Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Mobile Messaging Best Practices for Political Programs in the United States

April 2020

The reference URL for this document is:
https://www.m3aawg.org/sites/default/files/m3aawg-mobile-messaging-bcp-political-programs-US-2020-04.pdf

For information on M3AAWG and other mobile-related anti-abuse work, please see www.m3aawg.org.

Table of Contents

1. Introduction

1.1. Objectives

The objectives of this document are to help maximize the successful delivery of wanted political text messages and minimize the incidence of unwanted and/or abusive political text messaging, while ensuring that the rights of all participants in political processes are respected. This document defines best practices that promote trust, transparency and collaboration among ecosystem providers.

1.2. Goals

- Protect wireless consumers from unwanted and/or abusive political messages.
- Ensure reliable delivery of wanted political messages.
- Maximize trust in messages and the messaging ecosystem.
- Promote transparency for wireless consumers, carriers, messaging aggregators, platform providers and political campaigns.
- Encourage uniform practices that improve ecosystem performance.
- Prevent or minimize adverse impacts on industry participants, and facilitate rapid and efficient investigation and resolution of suspected abuse.

1.3. Scope

The scope of this document is interoperable mobile messaging services, including mobile SMS, MMS, RCS and connected messaging services such as landline SIP services, that use a unique United States E.164 phone number as an account identifier and network address.

Note that in addition to this document's requirements and recommendations, additional recommendations, regulations and legal requirements may apply. These may include the Telephone Consumer Protection Act (TCPA), "M³AAWG Mobile Messaging Best Practices for Service Providers," and mobile carrier requirements.

1.4. Definitions

- **Campaign**: To avoid confusion, the term "campaign" in this document refers **only** to an organized course of action designed to influence voting in an election, or to sway public opinion for or against some political object. In this document, "campaign" does **not** refer to a program to send text messages to wireless consumers, though that is a common meaning of the word "campaign" within the wireless industry.
- **Carriers**: Telecommunications service providers that have the means to terminate messages to wireless consumers.
- **Message**: An SMS, MMS, or RCS message.
- **Message Sender**: Any organization or individual responsible for message content and initiation of sending messages to wireless consumers.
- **Provider**: Any platform or aggregator that allows messages to be transmitted to wireless consumers via the carriers.
- **Program**. A course of action that uses automation (other than consumer automation provided by mobile device messaging clients) to define recipients and/or assist in content specification which results in the transmission of text messages or a series of text messages to wireless consumers. This course of action is more commonly called a "campaign" within the wireless industry. The term "program" is used here to avoid confusion with political campaigns.
- **Wireless Consumer**: End-user, recipient, mobile subscriber who receives messages.

2. Political Message Definition

2.1. What is a Political Message?

For the scope of this document, a political message is one that attempts to influence the results of a federal, state or local government election, law, regulation and/or ballot measure in the United States of America. Some examples of political messages include messages that:

- Advocate a position on a specific candidate for political office, political party, political issue or a specific ballot measure (e.g. issuance of bonds, referendum, proposition, initiative, etc.).
- Communicate a candidate's viewpoints on government policy.
- Request donations to help fund a political activity.
- Seek a wireless consumer's participation in rallies for a candidate for office.

- Advocate, to establish, amend or repeal laws and/or regulations (e.g., immigration laws, gun laws, reproductive rights).

2.2. Exclusions

Some messages may share some elements of political messages as described in Section 2.1 above, but are not political within the scope of this document. However, such messages should also be compliant with general best practices for opt-in, opt-out, etc. These may include:

- Elections for union leaders, labor representatives,
- Broadly targeted informational messages designed solely to provide information about electoral processes, e.g. location and hours of polling places, voter registration, voting process, required forms of identification, blank sample ballots, etc., or
- Elections for non-governmental organizations such as school PTAs, homeowners associations, and non-governmental boards of directors.

3. Political Message Program Types and Message Sender Qualifications

3.1. Elections for Public Office

For messages pertaining to a candidate for election in the United States, i.e., an individual seeking election to an office listed on a government-issued election ballot (see section 2.1 above), the message sender must:

- Be sending messages on behalf of an entity/individual required to file a report with the appropriate election authority (e.g., Federal Elections Commission (FEC), State Board of Elections, etc.),
- Be a recognized corporation or organization legally recognized in the country targeted by its programs, and
- Send from a location within the United States or its territories.

3.2. General Advocacy

General advocacy messages (i.e., advocating to establish, amend or repeal laws or regulations) within the United States, must:

- Only be sent on behalf of an entity that
    - Possesses current and appropriate IRS tax-exempt status (see IRS Publication 557, "Tax-Exempt Status for Your Organization"), and/or
    - Is required to file a report with the appropriate elections authority (e.g., Federal Elections Commission (FEC), State Board of Elections, etc.), as applicable;
- Be incorporated in the United States, or have a subsidiary that is incorporated in the United States; and
- Be sending from a location within the United States.

4. Consent: Opt-in

Political message program guidelines require that the message sender obtain, from the consumer recipient, express written consent before sending any messages to that consumer's mobile device. Best practices for obtaining and memorializing a wireless consumer's consent to receive messages can be found in the CTIA "Messaging Principles & Best Practices."

Additional recommendations specific to political campaigns include the following:

4.1. Opt-in Exclusivity

Message senders should not use or allow other message senders to use opt-in lists that have been rented, sold or shared. Message senders should generate and manage their own opt-in lists by gaining the appropriate opt-in from the wireless consumer.

4.2. Reliance upon Opt-ins from Previous Campaign

Opt-ins obtained in a previous election campaign may carry over to a new election cycle as long as they are from the same organization. In jurisdictions in which carriers are not required to enforce laws related to consent, service providers may elect not to block non-malicious and predominantly-wanted message streams with no obligation to assume the burden of determining whether or not consent meets that jurisdiction's legal consent requirements.

4.3. Proof of Opt-in

Message senders should make a record of each wireless consumer's express written consent, consistent with guidelines set forth in CTIA's "Messaging Principles & Best Practices."

5. Revoked Consent: Opt-out

5.1. "STOP" Language

All programs must always honor opt-out requests (e.g. "STOP").

Once a wireless consumer opts out of messages, the wireless consumer should no longer receive messages related to that political campaign from the organization sending messages.

5.2. Deactivation File Processing

To ensure that messages are not sent to phone numbers that were cancelled by the wireless consumer user who initially opted in and subsequently reassigned to a new wireless consumer, message senders should process the Carrier Deactivation Files monthly.

5.3. Scope of Opt-out

Opt-out actions should, by default result in:

- The revocation of the broadest consent earlier given to the sender, and

- The revocation of consent to all senders that use the sending phone number or, if similar messages are sent from a pool, all senders using that pool of phone numbers.

However, if a consumer has consented to receive multiple types of messages (e.g., to receive messages sent supporting three candidates of a given political party by that party), the opt-out confirmation message may include options and/or instructions for narrowing the opt-out (e.g., opt-out only from messages related to a specific candidate).

5.4. Notice when Relying on Prior Campaign Opt-in

Message senders may rely upon a wireless consumer's qualified opt-in from a previous election cycle but the first message sent in the new election cycle should contain these elements:

- Specific reference to the previous campaign (e.g., "You supported us in 2018.").
- Opt-out language indicating how the wireless consumer can revoke consent at any time.

6. Sending Practices

6.1. Transparency

Messages should clearly identify the message sender, either by explicit identification within the message, or by ensuring the accuracy of caller ID mechanisms and widely-used reverse phone lookup mechanisms. Message senders should provide contact information to the provider through which messages are originated, and authorize the provider to forward this information to other providers and carriers on demand for the purposes of investigating or resolving suspected abuse.

6.2. Consent/Opt-in

Message senders should only send messages to wireless consumers who have provided consent/opt-in to receive messages from the message sender for the specific Political Message Program.

6.3. Revoked Consent/Opt-out

No messages other than one containing an opt-out confirmation should be sent to a wireless consumer who has revoked their consent. Opt-out requests should be fulfilled promptly.

6.4. Shared Numbers or Number Pools

Sending phone numbers, or number pools if more than one phone number is used, should be dedicated to a specific sender, and not shared by multiple senders. Senders should be mindful that the default scope of consumer opt-out messages is all messages sent from the sending number or number pool and all sending organizations using that pool.

6.5. Time-of-Day Restrictions

Messages should only be sent between the hours of 8:00 AM and 9:00 PM. Because the NPA (Area Code) of a wireless consumer's telephone number is no longer a reliable predictor of geographic area, message senders should make reasonable efforts to comply with these time-of-day restrictions.

7. Responsibilities of Message Senders

7.1. Creating Record of Consent

Message senders are responsible for obtaining, storing and managing all wireless consumer consent opt-ins for messaging programs they enable.

7.2. Compliance with Carrier Guidelines

Carrier-specific guidelines, which are usually derived from CTIA "Messaging Principles & Best Practices," referenced in Section 8 of this document, generally categorize political message programs as non-consumer application-to-person (A2P) traffic.

This M3AAWG Best Practices document supplements existing carrier-specific guidelines and policies for general A2P traffic. Although individual wireless carriers maintain individual business policies for A2P traffic. Although individual wireless carriers maintain individual policies for A2P traffic, carriers generally require compliance with the guidelines contained in the CTIA "Short Code Monitoring Handbook." These guidelines were originally developed for A2P programs using short codes, but the principles are applicable to all A2P programs irrespective of the specific identifier(short code, long code, toll-free, etc.) (short code, long code, toll-free, etc.) utilized.

7.3. Notice and Ability to Revoke Consent

Senders should ensure that consumers are notified that they may opt out by replying "STOP" or, where the message is a language other than English, a similar expression in the appropriate language. Senders are also responsible for receiving and acting appropriately on receipt of such a request by the consumer, i.e., the sender must cease messaging that consumer beyond a prompt opt-out confirmation message.

7.4. Providing Proper Notice of Changes in Phone Number(s)

If a political message program changes the phone number from which messages are sent, clear notice must be provided to wireless consumers so that they do not regard messages from a new (and unknown) number as spam.

- Notice should be sent from the retiring number informing wireless consumers that they will soon be receiving messages from a new number. Example: "Senator Smith will continue to keep you informed on important policy issues, but starting tomorrow they'll come from a new phone number, (800) 555-1212."

- A message from the new number should follow the initial message sent from the retiring number within 24 hours.

8. References

1. "M3AAWG Mobile Messaging Best Practices for Service Providers"
2. IRS Publication 557, "Tax-Exempt Status for Your Organization"
3. "CTIA Messaging Principles and Best Practices," July 2019.
4. (CTIA SCM) "CTIA Short Code Monitoring Handbook v1.7," 27 March 2017.
5. "FCC Enforcement Advisory: Robotext Consumer Protection," 18 November 2016.

As with all documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates.

M3AAWG-133