Managing Unsolicited Communication Leveraging STIR/SHAKEN and Blockchain

Tech Mahindra and IBM POV

Table of Contents

Introduction 3

STIR/SHAKEN Framework 3

Secured Telephony Identity Revisited (STIR) 3

Signature-based Handling of Asserted information using toKENs (SHAKEN) 4

How do STIR/SHAKEN work in a telecom network? 4

Limitations of STIR/SHAKEN Framework 5

How is India resolving the Great '1 Bn Subscriber Problem" by adopting Blockchain? 5

Benefits of DLT UCC Solution 6

Architecture for implementation of UCC ecosystem based on DLT 6

Ledgers for DLT UCC Solution 7

Performance of the DLT UCC Solution 8

Platform To Curb RoboCalls and Caller ID Spoofing for US Operators: 8

A Use Case for Integration of DLT UCC Solution with the STIR/SHAKEN framework 8

Call flow with integrated STIR/SHAKEN and DLT UCC Solution 9

Why the IBM Blockchain Platform for the DLT? 10

Conclusion 10

Connected World. Connected Solutions.

Introduction

The Federal Trade Commission (FTC) is a bipartisan federal agency with a dual mission to protect consumers and promote competition. Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states. The District of Columbia and US territories regularly cite “unwanted and illegal robocalls" as their top complaint category. The FTC got more than 1.9 million complaints filed in the first five months of 2017 and around 5.3 million in 2016. The FCC has stated that it gets more than 200,000 complaints about unwanted telemarketing calls each year. The consumers are increasingly the targets of unsolicited and often fraudulent robocalls, which are enabled by caller ID spoofing. Unfortunately, many robocalls originate from outside the United States. It could be challenging to track down the callers behind these international calls.

To this end, the Chairman of the FCC proposed a Notice of Inquiry (NOI) to seek comment on call authentication frameworks to free consumers from many of these unwanted and often fraudulent calls.

To address unwanted and illegal robocalls, ATIS (Alliance for Telecommunications and Industry Solution) and the SIP (Session Initiation Protocol) Forum worked together to develop standards that verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network using the Session Initiation Protocol (SIP). The ATIS and SIP Forum work involves a multi-phased approach to solve the issue of caller identification, using a digital certificate to verify, authenticate caller identification for calls carried over an Internet Protocol (IP) network, called the STIR/SHAKEN Framework.

In India, the TRAI (Telecom Regulatory Authority of India) has decided to address the unwanted commercial communication to consumers using the Distributed Ledger Technology. As per TRAI, 2 million complaints were filed till 2018, even after disconnection of 1.4 million numbers and blacklisting of 0.46 million numbers. The key telecom operators in India have implemented this solution.

A combination of STIR/SHAKEN with the DLT solution in India will address the issue of both illegal and legal unwanted calls for the end consumers.

STIR/SHAKEN Framework

Secured Telephony Identity Revisited (STIR)

STIR is the framework that guarantees no spoofing of a telephone number along the way. This electronically validates phone calls as they make transfer through the many networks needed to complete the call. This allows a telecom firm to verify that an incoming call is coming from a listed source.

STIR defines a digital signature to verify the calling number, and specifies how it will be transported in SIP." STIR's framework includes a certificate model to create credentials based on an X.509 credential system. These credentials are then used by authentication services to confirm the authenticity of SIP calls.

- Protocol for creating a digital signature with calling party info
- Allows signature to be created/verified in various locations

Connected World. Connected Solutions.

Signature-based Handling of Asserted information using toKENs (SHAKEN)

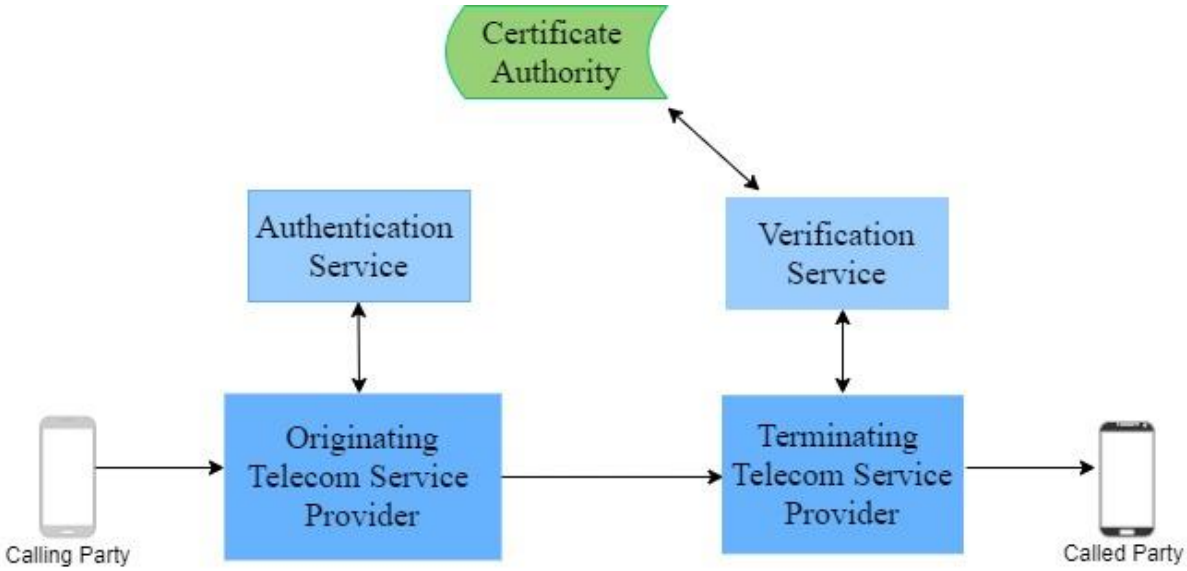
SHAKEN is a framework for managing the deployment of Secure Telephone Identity (STI) technologies to provide end-to-end cryptographic authentication, verification of the telephone identity, and other information in an Internet Protocol (IP)-based service provider voice network.

It is designed to use PASSporT [Personal Assertion Token] as a method of asserting the caller's telephone identity along with the date and destination telephone numbers to avoid replay attacks using valid identity header fields. In addition to the PASSporT claims, "attest the identity being asserted" and "originating id," SHAKEN provides :

1. The ability to provide an attestation indicator for the context of how the call originated.
2. The ability to provide unique originating identifier that can serve as an opaque indication of where in the service provider network the call originated.

How do STIR/SHAKEN work in a telecom network?

Together STIR/SHAKEN creates the framework to ensure every Internet Protocol-based call has a certificate of authenticity attached to it- a digital signature that allows service providers to verify caller ID to mitigate unwanted robocalls and prevents bad actors from using Caller ID spoofing.



- When a customer places a call through a service provider under the STIR/SHAKEN model, the originating service provider contacts the authentication service to get a private key using which it signs the call.
- The originating communication service provider then uses the key to sign the call with the customer's information and authentication service's certificate.
- When the terminating service provider receives the call, it sends the identifying information and the digital certificate to an authentication service.
- The authentication service checks with a certificate repository to ensure that the authentication service is authorized and it has a valid certificate.

Connected World. Connected Solutions.

- It then uses the public key that corresponds uniquely to the sending authentication service's private key to verify the signed call
- Information about whether the call has been verified or if some problem has occurred (e.g., the call did not match asserted caller's identity, it has an expired certificate, information was in improper format) is then sent to the terminating service provider.

Limitations of STIR/SHAKEN Framework

- Communication Type:
  - It is focused only on Robocalls and only works on IP end to end call path
  - It does not restrict the unwanted legitimate calls such as marketing and promotion communication
  - It is limited to voice calls and does not cater to text messages

- Caller Identification: It can only identify if the call was not spoofed
- Content Validation: It does not authenticate the content of the call
- It may not consider the Do Not Call or Do Not Disturb preference/consent of the end customer

How is India resolving the Great '1 Bn Subscriber Problem" by adopting Blockchain?

UCC or spam calls have become a major nuisance to telecom subscribers in India, and the Telecom Regulatory Authority of India (TRAI) had been working with stakeholders to curb this menace. In July 2018, TRAI had mandated all telcos in India to use Distributed Ledger Technology to resolve this.

Tech Mahindra developed a DLT based solution to help telcos address the regulatory and compliance requirements, following TRAI recommendations. With our expertise in Blockchain & telecom experience, we designed DLT solution that comprises of various levers, block studio, block engage, block talks, block geeks, block accelerate, block access & block value. This is aimed at creating industry-leading applications that are architected on innovation and human excellence to unlock significant value for all stakeholders.

DLT based solution was recommended to improve the regulation and delivery of commercial communications fundamentally. The TRAI UCC Regulation put down guidelines for all players (Telecom Operators, Tele-marketers, Service providers, and Business Entities) in the ecosystem as listed below:

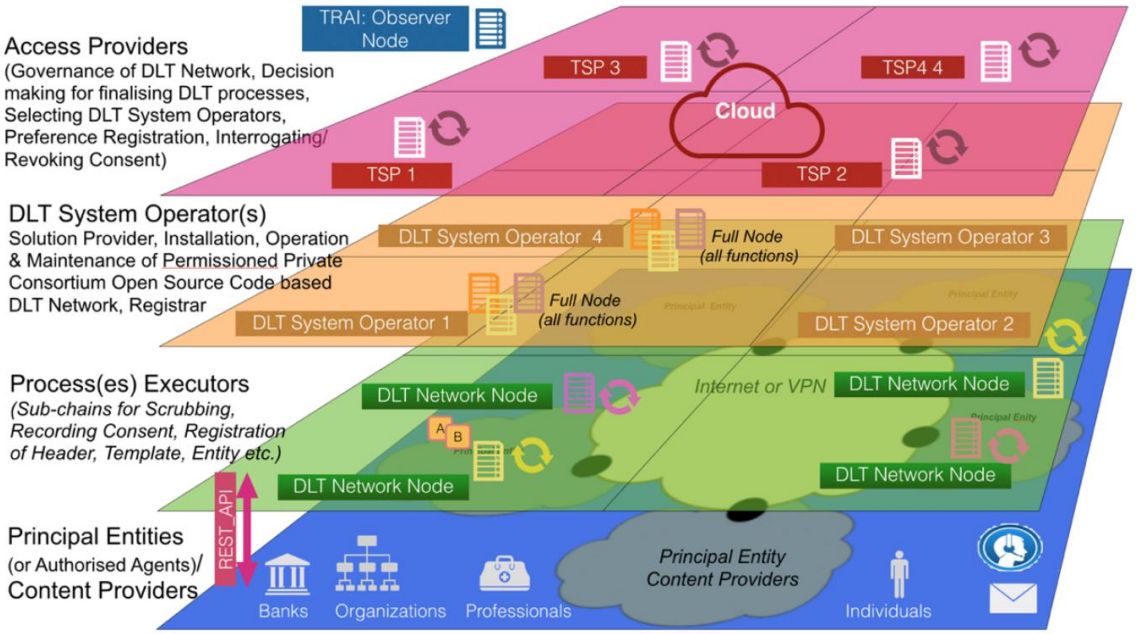
1. Provide a way for consumers to record preferences, consents, revocation of consents, and complaints.
2. Share consumer's complete and accurate preferences/consent.
3. Ensure that all necessary regulatory pre-checks are carried out for sending Commercial Communication.
4. Operate smart contracts among entities for effectively controlling the flow of Commercial Communication.
5. Ensure compliance by the registered sender(s) who have notified the access provider about the use of auto dialer(s), and to take action against the sender(s).
6. Scrubbing As a Service to be offered by Telecom Operators. "Scrubbing" is a way to remove numbers that have registered as part of do not disturb/call.

Connected World. Connected Solutions.

Benefits of DLT UCC Solution

1. Streamlining of processes by making non-repudiable records available to relevant stakeholders, allowing faster automatic resolution of issues, minimize disputes and effective complaint redressal in time bound manner
2. Better control of all the players in the ecosystem and ease of management for the regulator
3. Enhanced consumer experience without compromising their privacy by preventing unwanted calls and text messages from registered Tele-marketers
4. Business entities can perform targeted promotions to the interested consumers, thereby reducing their spend and enhancing their business opportunities
5. Every telemarketer can use infrastructure provided by the network rather than investing in setting up their infrastructure
6. Enforcing technology-driven compliance rather than reactive compliance based on consumer complaints
7. Identify patterns of suspicion and detection of spam across all the telecom operators

Architecture for implementation of UCC ecosystem based on DLT



The different roles and responsibilities performed by key stakeholders in the UCC solution:

1. The Telephone Service Providers Access Providers shall deploy, maintain, and operate a system, by themselves or through delegation, to ensure that requisite functions are performed in a non-repudiable and immutable manner :
    a. Customer Details: to record preference(s), consent(s), revocation of consent(s), complaint(s) etc.

b. Message Delivery: to carry out regulatory pre-checks and post-checks in respect of Commercial Communication being offered for delivery and also to keep records of actions performed;
c. Entity Registration: to register person(s), business entities or legal entities) in making Commercial Communication through its network involved from origination, transmission or delivery and have adequate documentary evidence in support to prove its identity;
d. Entity Functions: to ensure that functions and actions performed by registered entities are identifiable, distinguishable and recordable;
e. Security & Auditability: to ensure that the data is stored and shared securely and safely;
f. Identity & Access Management: to ensure that data is accessible only to the relevant entities for performing roles assigned to them under these regulations;

2. DLT System Operators will build, manage, govern the DLT network for all entities in the UCC ecosystem.
3. Telemarketers, Content Providers, Businesses are the principal entities responsible for commercial communication.

Ledgers for DLT UCC Solution

A Permissioned DLT network would have to be established, operated, and maintained by the Telecom Service Provider. DLT will provide processes of registration of entities like telemarketers, content providers, and identities like SMS headers, Calling line identities for voice calls. The following ledgers will have to be maintained in the DLT:

1. **"Preference Register"** (DL-Preference) keeps records of preference(s) of customers about the category of content, mode(s) of communication, time band(s), type of day(s) along with the details of the customer who has exercised choices of preference(s), day and time such choices or changes in choices were exercised safely and securely.
   Category: Banking/Insurance/Financial Products/Credit Card, Real Estate, Education, Health, Consumer Goods and Automobiles, Communication/Broadcasting/Entertainment/IT, Tourism & Leisure, Food & Beverages
   Mode of Communication: Voice, SMS, Auto-Dialer (with pre-recorded announcement), Auto-Dialer(with connectivity to live agent), Robo-calls
   Time slots and days of the week.

2. **"Entity Register"** (DL-Entities) for having records of all entities registered to carry out telemarketing related functions with all relevant details**.** The entities could be Telemarketers, Service Providers, Business Enterprises.

3. **"Header Register"** (DL-Header) keeps records of the header(s), its purpose of sending commercial communications, and details of the sender to whom it is assigned safely and securely.

4. **"Content Template Register"** keeps records of unique content template identity along with the content of content template and details of sender who got it registered safely and securely.

5. **"Consent Register"** has all relevant details of consent acquired by sender, securely and safely, to send commercial communications and may be required for pre and post checks for regulatory compliance based on the consent.

Connected World. Connected Solutions.

The Telecom Service Provider will have to implement "Scrubbing." This is a process of comparing target list of the telephone number(s) provided by the sender, to whom it wishes to send commercial communication with the list of the telephone number(s) in DL-Preference and DL-Consent to check whether commercial communication(s) can be sent to the Recipient as per his registered preference(s) or as per consent.

Performance of the DLT UCC Solution

Blockchain solution is designed as a combination of on-chain and off-chain components to ensure the required performance and SLA's are met. The performance for UCC is based on several factors which are specific to the Telecom Service Provider:

- No. of Preferences / Consents captured per day.
- No. of Business Entities active on the Telecom Service Provider UCC application simultaneously performing Business Entity functions that require interaction with Blockchain network.
- No. of Telemarketers active on the Telecom Service Provider UCC application simultaneously performing Telemarketer functions that require interaction with Blockchain network.
- Avg. No. of simultaneous scrubbing requests.
- Speed of the bandwidth between the Blockchain nodes.
- Integrations with internal systems (CRM, SMSC Gateway, IMS, etc.) and the network speed.

Scrubbing is the most data-intensive and critical service in UCC and directly affects the business as usual for each Telecom operator. Every text or voice request has to go through scrubbing, and having any delay or additional latency introduced in the current text or voice delivery process is inadmissible, hence Scrubbing as a service is designed off-chain on purpose. This off-chain scrubbing service ensures that there is real-time data replicated from Blockchain in high performance and a highly available database. All activities on the off-chain database and Scrubbing service are recorded on Blockchain for immutable audit trail and transparency.

Registers which are cached off-chain in UCC are as below:

- Preference Register
- Consent Register
- Header Register
- Template Register

Platform To Curb RoboCalls and Caller ID Spoofing for US Operators:

A Use Case for Integration of DLT UCC Solution with the STIR/SHAKEN framework

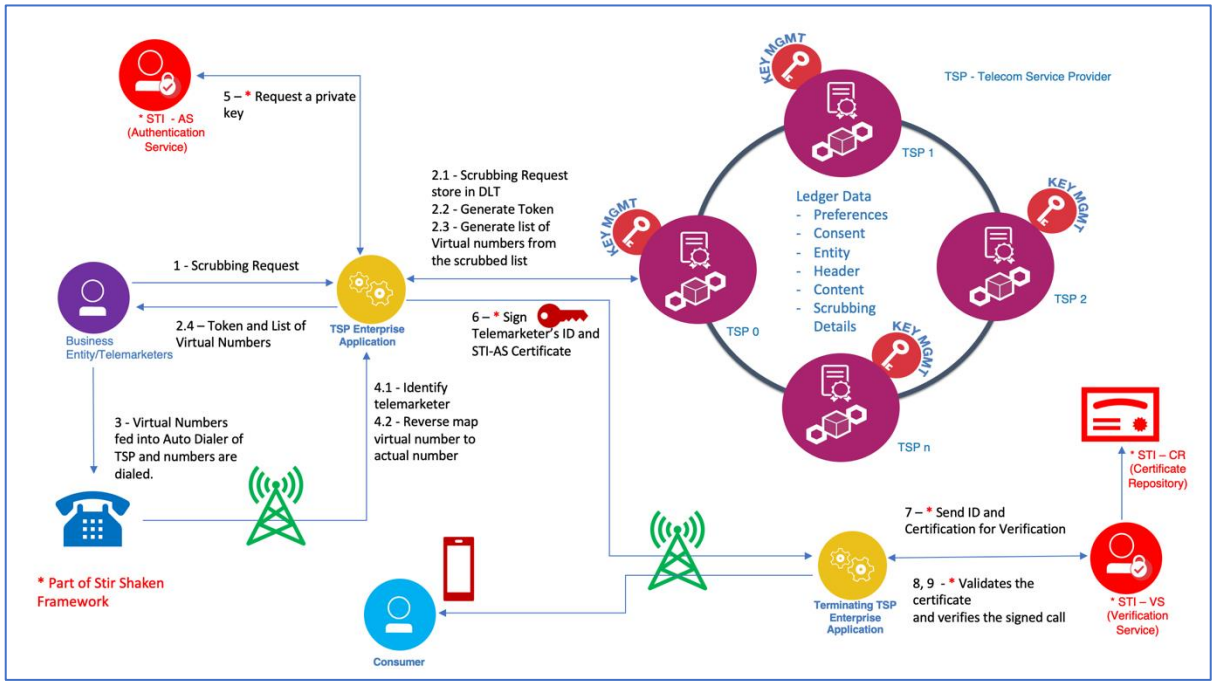
The STIR/SHAKEN provides the framework that allows telecom service providers to verify caller ID to mitigate unwanted robocalls and prevents bad actors from using Caller ID spoofing. The STIR-SHAKEN framework, coupled with DLT UCC solution, will ensure the consumer's preferences are honored and only the relevant communication, text or calls, reach the consumer. DLT UCC Solution will maintain an immutable trace of end to end activities of commercial communication and ensure technology-driven compliance to prevent unwanted calls.

DLT based combined solution will help streamline the process for commercial communication and bring-in better governance. Key benefits include:

Connected World. Connected Solutions.

- Effective redressal and resolution of disputes by the Regulatory Authorities
- Elimination on the need for written consent from consumers for auto-dialer calls
- Enhanced visibility on whether the telemarketers are adhering to the specified guidelines
- Enhanced visibility on the content of the call as the registered telemarketer will share the details of communication when a scrubbing request is made
- Opportunity to create new avenues for monetization for Telecom Service Providers
- Blocking of unwanted calls as well as text messages per the consent/preference registered by the end consumer will lead to enhanced consumer satisfaction
- The combined solution enhances the security layer by both Blockchain and stir shaken capabilities.

Call flow with integrated STIR/SHAKEN and DLT UCC Solution



1. The Telemarketers/Business Entities/Service Provider will reach out to the Telecom Service Provider for Number Scrubbing for commercial communication. The header (content-type, e.g., education, health, etc.), the template (the content of the call), and list of numbers will be sent in the Scrubbing request.
2. The Telecom Service Provider will store the Scrubbing Request into the DLT along with the scrubbed list and generate a token. The response to the Telemarketers/Business Entities/Service Provider will include a token and list of virtual numbers. Virtual numbers will be a unique identifier for each consumer eligible to receive commercial communication, thereby preserving the privacy of the consumer's preference.
3. The Telemarketers will feed the scrubbed virtual number list along with the token to the auto-dialer to make the calls.

4. When the auto-dialer dials the virtual numbers, the Telecom Service Provider will identify the telemarketer based on the registered auto-dialer ID and the scrubbing token, reverse map the virtual number to the actual number.
5. The Telecom Service Provider's network will contact the authentication service to obtain a private key with which it can sign the call.
6. The Telecom Service Provider will use the key to sign the call with the telemarketer's information and the authentication service's certificate.
7. On receiving the call, the terminating Telecom Service Provider will send the identifying information and the certificate to a verification service.
8. The verification service will check with a certificate repository to ensure that the authentication service is authorized and that its certificate is valid. It then uses the public key that corresponds uniquely to the sending authentication service's private key to verify the signed call.
9. Information about whether the call has been verified or if some problem has occurred (e.g., the call did not match asserted caller's identity, certificates have expired, information was in an improper format) will be then sent to the terminating Telecom Service Provider.

Why the IBM Blockchain Platform for the DLT?

The UCC solution has been implemented on Hyperledger Fabric, which is the premier blockchain framework for enterprise use. The IBM Blockchain Platform, built around Hyperledger Fabric, offers an array of capabilities that expand and enhance the value of Fabric. It allows members to model, create, and operate networks with the performance and security necessary for a multitude of use cases in regulated industries. IBM Blockchain Platform software, is optimized to deploy on Red Hat OpenShift, Red Hat's state-of-the-art enterprise Kubernetes platform. This means we now have even more flexibility when choosing where to deploy your blockchain network components, whether on-premises, in public clouds, or hybrid/multi-cloud architectures.

Conclusion

In India, the DLT solution for Unsolicited Commercial Communication has been implemented by the key Telecom Service Providers like Airtel, Jio, Vodafone, etc., which have a combined consumer base of around 1 Billion. The solution is expected to go live in the second half of 2020.

Meanwhile, the FCC mandated STIR/SHAKEN implementation will be in three phases -

1. Consists of development of the SHAKEN (Signature-based Handling of Asserted information using toKENs) framework, based on the protocols developed by the IETF's (Internet Engineering Task Force) STIR (Secured Telephony Identity Revisited) working group.
2. Consists of the "Governance Model and Certificate Management for the Trust Anchor," describing how entities will be granted the trust necessary to vouch for call authenticity, and the organizational structures needed to manage this process.
3. Consists of the "Call Validation Display Framework" that will recommend how to display SHAKEN/STIR information to consumers. ATIS and the SIP Forum are still developing phase 3.

The first phase of STIR/SHAKEN is on its way to completion.

Hence it's a convenient time for the STIR/SHAKEN and UCC DLT solution be combined to holistically solve the problem of illegal and legal unwanted commercial communication for the end consumers.

Connected World. Connected Solutions.

Sources:

STIR/SHAKEN :

https://www.atis.org/sti-ga/resources/docs/ATIS-1000074.pdf
https://www.atis.org/sti-ga/resources/docs/ATIS-1000080.pdf
https://www.sipforum.org/download/sip-forum-twg-10-signature-based-handling-of-asserted-information-using-tokens-shaken-pdf/
https://tools.ietf.org/html/draft-ietf-stir-passport-shaken-06
https://tools.ietf.org/html/rfc8225
https://tools.ietf.org/html/draft-ietf-stir-passport-shaken-06#ref-ATIS-1000074
https://www.atis.org/01_legal/docs/Robocall%20Blocking%20Comments-FINAL.pdf
https://www.atis.org/01_news_events/webinar-pptslides/SHAKEN101_%20MitigatingIllegalRobocalling01302019.pdf

Unsolicited Customer Communication :
https://main.trai.gov.in/sites/default/files/RegulationUcc19072018.pdf
https://main.trai.gov.in/sites/default/files/UCC_CP_14092017.pdf
https://m.economictimes.com/industry/telecom/telecom-policy/trai-overhauls-rules-on-pesky-calls-spam-messages-spells-out-obligation-of-telcos/articleshow/65057432.cms

https://www.ftc.gov/about-ftc/what-we-do
https://www.fcc.gov/about/overview

Tech Mahindra

Tech Mahindra

www.techmahindra.com
connect@techmahindra.com
www.youtube.com/user/techmahindra09
www.facebook.com/techmahindra
www.twitter.com/tech_mahindra
www.linkedin.com/company/tech-mahindra