Messaging Principles and Best Practices

January 19, 2017

ctia Everything™ Wireless

Table of Contents

1 Executive Summary

The Messaging Principles and Best Practices (Principles and Best Practices) is a set of voluntary best practices developed by wireless messaging ecosystem stakeholders. It identifies parameters for facilitating the exchange via transmission, storage and retrieval (exchange), of person-to-person (P2P) and application-to-person (A2P) messages via wireless provider messaging networks while protecting consumers from unwanted messages.[1]

Messaging's popularity is largely attributable to its status as a trusted and convenient communications environment. Thus, the objectives of this document are to support a robust and dynamic wireless messaging community where:

- Wireless consumers can exchange wanted messages with other wireless consumers;
- Enterprises and consumers can exchange wanted messages; and
- Consumers are protected from unwanted messages, including in conformity with applicable laws and regulations, such as the United States' Telephone Consumer Protection Act (TCPA).

[1] For simplicity, the Principles and Best Practices uses the term "unwanted messages" to describe unsolicited bulk commercial messages (i.e. spam); "phishing" messages intended to access private or confidential information through deception; other forms of abusive, harmful, or malicious, unlawful, or otherwise inappropriate messages; and messages which required an opt-in that was not obtained or revoked.

2 Scope

2.1 Purpose

The Principles and Best Practices are intended for entities primarily operating in the wireless messaging ecosystem to facilitate innovation and the use of wireless messaging while protecting consumers from unwanted messages. The Principles and Best Practices may also be helpful to inform consumers of wireless messaging services, and anyone with an interest in the wireless messaging ecosystem.

The Principles and Best Practices replace CTIA's SMS and MMS Interoperability Guidelines that were developed in consultation with stakeholders for an earlier period in the messaging ecosystem. These Principles and Best Practices offer a broader, simpler and less technical set of recommendations that reflect an evolving wireless messaging ecosystem.

These Principles and Best Practices represent an important further step in the wireless industry's effort to support new uses and business opportunities in wireless messaging services while still maintaining protections for consumers. The recommendations described in this document, however, will require ongoing operational and technical efforts by stakeholders in the messaging ecosystem to align individual company processes and systems that are necessary for implementation.

Although the specific technical and operational details required for service provider implementation are beyond the scope of this document, the Principles and Best Practices acknowledge that service provider implementation will be an ongoing process that continues to evolve as new use cases arise throughout the wireless messaging ecosystem.

2.2 Wireless Messaging Services

The Principles and Best Practices primarily address wireless messaging services that use 10-digit telephone numbers assigned from the North American Numbering Plan (NANP) as the unique identifier for the sender and/or recipient(s) of individual or group messages. Generally, wireless messages between subscribers are exchanged between 10-digit NANP telephone numbers via wireless providers' messaging networks. These messaging services include:

- Short Message Service (SMS)
- Multimedia Messaging Service (MMS); and
- Rich Communications Suite (RCS).

As described in Section 5.1 below, a five or six-digit number known as a *short code* can also be used to exchange wireless messages via wireless providers' messaging networks.

The messaging ecosystem also includes cloud-based services that require the use of a separate messaging client (e.g. an app) that is distinct from and does not interoperate with wireless providers' messaging networks. These Principles and Best Practices are intended to apply to messaging services that interoperate between cloud-based platforms and wireless providers' messaging networks using the applicable services, such as SMS, MMS or RCS.

While these Principles and Best Practices are applicable to emerging messaging services, such as RCS, the CTIA Unwanted Messaging Traffic Threat Forum will continue to monitor the messaging ecosystem and consider revisions to these Principles and Best Practices, as necessary.

2.3 Scope Limitations & Disclaimer of Legal Guidance or Advice

CTIA's Principles and Best Practices do not constitute or convey legal advice and should not be used as a substitute for obtaining legal advice from qualified counsel. Use of and access to the Principles and Best Practices or any of the links contained herein do not create an attorney-client relationship with CTIA and the user.

Messaging services may be subject to a number of legal requirements, including those established by the Telephone Consumer Protection Act (TCPA) and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), as well as implementing regulations adopted by the Communications Act of 1934, as amended. Messaging ecosystem stakeholders or readers of this document should consider obtaining legal and/or regulatory advice prior to taking any action related to the provision of messaging services.

As a set of voluntary best practices, CTIA's Principles and Best Practices do not impose, prescribe or require contractual or technical implementation on messaging ecosystem stakeholders, including service providers. Due to contractual, technical, or other practical factors, methods of implementing the Principles and Best Practices may vary among stakeholders.

3 Wireless Messaging Ecosystem

3.1 Background

When wireless messaging first arose in the late 1990s, all traffic was delivered on a P2P basis using 10-digit NANP telephone numbers. These early messaging systems did not offer carrier interoperability – a subscriber could only communicate by messaging with other subscribers of the same wireless provider. To address this problem, in the early 2000s, CTIA convened the wireless industry to help solve the consumer challenge of using SMS messaging services across other mobile networks. CTIA established the *SMS Interoperability Guidelines* to unlock inter-carrier messaging and industry standards for SMS interoperation among mobile networks. Today, SMS and MMS messaging services have become a convenient and trusted communication tool for consumers and, increasingly, enterprise users.

In the early 2000s, CTIA and other messaging ecosystem stakeholders developed the short code platform (i.e. five or six digit codes) to facilitate the appropriate use of bulk wireless messages. Short code messages enable wireless messaging campaigns that are vetted by wireless providers. The combination of upfront vetting with ongoing auditing means that short codes can enable high-volume messaging campaigns while minimizing the risk that short codes will be used to distribute unwanted messages.

In 2009, building on the successful SMS and MMS inter-carrier interoperability initiative, CTIA and messaging stakeholders expanded the *SMS Interoperability Guidelines* to guide how non-mobile networks could exchange SMS message traffic with mobile wireless networks. In 2011, CTIA and the messaging stakeholders further expanded the *SMS Interoperability Guidelines* to include cloud-based services that use 10-digit NANP telephone numbers, and addressed unwanted message risks associated with this expanded ecosystem. In 2014, as the messaging ecosystem evolved, CTIA and messaging stakeholders also revised the *SMS Interoperability Guidelines* to account for group messaging and text-enabled toll-free telephone numbers.

All of these efforts have been premised on the common goal of maintaining and enhancing a dynamic and competitive wireless messaging ecosystem, while limiting consumers' exposure to unwanted messages. In pursuit of this goal and consistent with these Principles and Best Practices, messaging ecosystem stakeholders should promote the exchange of wanted messages among wireless consumers and enterprises, minimize risks to wireless consumers of receiving unwanted messages, and conduct fair dealing with each other, as well as comply with applicable laws and obligations.

3.2 The Current Wireless Messaging Ecosystem

Messaging to 10-digit NANP telephone numbers has enabled wireless consumers to communicate with each other, enterprises and other organizations, generally, in a low-volume conversational manner. The wireless messaging ecosystem has strived to enable such low-volume, consumer-oriented communications, while simultaneously seeking to inhibit unwanted messages from reaching consumers.

Messaging's popularity among consumers is largely attributable to its status as a trusted and convenient wireless communications environment. For enterprises, messaging is an increasingly attractive platform to reach consumers because of broad adoption by wireless consumers and consumers' abilities to retrieve messages when convenient and to store them as desired.

As the role of wireless messaging services evolves among consumer communications tools, new business models are emerging around exchanging high-volume messaging traffic using 10-digit NANP telephone numbers. To protect consumers from unwanted messages, service providers deploy filters that limit messaging traffic bearing the characteristics of unwanted messages. Messaging using short codes also offers opportunities to exchange high-volume traffic in ways that inhibit unwanted messages from reaching consumers. As these new models develop, these Principles and Best Practices are focused on maintaining a wireless messaging environment largely free of unwanted messages.

3.2.1 Ongoing Efforts to Combat Unwanted Messages

Technological advances in wireless messaging hold tremendous promise for consumers to engage in social and commercial communications, but these advances also pose threats if unwanted messages negatively impact the role of messaging as a trusted and convenient wireless communications environment. Section 6 of these Principles and Best Practices describe efforts to inhibit unwanted messages.

3.2.2 Introduction of Application-to-Person (A2P) Messaging using 10-Digit NANP Telephone Numbers

CTIA's *SMS Messaging Interoperability Guidelines* focused on Peer-to-Peer (P2P) communication (see description of P2P in Section 4.1). Enterprise users seeking to achieve higher messaging traffic volumes have used the short code platform to deliver A2P messages (*see* description of A2P in Section 4.2). Among other things, these Principles and Best Practices account for new business models and messaging technologies involving the distribution of higher volumes of messages using 10-digit NANP telephone numbers through A2P and short code messaging.

3.3 Messaging Ecosystem Roles

The messaging ecosystem comprises many stakeholders working together to create, route, deliver, store, retrieve, and consume messaging services.

3.3.1 Consumers

Consumers are individual persons who subscribe to specific wireless messaging services or messaging applications.

3.3.2 Enterprises

An *enterprise* is a business or entity that uses messaging to communicate with consumers. Examples include social networks, large and small businesses, financial institutions, schools, medical practices, and non-profits.

3.3.3 Wireless Facilities-Based Service Providers (Wireless Providers)

Wireless providers own and operate radio telephone and data networks, and make available to consumers a wide variety of wireless communications products and services, including wireless messaging services, such as SMS, MMS and RCS.

3.3.4 Mobile Virtual Network Operators (MVNOs)

MVNOs are wireless service providers that do not own the network infrastructure over which they provide services. Instead they resell network services maintained by one or more wireless providers.

3.3.5 Cloud-Based Providers

Cloud-based providers enable services like voice and messaging to end users using over-the-top IP connectivity or through interoperability with wireless carrier-networked services, including wireless messaging. Some cloud-based providers offer an API to access wireless services while others offer standalone applications.

3.3.6 Inter-Carrier Vendors (ICVs)

Also called hub providers, *ICVs* act as hubs to facilitate interoperability by transporting messaging traffic between multiple wireless providers and cloud-based providers.

3.3.7 Connection Aggregators

Connection aggregators offer a variety of value-added services to enterprise customers – not the least is messaging connectivity into multiple wireless providers. Unlike ICVs, connection aggregators do not typically support inter-carrier peering traffic.

3.3.8 Competitive Local Exchange Carriers (CLECs)

In the messaging ecosystem, *CLECs* provide 10-digit NANP telephone numbers and traffic routing services to cloud-based providers.

3.3.9 Registries

In order to establish a record of 10-digit NANP telephone number resources used to support the effective exchange of wireless messages, *registries* operate databases of telephone numbers and the associated communications provider or providers (CLEC, wireless provider, cloud-based provider) enabling wireless messaging service to those

10-digit NANP telephone numbers. Customers of the registries include CLECs, wireless providers, ICVs, cloud-based providers, and enterprises.

3.3.10 Network Security Vendors

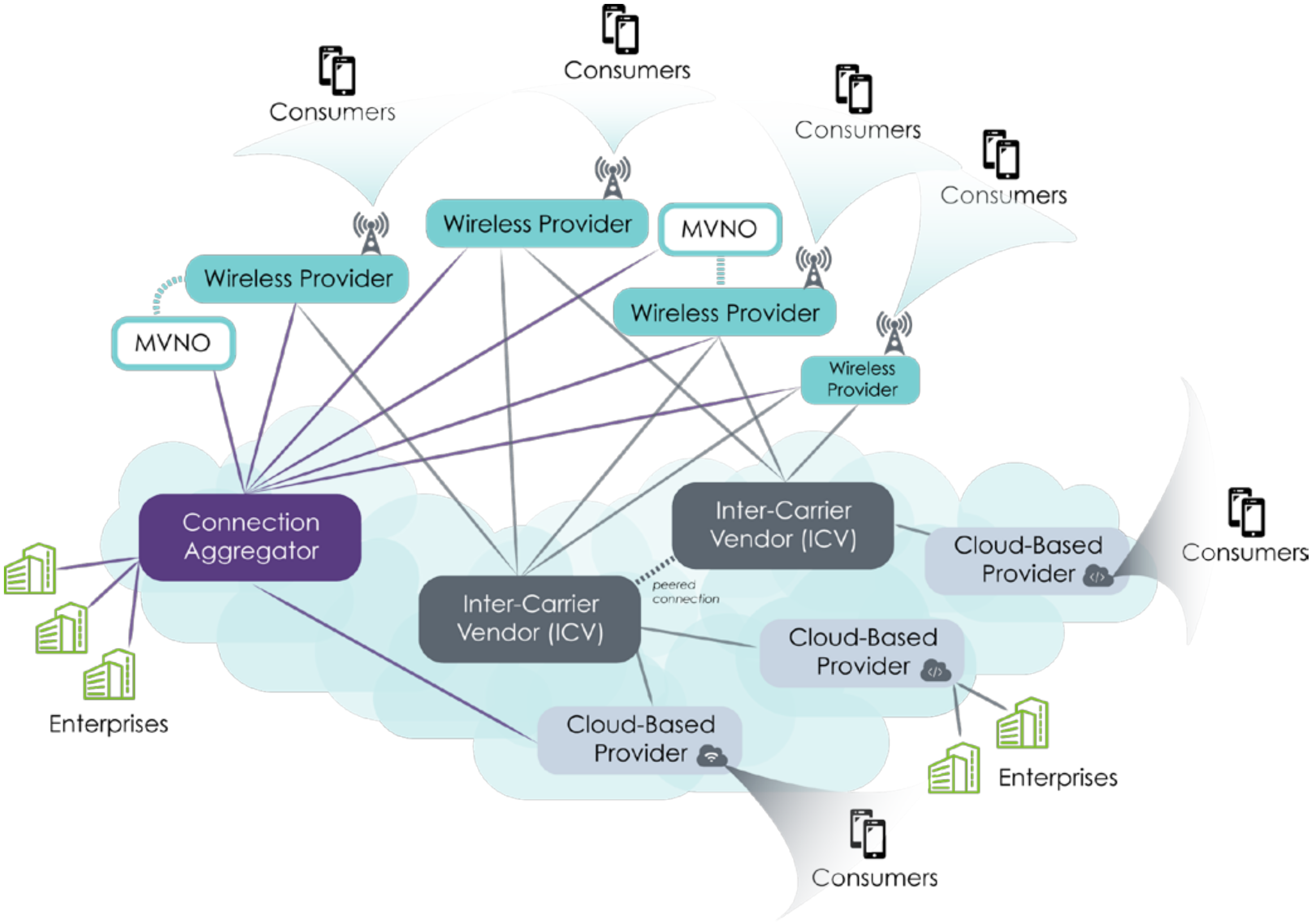
Network security vendors provide solutions that enable wireless providers, cloud-based providers, and ICVs to identify unwanted message traffic. These solutions deliver a variety of network security features, including spam containment and management.

3.3.11 Service Providers

These Principles and Best Practices use the term *service provider* to refer to any of the parties identified above that offer messaging services or messaging-related services to consumers or enterprises using 10-digit NANP telephone number or short codes, including wireless providers, MVNOs, cloud-based providers and CLECs.

3.4 Wireless Messaging Ecosystem Schematic

Exhibit I Wireless Messaging Ecosystem Schematic



4 Traffic Classification

4.1 Person-to-Person (P2P)

Person-to-Person (P2P) generally describes the low-volume exchange of wireless messages between end users. To date, most end users exchanging this type of low-volume messaging traffic are individual wireless consumers, but, more recently, exchanges between wireless consumers and other endpoints, such as consumers of cloud-based messaging services or enterprises, are becoming more common.

To provide greater certainty and consistency of classification across the messaging community, these Principles and Best Practices establish consensus-based definitions of P2P wireless messaging traffic around the concept of typical human operation.

4.1.1 Typical Human Operation

For purposes of these Principles and Best Practices, the concept of ***consistent with typical human operation*** defines P2P traffic to distinguish P2P from A2P traffic (see Section 4.2).

Exhibit II outlines the characteristics and attributes of typical human operation for the purpose of classifying P2P messaging traffic.

Exhibit II Attributes of Typical Human Operation for Classifying P2P Wireless Messaging Traffic

	METRIC	LIMIT	NOTES
Throughput	Messages/telephone number (TN)/minute	15 to 60 messages per minute	A human is typically not able to originate more than about one message per second.
Volume	Messages/TN over time	1,000 per day	Only in unusual cases do humans send more than a few hundred messages in a day, nor can a human send messages continuously over a long period of time.
Unique Recipients	Number of distinct recipients/TN	200	A human has a relatively small number of contacts.
Balance	Ratio of outgoing to incoming messages per TN	1:1 with some latitude in either direction	Human communications are conversational. An

	incoming message typically generates a response from the recipient.

4.1.2 Treatment of P2P Traffic

Subject to the Classification Framework of A2P described in Section 4.3, in general, wireless messaging traffic from a 10-digit NANP telephone number that is consistent with all of the attributes of typical human operation described in Section 4.1 above and does not exhibit characteristics of unwanted messaging traffic, as identified consistent with Section 6 below, should be expected to be deliverable across the messaging ecosystem.

4.2 Application-to-Person (A2P)

A2P traffic is all messaging that falls outside the definition of P2P (*i.e.,* traffic that is ***not consistent with typical human operation***).

These Principles and Best Practices identify the protection of consumers from unwanted messages, particularly from high-volume messaging traffic, as a key consensus-based goal among messaging ecosystem stakeholders. The establishment of clear parameters around P2P traffic will help facilitate the continued deployment of A2P services and options consistent with protecting networks and consumers. Individualized arrangements and close collaboration among messaging ecosystem stakeholders afford an appropriate environment for the deployment of emerging A2P business models.

4.2.1 A2P Traffic and Commercial Arrangements

The wide range of use cases that continue to emerge in the marketplace precludes any simple, rigid categorization of A2P traffic at this time. In the evolving marketplace, the messaging ecosystem stakeholders will continue to work to enable effective interoperability. Without A2P commercial arrangements, messaging traffic that is being represented as P2P, but is inconsistent with typical human operation, may be inhibited as unwanted. If facilitating the exchange of this traffic as A2P messages is appropriate, technical and contractual arrangements should be negotiated independently among the messaging ecosystem stakeholders and on an individualized basis.

4.2.2 A2P Traffic and Consumer Choice

Although these Principles and Best Practices do not provide legal advice or guidance, the messaging ecosystem should operate consistent with relevant laws and regulations, such as the Telephone Consumer Protection Act (TCPA) and associated FCC regulations regarding the provision and revocation of consumer consent for communications. For this reason, A2P messages should consider:

- The consumer's express consent to receive informational messages;
- The consumer's express *written* consent to receive marketing messages; and

- The ability for the consumer to revoke consent.

Individual service providers may adopt additional consumer protection measures for vendors for A2P messaging, as described below in Section 6. Such measures may include campaign pre-approval, service provider vetting, in-market audits, or unwanted message filtering practices that are tailored to facilitate the exchange of wanted messaging traffic among consumers and enterprises.

4.3 Message Classification Framework

Exhibit III combines the definitions of P2P and A2P into a framework for message classification.

Exhibit III Messaging Classification Framework

	P2P	A2P
Opt-In and Opt-Out	Typically not required as consumer-to-consumer	Express consent Opt-out (e.g., STOP keyword)
Traffic Volume	Consistent with typical human operation	As contractually agreed
Program Review Process	Not required	May be required
Recommended Usage	Consumers texting one or more consumers	Enterprises texting multiple consumers simultaneously Call center scenarios Alerts and notifications Machine to Machine
Typical Scenarios	Traditional individual conversational texting. Group messaging with appropriate opt-out capabilities. One-time or very rare exceptions for spikes (*e.g.*, when user notifies his/her contacts of new number).	Call center scenarios; session typically initiated by consumer but not required. Permission for session is assumed. Typical bulk messaging, campaigns, marketing, business outreach, 2-way campaigns, notification, Two factor authentication Recipients should be notified periodically how to opt out. Service providers enforce the STOP layer.

5 Additional Best Practices

5.1 Common Short Codes

Common short codes are non-NANP addresses of 5 or 6 digits typically used by enterprises for communicating with consumers at high-volume (e.g., airline flight delays, banking account alerts, shipping company delivery notifications, school delays etc.). The short code platform was developed to accommodate higher volume SMS traffic with upfront consumer protections from unwanted messaging traffic and review procedures to ensure appropriate use of the platform.

In the United States, the Common Short Code Administration (CSCA) operates the cross-carrier short code registry. The CTIA Short Code Monitoring Handbook offers best practices and other guidelines for conducting A2P messaging campaigns using short codes.

In Canada, the Canadian Wireless Telecommunications Association (CWTA) administers short code assignments through its txt.ca website. The Canadian Common Short Code Application Guidelines publication offers best practices and other guidelines for short code campaigns in the Canadian marketplace.

5.2 Group Messaging

Group messaging is typically facilitated through cloud-based services (e.g. a mobile app) that enables the creation of consumer messaging groups.

Due to its one-to-many nature, group messaging requires special accommodation in the definition of P2P traffic. Thus, it is recommended that group messaging traffic:

- Be classified as consistent with human operation and classified as P2P provided that messaging traffic to/from the group number is itself consistent with the Attributes of Typical Human Operation (see Exhibit II above);
- Have strong anti-abuse controls that are appropriate for systems with potentially large message distribution, consistent with Section 6 below;
- Support the ability of any member to opt out of the group at any time; and
- Employ mechanisms to prevent recursive group messaging and cyclical messaging involving more than one group (e.g., in which one group is a member of another group).

Although group messaging services are classified as P2P, special arrangements may be required between the messaging service provider(s) hosting a group messaging service and other service providers whose customers use the group service to ensure wanted messages are deliverable.

5.3 Proxy Numbers

Messaging providers may also utilize a 10-digit NANP telephone number as a proxy number that functions as a relay point between possibly large sets of and/or frequently-changing phone numbers in certain wireless messaging use cases.

For example, a driver for a ride-sharing service may need to communicate with a prospective passenger to confirm a pick-up location. The proxy telephone number functions as a conference call bridge telephone number, allowing the driver and passenger to communicate without either party having to reveal his or her personal telephone number. Another example is a service that allows a user to establish a single telephone number with the ability to relay calls and messages to any of several other telephone numbers held by the user.

A 10-digit NANP telephone number used as a proxy is typically only a means to achieve the end of connecting two individuals, but proxy numbers are commonly re-used in a way that may create volumes of messaging traffic that exceed Typical Human Operation.

Given the use of proxy numbers to facilitate high-volume messaging traffic among multiple 10-digit NANP telephone numbers, the proxy number should be classified as A2P wireless messaging traffic. Although P2P group messaging services may use proxy numbers and display some volumetric characteristics of A2P, special routing consideration can be given for these group messaging services, as discussed in Section 5.2 above.

5.4 Toll-Free

Toll-free telephone numbers are a subset of NANP telephone numbers that use the following numbering plan area codes (NPAs): 800, 888, 877, 866, 855 and 844, with 833 tentatively set to open in 2017. While toll-free numbers (TFNs) have generally supported only voice calling, the messaging ecosystem has evolved to use a toll-free telephone number as the identifier for wireless messaging services.

To uphold the integrity of toll-free telephone numbers, provide transparency to Responsible Organizations (Resp Orgs) who manage the use of toll-free telephone numbers for voice services, and protect consumers from unwanted messages from toll-free telephone numbers, it is recommended that messaging ecosystem stakeholders should operate in accordance with the following:

5.4.1 Authority to Text-Enable Rests with the Toll-Free Voice Subscriber

The toll-free subscriber who is the holder of record of a TFN for voice services has the sole authority to control additional services associated with that TFN. Only TFNs that are currently reserved or in working status for the benefit of a TFN voice subscriber should be enabled for messaging.

At this time, additional discussions among messaging ecosystem stakeholders are necessary to consider appropriate approaches to wireless message enabling of TFNs that protect the toll-free subscriber's authority to control voice, messaging and other services associated with that TFN. In order to facilitate the innovative use of TFNs for messaging services, individually negotiated contractual relationships should be utilized until these Principles and Best Practices can be evolved to reflect a consensus-based view about the appropriate approach to wireless message-enabling TFNs.

5.4.2 Transparency to Resp Orgs

In order to provide transparency to Resp Orgs and other service providers about TFNs that are wireless messaging enabled, any process for provisioning messaging associated with a TFN should allow or provide for synchronization with a registry or registries that provide a comprehensive record of text-enabled TFNs and associated TFN subscribers. In addition, registries should be operated consistent with the principles in Section 5.5 below.

5.4.3 Special Considerations for Shared Use Toll-Free Telephone Numbers

For the benefit of a TFN voice subscriber, message enablement of a TFN should account for any shared use arrangements that are part of the voice service associated with the TFN. In the case of shared use TFNs, the toll-free voice service provider should be treated as the toll-free subscriber to uphold the integrity of the toll-free number and protect subscribers of a toll free voice service which terminates voice telephony traffic to more than one subscriber. Such shared use arrangements include, but are not limited to, geographic-based and time-of-day-based sharing.

5.5 Registries

To achieve impartiality with respect to number registration, registry service providers should commit to fair dealing, on reasonable and non-discriminatory rates, terms and conditions with stakeholders of the messaging ecosystem and operating the registry in good faith.

6 Unwanted Messaging Traffic Threat Containment

6.1 Core Principles

It is in the best interests of consumers and all members of the wireless messaging ecosystem to enable consumers to freely exchange wireless messages with other consumers and enterprises while endeavoring to eliminate unwanted messaging traffic threats.

Wireless messaging is a trusted and convenient communications platform among consumers and enterprises. The immediacy, retrieval and storage capabilities, and high open rates associated with wireless messaging services make wireless messaging an ideal medium for all sorts of communications – including relaying urgent information to consumers such as fraud alerts or flight changes. This high trust and open rate is believed to be associated with the spam-free environment of messaging.

Unwanted messaging traffic or reduction in reliable delivery diminishes consumer trust in the wireless messaging ecosystem. It is vital that the wireless messaging ecosystem stakeholders work together to keep the relatively pristine wireless messaging environment free of unwanted messaging traffic while taking steps to support the exchange of wanted wireless messages among consumers and enterprises.

The following core principles help ensure that consumers are protected from unwanted messaging traffic:

- All service providers should use reasonable efforts to prevent unwanted messaging traffic from being sent by or to their subscribers, including review to ensure that messages are not unwanted;
- All service providers may block unwanted messaging traffic before it reaches consumers; and
- To the extent practicable, supported by messaging architecture and protocols, reasonable and in a manner consistent with Unwanted Messaging Traffic Containment Best Practices below, all service providers should notify the service provider from which unwanted messaging traffic was received when blocking unwanted messaging traffic.

6.2 Unwanted Traffic Containment Best Practices

Service providers should adopt unwanted messaging traffic practices that protect consumers in a manner that facilitates the exchange of wanted wireless messaging traffic among consumers and enterprises.

6.2.1 Protecting Consumers

Service providers should give consumers a choice whether or not to receive wanted wireless messages. They should also support the systems and processes required to process consumer choices.

6.2.1.1 Blocking Unwanted Messaging Traffic

Unwanted messaging traffic can be blocked by consumers and by service providers. Service providers should give consumers the option to block traffic from specific telephone numbers, including those sending unwanted messaging traffic.

Service providers should contain their emission of unwanted messaging traffic, making use of available information, such as message blocking indications received from other service providers. Service providers may incorporate unwanted messaging traffic filtering and blocking capabilities through individually negotiated contractual relationships, including enabling direct relationships between end-users and third party solution providers.

To the extent practicable, consistent with messaging architecture and protocols, reasonable and in a manner consistent with unwanted messaging traffic containment best practices, service providers should notify the service provider from which unwanted messaging traffic was received when blocking unwanted messaging traffic. If blocking or filtering of unwanted messaging traffic is implemented by service providers, the service provider should correspondingly offer appropriate unblocking processes to service providers.

6.2.1.2 Reporting Unwanted Messaging Traffic

In addition to blocking, consumers should be able to report unwanted messaging traffic to their service provider. Service providers should establish and maintain an automated system to collect complaints detailing unwanted messaging traffic.

6.2.1.3 Honoring Consumer Consent

For messages that require the consent of the recipient, senders or their service provider should present consumers with a TCPA-compliant opt-in process. Equally, senders or their service providers should support simple opt-out processes so that consumers can choose to stop receiving messages at any time.

6.2.2 Protecting the Wireless Messaging Ecosystem

Well-organized, rapid communication between service providers is essential to address unwanted messaging threats based on the best available information. Unwanted messaging traffic control measures should be refined continually to support the exchange of wanted messaging traffic among consumers and enterprises.

6.2.2.1 Open Communication

Service providers should consult with one another openly and in good faith when a potential unwanted messaging threat is identified. Providers should attempt to resolve the threat without suspending traffic between service providers, if possible.

6.2.2.2 Suspending Unwanted Messaging Traffic

Service providers may suspend the exchange of all unwanted messaging traffic when all other available and practical controls fail to stop the flow of unwanted messaging traffic. Notice of any such suspension can be provided to the impacted provider and any suspension of service should last only as long as reasonably necessary to identify and correct the problem, if restoration of service is requested by the suspended party.

6.2.2.3 Transparency of Traffic

If feasible, service providers may consider developing a unique identifier for enterprises that originate messaging traffic in order to protect the wireless messaging ecosystem against repeat unwanted messaging traffic offenders.

6.2.2.4 Network Operations Center

Service providers should maintain a network operations center (NOC) in service.

6.2.3 Recommended Response Intervals for Unwanted Messaging Traffic Threat Incidents

The timing and nature of notifications of unwanted messaging traffic incidents or threats as between service providers, and mitigation efforts by affected service providers, should correspond to the severity of the incident or threat.

6.3 CTIA Unwanted Messaging Traffic Threat Forum

CTIA’s Unwanted Messaging Traffic Threat Forum serves as the hub for the North American wireless messaging community’s efforts to maintain wireless messaging’s popularity of messaging among consumers as a trusted wireless communications environment.

To combat unwanted messaging traffic, the Forum will:

- Host regular conference calls devoted to threat identification and mitigation strategies;
- Engage as needed with related industry groups;
- Monitor unwanted messaging traffic threats; and

- Where appropriate, develop proposals to revise these Principles and Best Practices.

All qualified members of the messaging ecosystem should participate in the Unwanted Messaging Traffic Threat Forum to learn of attacks in the wireless messaging ecosystem and to share information about attacks observed on their platforms. The Forum operates in alliance with the Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG).