3	OBLIGATIONS OF ACCESS PROVIDERS – Page 16	Immediate actions to be taken in case of non-compliance. What all actions need to be taken and how to we measure compliance. The compliance cannot be at the descition of Access Providers, bacuase in case of pre-checks and post checks, the complaince standardization will define on messaging success, without duplication of work. TRAI should prescribe actual conditions of compliance check.
4	Verification of Consumer Identity	Other than OTP verification, what all methods are prescribed by TRAI to verify consumer identity. Is TRAI looking at a private key for each consumer for verification of consent.
5	Chapter V, Clause 13 - page 17	DLT Network Operators - we need a definition of DLT network operator
6	Chapter V, Clause 16 - page 17	TRAI should prescibe a common minimum Code(s) of Practice for compliance. System changes based on different COPs would lead to separate systems and may threaten uniformity of system. TRAI should after taking input from all Access Providers, prescibe its own set of COPs.
7	Chapter V, Clause 35 - page 28	By defining the charges between OAP and TAP. It seems that the Cost of new system envisaged has to be borne by the OAP. In this case what all checks need to be defined by the TAP? If each Access provider has its own DLT then how will OAP perform checks on behalf of TAP. if TAP has to perform all the checks independently, that means TAP has to take our costs of program from 5 paisa charge. OAP in this case gets charge of operator lookup and passing on message. TRAI needs to seperately define charge for TCCP activities and define allocation of charge to TAP or OAP
8	Schedule 1 Point 4 (1) - C	Headers assigned to business entities should not be bound to a mobilenumber of a device. Large business entities may have a team to do the changes, binding it to one device or mobile number may not work. Portal access with login credentials is a better choice. Mobile numbers can be used for OTP, along with email OTPs.
9	Schedule 1 Point 4 (2) - b	The content of the message may change as many times as possible, while taking consent, we should only take consent on the intent of messages (promotion, etc.). Entire content cannot be shown to customer for consent as the content can change very often, specially for promotion messages.
10	Schedule 1 Point 4 (3) - d	The Access provider should de-register template or can temporarily suspend the use of template. This subjectivity or descrition can lead to dispute between Sender and Access Provider. In an event of dispute, what will be the dispute resolution mechanism?

11	Schedule 1 Point 6 (2) - c,d	The verification of time band and day band can be done at the scrubbing level, how will this information be communicated to Sender. The consumer may change its preference a number of times without informing the sender. The sender will continue to send the messages on non preferred time and day, the scrubbing service provider will continue to block it. this may not change unless the information is communicated back to sender, else this hit and trial method will take a large chunk of service load. how do we communicate to sender (both current and potential), abour consumer preference of day and time? and ensure sender is acting based on the information
12	Chapter I, Clause bq, Page 11	"provided such a message is sent within 30 minutes of the transaction being performed…" 1) What is the rationale for the 30 minute window for the triggered Transactional Message ? Consider the Retail delivery notifications about ETA of goods that improve customer experience and are delivered periodically until immediately after the goods are delivered. Are these then better categorized as Service messages? 2) How is this requirement to be validated ? Transaction times are not known to the RTMs or APs and therefore they will not be in a position to validate compliance to this rule
13	Chapter IV, Clause 7, Page 14	"no delivery of commercial communication is made or blocked in contravention to the subscribers' preference after twenty-four hours or such time as the Authority may prescribe" If subscribers preferences are allowed to be changed at a frequency of more than once a day (as is expected in current times by App users), there is a possibility of conflicting preferences within a 24 hour period that then leads to contravention of the subscriber preference depending on which preference is applied by the Scrubber. What is the tolerance in deviation from the precise preference allowed in this scenario? What is the maximum time allowed for implementation of changes to subscriber's preferences?
14	Chapter V, Clause 12.2, Page 16	Are post-checks to be applied to every message or Voice call? Can Auditability of data alone be adequate replacement for a post-check?
15	Chapter V, Clause 12.5, Page 16	Please provide specifics of security compliance. What Industry standards or Regulatory requirements would be relevant?
16	Chapter V, Clause 13.2, Page 17	Please clarify intent and nature of smart contracts in this case. Are cases of lapse of consent subsequent to subscriber preference updates, PE de-registration etc. in consideration
17	Chapter V, Clause 24.3, Page 20	This requires complaint history to be maintained for 3 years and yet maintain it as immutable. Can this be implemented in non-DLT solutions?
18	Chapter V, Clause 25.5, Page 22	In a DLT environment, coordination of SMS messages to restrict outbound messages to 20 in day may be technically restrictive and lead to economically unviable solutions. Is there room to relax the constraints?