CTIA Publishes New Messaging Principles and Best Practices Guidance

February 3, 2017

On January 19, 2017, CTIA issued a new guidance document developed by industry stakeholders with voluntary best practices for businesses that participate in the wireless messaging ecosystem entitled "Messaging Principles and Best Practices," (Messaging Best Practices or the Document). The Messaging Best Practices present a revised approach to wireless messaging, replacing the previous SMS and MMS Interoperability Guidelines with "a broader, simpler and less technical set of recommendations that reflect an evolving wireless messaging ecosystem."

This client advisory provides an overview of the Messaging Best Practices and how the guidance applies to the various entities who participate in the messaging ecosystem by sending, receiving, routing, storing, or delivering messaging services.

The stated objective of the Messaging Best Practices is to facilitate growth and innovation in the messaging industry while protecting consumers from unwanted messages.

Scope of Messaging Best Practices

The Messaging Best Practices focus primarily on wireless messaging services that use 10-digit telephone numbers assigned by the North American Numbering Plan (NANP) as the way to identify the sender and recipient of messages. The Document includes discussion about the following messaging types that are a part of the broader messaging ecosystem:

- **Wireless subscriber messaging** using NANP phone numbers over wireless providers' network which includes short messaging service (SMS), multimedia messaging service (MMS), and rich communications service.
- **Short code messaging** using a five or six-digit numbers to send messages via wireless providers' networks, generally used by enterprises.
- **Cloud-based messaging** that involves the use of a messaging tool like an app over the Internet rather than via wireless providers' networks.

State of the Wireless Messaging Ecosystem

The Messaging Best Practices explain that traditionally the messaging environment involving NANP phone numbers has focused on facilitating low-volume conversational communication between wireless consumers, enterprises and other organizations. However, messaging's popularity has increased and it has become a preferred form of communication for many consumers. As a result, there is greater interest by enterprises in using messaging as a platform to reach consumers. It recognizes that this has resulted in a continually evolving messaging ecosystem with new business models emerging to enable high-volume messaging using 10-digit NANP phone numbers.

The Messaging Best Practices consider the use of application-to-person (A2P) messaging and short codes, not just peer-to-peer (P2P) messaging, and account for new business models and messaging technologies. To account for the development of these new models, the Messaging Best Practices' guidance focuses simply on the principle that all ecosystem participants should ensure the successful transmission of **wanted messages** between consumers and enterprises while minimizing the risk of unwanted messages by employing principles of fair dealing.

The Document's description of the wireless messaging ecosystem includes the following roles and participants:

1. **Consumers** – People who subscribe to wireless messaging services or applications.

2. **Enterprises** – Businesses or organizations that employ messaging to communicate with consumers.

3. **Wireless Providers**

   a. **Facilities-based service providers** – Wireless providers that are the owners and operators of radio telephone and data network infrastructure who also offer a variety of wireless communications products and services, including wireless messaging, to consumers.

b. **Mobile virtual network operators (MVNOs)/resellers** – Wireless providers that resell rather than own the network infrastructure that they use to provide wireless communications products and services.

4. **Cloud-based providers** - Providers of voice and messaging services to consumers via over-the-top IP connectivity or interoperability with wireless provider-networked services including wireless messaging.

5. **Inter-carrier vendors (ICVs)** – Entities, also called hub providers, that enable interoperability by transporting messaging traffic between multiple wireless providers and cloud-based providers.

6. **Connection aggregators** – Entities that provide services to enterprise customers like messaging connectivity with wireless providers. Unlike ICVs, aggregators do not usually provide for peering traffic between aggregators.

7. **Competitive local exchange carriers (CLECs)** – Carriers that provide NANP phone numbers and traffic routing services to cloud-based providers.

8. **Registries** – Entities that maintain databases of telephone numbers and the associated communications provider that is enabling wireless messaging to those NANP phone numbers. This ensures there is an established record of NANP phone number resources that can be used to enable effective exchange of wireless messages.

9. **Network security vendors** – Solution providers that facilitate identification of unwanted messaging traffic for wireless providers, cloud-based providers, and ICVs.

10. **Services providers** – This refers to any entity that offers messaging services or messaging-related services to consumers or enterprises using NANP phone numbers or short codes including wireless providers, MVNOs, cloud-based providers and CLECs.

Classification of Messaging Traffic

The Messaging Best Practices provide guidance on how service providers should distinguish, classify, and treat differing classes of messaging traffic.

P2P Traffic

The P2P label should be applied to the low-volume exchange of wireless messages between end users, which typically involves messaging between individual wireless consumers. More recently, the exchange of P2P messages also includes consumers who use cloud-based messaging services as well as some enterprises. P2P should be distinguished from A2P traffic based on its consistency with **typical human operation**. Traffic that has the attributes of typical human operation and does not exhibit characteristics of unwanted messaging should be expected to be deliverable across the messaging ecosystem. Metrics for assessing whether messaging traffic is consistent with typical human operation are as follows:

- **Throughput** – number of messages per telephone number per minute
- **Volume** – number of messages per telephone number over a long period of time
- **Unique recipients** – number of distinct recipients per telephone number
- **Balance** – ratio of outgoing to incoming messages per telephone number

A2P Traffic

The Document classifies A2P traffic as any wireless messaging traffic that does not meet the definition of P2P traffic. A key goal of messaging ecosystem participants is protection of consumers from unwanted messaging particularly those of the high-volume capacity. Therefore, messaging ecosystem stakeholders are encouraged to establish individual arrangements and collaborate closely to facilitate an environment for the continued deployment of A2P services and emerging A2P business models.

The Messaging Best Practices explain that because of the evolving messaging marketplace it is not possible develop specific categorization of A2P traffic attributes at this time. The Messaging Best Practices express that without the negotiation of commercial arrangements, certain traffic being represented as P2P-caliber may be inhibited due to the presence of features not consistent with typical human operation. The Document further encourages messaging stakeholders to ensure their operations are consistent with relevant laws and regulations including the Telephone Consumer Protection Act (TCPA) and Federal Communications Commission (FCC) regulations about the provision and revocation of consumer consent for communications.

The following framework combines the definition of P2P and A2P traffic to provide a recommended approach to messaging classification:

	Peer-to-peer (P2P)	**Application-to-peer (A2P)**
Opt-in and Opt-out	Typically not required as this is consumer-to-consumer communication	Seek express consent; provide opt-out option (e.g., STOP keyword)
Traffic Volume	Consistent with typical	Dependent on whatever

	human operation	is agreed on contractually
Program Review Process	Not required	May be required
Recommended Usage	For consumers texting other consumers	For 1) enterprises sending texts to multiple consumers simultaneously; 2) call center scenarios; 3) alerts and notifications; and 4) machine-to-machine
Typical Scenarios	1) Traditional individual conversational texting. 2) Group messaging with appropriate opt-out capabilities. 3) One-time or rare exceptions for spikes (e.g., when user notifies his/her contacts of a new number)	1) Call center scenarios; session typically initiated by consumer but not required. Permission for session is assumed. 2) Typical bulk messaging, campaigns, marketing, business outreach, two-way campaigns, notifications, two factor authentication. 3) Recipients should be notified periodically of how to opt-out. 4) Service providers enforce the STOP layer.

Best Practices for Other Aspects of Wireless Messaging

- For **common short codes**, the Best Practices recommends the CTIA Short Code Monitoring Handbook and highlights the existence of the cross-carrier short code registry, Common Short Code Administration.

- For consumer **group messaging**, the following special accommodations for the P2P traffic classification are recommended:

  - Despite the one-to-many nature, classify this kind of traffic as consistent with human operation and classify as P2P if it meets the requisite attributes;

  - Employ strong anti-abuse controls that are appropriate for large message distribution systems;

  - Enable the ability of members to opt out of the group message at any time; and

  - Prevent recursive group messaging and cyclical messaging involving more than one group (e.g., one messaging group is a member of another group).

- When a NANP telephone number is used as a **proxy number** that serves as relay point to achieve connections between two individuals (e.g., serving as a conference bridge number for ride sharing drivers to communicate with customers without providing their personal number), it may result in the phone number being re-used for communication with a large set of changing phone numbers. Proxy numbers are typically used to create high volumes of messaging traffic and should therefore be classified as A2P messaging traffic.

- For **toll-free number (TFN)** messaging, wireless messaging ecosystem stakeholders should operate in accordance with the principle that the toll-free subscriber, who is the holder of record for the TFN for voice services, has sole authority to control additional services associated with that TFN. The Document recommends, but does not require, that transparency should be provided to Responsible Organizations (Resp Orgs) that manage the use of TFNs for voice services by allowing synchronization with a registry or registries that provide a comprehensive record of text-enabled TFNs and associated subscribers. In addition, TFNs should only be text-enabled if they are currently reserved or in working status. Any process to text-enable TFNs should account for any shared use arrangements that are a part of the voice service for the number.

- **Registry** providers should commit to fair dealing, on reasonable and non-discriminatory rates, terms and conditions with all messaging ecosystem stakeholders and operate their registry in good faith to ensure there is impartiality regarding number registration.

Unwanted Messaging Traffic Threat Management

The Messaging Best Practices describe the current state of wireless messaging as “a trusted and convenient communications platform” that has been successful largely due to the reliability and spam-free environment. As a result, the Document outlines a number of principles that stakeholders should use to limit delivery of unwanted messages while maintaining the successful delivery rate for wanted communications. Specifically,

- Service providers should use reasonable efforts to limit unwanted messages from being sent by or to their subscribers;

- Service providers should block unwanted messages before they reach consumers;

- Service providers should notify the service provider from which unwanted messaging traffic is derived, to the extent practicable, when blocking those unwanted messages.

In addition, the Messaging Best Practices recommends that service providers give consumers the option to block traffic from specific phone numbers and should make use of blocking indicator information received from other service providers. Service providers may also incorporate unwanted message traffic filtering and blocking capabilities through individually negotiated contracts. The Document suggests service providers allow consumers to report unwanted messaging traffic and develop an automated mechanism for collecting complaints about unwanted messages. Entities that send messages requiring consumer consent should offer a TCPA-complaint opt-in process and provide an option for that allows them to stop receiving such messages at any time.

The Document also provides guidance on how wireless messaging ecosystem participants should engage with each other to address unwanted messaging threats and regularly review and update control measures to ensure wanted messages are able to be delivered. Service providers should a) consult with one another openly and in good faith when a threat is identified; b) suspend the exchange of unwanted messages if all other available and practical controls fail to stop the traffic for only the maximum necessary time; c) may consider developing a unique identifier for enterprises that originate messaging traffic; and d) maintain a network operations center.

The Messaging Best Practices acknowledge that additional discussions will be necessary among wireless messaging stakeholders as further consideration is needed from details of service provider implementation and new use cases arise. As a result, it notes that CTIA’s Unwanted Messaging Traffic Threat Forum serves as the portal for North American wireless messaging stakeholders to engage with each other and manage threats to the wireless messaging ecosystem.

For additional information about the laws and rules relating to wireless messaging, please contact a member of Kelley Drye’s Communications Practice.