Response to TRAI's Consultation Paper on
Review of Telecom Consumers Protection Regulations (TCPR), 2012

Date: Aug 7, 2024

To,
Shri Amit Sharma,
Advisor (F&EA),
Telecom Regulatory Authority of India
Tower-F, NBCC World Trade Center, Nauroji Nagar,
New Delhi 110029
Email: advfea1@trai.gov.in

Dear Sir/Madam,

With reference to your Consultation Paper on Review of Telecom Consumers Protection Regulations (TCPR), 2012, dated July 26, 2024, I respectfully offer the following response for your kind consideration.

With best regards,

Parag Palsapure
Navi Mumbai, India
pparag@yahoo.com / +91-9322662040

Question 2: Is there a need for separate plans for Voice & SMS and data to meet the specific requirements of subscribers. Please justify with reasons.

Response to Q2:

Telecom subscribers should have the freedom to choose and subscribe to specific services such as Voice, SMS, or Data, without being compelled to purchase bundled or additional services they do not need, or cannot deactivate.

The reasons for providing such choice can be,

(1) For potential cost savings
(2) Extend battery life (data services often drain battery very fast)
(3) Freedom of choice, not to be disturbed by spammers
and MOST IMPORTANTLY
(4) To protect against PRIVACY BREACHES and DATA COMPROMISES caused by apps with questionable credentials and potential software vulnerabilities

While TRAI has already acknowledged the potential cost savings, I take this opportunity to highlight the concerns about privacy and data security.

a. It is a known fact that most mobile handsets come with a host of pre-installed applications, of which many are hidden and not removable by ordinary users.

b. Some pre-installed applications or software components may have questionable functionality, vulnerabilities and potential backdoors, which can be exploited by any hacker connected to the Internet.

c. Some apps run in the background, are capable to upload/backup/steal private data without user knowledge or consent, push software updates/upgrades and even initiate or authorise undesirable financial and non-financial transactions. Many of these can pose serious threats, including to national security. Some examples are provided below:

    a. Access to SMS for OTPs: Many applications can read incoming SMS messages without explicit user consent, enabling potential fraudulent financial activities. Even widely used apps like WhatsApp and Signal are known to access SMS content immediately upon installation, bypassing necessary user permissions. Furthermore, certain applications initiate verifications (e.g. email IDs, phone number, penny financial transactions etc) via SMS messages without user authorization. Unauthorized access and misuse of OTPs for Aadhar authentication, financial and non-financial transactions are real and pose significant risks.

    b. The risks of automatic updates app downloads are real. Recent global disruptions caused by the CloudStrike client update on Microsoft Windows OS highlight the potential for unforeseen consequences, including widespread outages in critical sectors like aviation, finance, and healthcare, resulting in billions of dollars in losses. Untested or unwanted software updates can render devices inoperable for extended periods or permanently. I have personally experienced this on my devices, where forced updates resulted in unauthorized installation of multiple apps, some introduced new vulnerabilities and a bug that rebooted my device on every network transition.

    c. Photo Gallery / Cloud Drive sync: Smartphone users often capture photos of important or confidential documents such as Aadhar cards, PAN cards, Driving Licenses, Debit cards, Medical or Business critical documents. Default settings on phone enable the apps on phone to access, process and upload documents and data to the cloud-based servers, often under the garb of automated backup. Such photos and documents are automatically analysed, classified, content indexed and made searchable. Collected confidential user data can be potentially misused or available to hackers on the dark-web. It may be noted that unauthorised uploading/storing/processing/sharing of certain confidential documents could be punishable offence under various laws.

    d. Unrestricted access to photos and live camera feeds by applications poses significant privacy and security risks. Many apps continuously activate the mobile camera under

the guise of features like “face ID unlock” or “smart lock”, capturing videos or images without user consent or awareness. This can be particularly dangerous for individuals in sensitive roles, as it could expose confidential information or compromise national security, where the smartphones could be uploading visual feeds and location data to enemy servers without user’s knowledge. Additionally, the proliferation of AI tools has made it easy for malicious actors to manipulate captured images and videos to create deepfakes for blackmail or other harmful purposes.

e. Voice samples, recordings, and live microphone access too raise concerns about privacy and surveillance. While voice assistants like Alexa, Google, and Siri rely on continuous audio monitoring, it's essential to control when voice data is collected and transmitted. As outlined above, indiscriminate collection of voice samples (e.g. banks, offices of security forces, R&D etc) can lead to significant risks, including privacy breaches and unauthorized use and potential compromise of national security.

f. Unauthorized access to Phone book. There have been instances of subscribers being driven to suicide after being blackmailed with manipulated photos and deepfakes distributed to their contacts, mainly by unauthorized money lenders (Digital Loans) through their associated apps. Additionally, phonebook contacts are frequently subjected to harassment through spam and other unwanted communications. Even common messaging and calendar applications upload user contacts and send out spam as they sell the data to their ‘business accounts’.

g. Live location / tracking data and location history can also be used for improving navigation services (often done without user’s knowledge and without providing compensation to the user) however, the same capabilities can also be used for malicious or criminal purposes.

h. Access NFC sensor and authorize financial transactions or data transfer when in vicinity of another capable device.

i. Modify device settings, or give unwanted permissions to apps, or taking control of the device remotely. After every OS upgrade/update, such changes in permissions are noticed on most mobile devices.

j. Frequently pushing annoying spammy notifications and advertisements by hidden apps in skins/customized OS on mobiles. Some mobile apps download and force install new apps on the mobile devices, at the mobile subscriber’s costs and risks.

k. Mining cryptocurrency or unauthorised use of mobile device’s computing powers.

l. Launching Distributed Denial of Service (DDoS) security attacks through mobile phones. DDoS attacks can bring down targeted telecom networks, financial/payment systems, e-governance systems, corporate systems and raise risk of severely impacting economy of our country.

m. Take complete control of the devices or potentially “brick” them, either individually or on massive scale during e-warfare or as part of DDOS strategy.

n. Backdoor entry on corporate / secured networks: Mobile device can provide direct backdoor entry to corporate networks which often typically use multiple levels of firewalls, security appliances and software layers to connect to the public Internet. Data-service blocked phones in sensitive offices can help mitigate certain risks.

d. Isolating mobile devices from the internet can enhance security by preventing unauthorized data transfers, remote transaction approvals, or exploitation of vulnerabilities by hackers. Most smartphones provide “settings” where mobile data can be disabled. However, many apps disregard user settings and automatically reactivate mobile data, undermining these security measures.

e. Many subscribers may have fixed broadband connections at the home or workplace, or another subscription from another provider. In such cases, the subscriber may not want data service from the mobile telecom service providers and must have an option to choose the “best provider” for each of the service, without paying excessive charges for all services from all providers.

f. It is therefore highly desirable to have subscription plans that provides mobile data as optional with mobile subscription i.e.

    a. Pure Voice and SMS subscription plans for subscribers who do not want to stay isolated from mobile internet due to privacy and security concerns or for economic reasons
    b. Ability for subscriber to disable/enable data service on the subscription plan, through the telecom service provider’s portal.

If the mobile device is not connected to the Internet on 24x7 basis (no data plan or wi-fi connectivity), many risks mentioned above can be mitigated.

Therefore, as a citizen of India and a telecom subscriber, I urge the TRAI to ensure all telecom service providers provide a choice of tariff plans, where a subscriber can

1. Choose pure Voice+SMS plan,
2. Choose Voice+SMS+Data plan, with a provision to disable / enable Data services on V+S+D plans through portal/helpline
3. Choose SMS+Data plan

TRAI is aware that CNAP (Calling Name Presentation) service is still not available in India and that there is no respite from phishers and spam callers.

To mitigate this problem, I humbly propose that telecom operators implement hourly, daily, and weekly limits on outbound calls for all new and ported connections. Additionally, an automated

verification system should be introduced to detect and deter IVR/robocall abuse through random call backs to subscribers after a specified number of outbound calls made within a short time.

I thank TRAI for making progressive moves to protect the interest of consumers, telecom operators and the national security.

Jai Hind