Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matters of	)	
	)	
Targeting and Eliminating	)	CG Docket No. 21-402
Unlawful Text Messages	)	
	)	
Rules and Regulations	)	CG Docket No. 02-278
Implementing the	)	
Telephone Consumer	)	
Protection Act of 1991	)	

COMMENTS OF THE MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP (M^{3}AAWG) ON THE NOTICE OF PROPOSED RULEMAKING

I. Introduction

The Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) is pleased to offer comments on the Further Notice of Proposed Rulemaking (FNPRM), Federal Communications Commission (FCC) 22-72, CG Dockets No. 21-402 concerning Targeting and Eliminating Unlawful Text Messages and No. 02-278 concerning Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 released on March 17, 2023.

M[3]AAWG is a technology-neutral global industry association. As a technical working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 members worldwide, we bring together stakeholders in the online community in a confidential, open forum, developing recommendations, best practices, and cooperative approaches for mitigating online abuse.

The FNPRM seeks comments on four topics. Two of these are proposals to extend Do-Not-Call (DNC) and TCPA's consumer consent regulations in ways that will help combat illegal and unwanted text messages. M[3]AAWG fully supports these proposals and believes that they are technically sound and in the best interests of the public text messaging ecosystem.

A third proposal is to require terminating mobile wireless providers to, on notice from the Commission, investigate and block certain illegal text messages. US wireless providers are notably active and agile in voluntarily blocking unwanted and/or illegal messages in response to consumer complaints, government inputs (e.g., from the Cybersecurity and Infrastructure Security Agency) as well as threat intelligence collection points open to public submission (e.g., those of various commercial spam filter vendors). We urge the Commission to consider that industry is expert at defining which messages to block and how to block them, and can do so more rapidly and accurately without additional processes needed for mandatory blocking. We recommend the Commission focus instead on fostering greater intelligence sharing among private industry, consumers, and the telecommunications providers. We also note that unwanted or illegal messages can originate from foreign sources and urge the Commission to coordinate with relevant federal government and international stakeholders to address these originating sources.

A fourth area concerns the ability to identify (e.g., through what the rulemaking terms "authentication") message sources and to take action against the sources of messages so identified. M[3]AAWG respectfully suggests that the Commission need not focus on additional message source authentication processes because highly effective anti-spoofing mechanisms are already in place.

In addressing these questions, we found indications that optimal rulemaking would be facilitated by additional information on how the text messaging ecosystem functions, and, in particular on the many important differences between voice and text messaging ecosystems. This information is beyond the scope of our written comments. However, M[3]AAWG would welcome the opportunity to

offer the Commission – in the form of a meeting or seminar, for example – more detailed information on the workings of the text messaging ecosystem, typical abuse cases, and the processes and technologies currently in place to fight abuse, and on areas (e.g., threat intelligence sharing and mitigating identity impersonation) for further government/industry action and collaboration.

In the following paragraphs, we offer more detailed comments.

II. Detailed Comments

1. Explicit Consent Regulations

M[3]AAWG supports regulations requiring that consent to receive messages apply only to messages that fall within any subject matter constraints of that consent. We further suggest that any such regulations prohibit messaging that goes beyond explicitly named senders or the scope of the original consent. Parties and terms of consent should be prominently displayed and distinct action required to affirm consent. It should be noted that CTIA's Messaging Principles & Best Practices [https://api.ctia.org/wp-content/uploads/2019/07/190719-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf] recommend, in Section 5.1, that consent not be transferable or assignable, and "apply only to the campaign(s) and specific Message Sender for which it was intended or obtained."

The FNPRM asks for information on the extent of this issue. The problem is not limited to cases of "consent creep" beyond the original scope; there are many cases where there may be false or difficult-to-disprove claims of such consent. Third parties may falsely claim to have received permission to send to a recipient, but those consent claims may be difficult or impossible to refute. Many unwanted messages are sent by parties claiming to have received consent from an affiliated organization. Leads are also often sold to unnamed third parties with the seller claiming to have permission for the purchaser to send to that address.

We do not find this to unfairly burden comparison shopping websites; such websites must simply explicitly identify any parties from whom the recipient is consenting to receive messages from. If, some time after receiving information from a consumer, a comparison website operator

would like to obtain consent for additional parties to send, it is free (provided the operator has consent to send such suggestions) to send messages soliciting any additional consent. We feel that this is necessary to allow consumers to retain control of their inboxes by stopping floods of unwanted messages from affiliates in cases where the consumer may not remember nor have a way of identifying the party to whom initial "transitive" consent was granted.

2. Do-Not-Call Protections

M[3]AAWG wholly supports extending Do Not Call to the text messaging space. While this places an additional **regulatory** consent burden on senders, CTIA's Messaging Principles & Best Practices, adopted as contractual requirements by all leading U.S. wireless providers, already recommend that consent be required for marketing texts. Thus, senders already have a duty to obtain consent, a reasonable burden necessary to control unwanted marketing communications, and are already collecting such consent, as stated above.

3. Blocking Orders

The Commission should not require terminating wireless carriers to, upon notice, investigate and potentially block illegal text messages. Industry has numerous active means of collecting threat intelligence and is highly receptive to consumers' and especially trusted parties' (including government's) inputs. Industry currently solicits and processes many millions of such inputs daily, knows how to evaluate these data, and often reacts by blocking in under 60 seconds.

Due to industry's agile defenses, mobile spam content and sending numbers now evolve exceedingly quickly. Phone numbers, internet domains and/or message text may differ from message to message, and many attacks last less than one minute. By the time a notice is issued to block specific content and/or numbers and a wireless provider's mandated analysis and investigation is completed by a carrier, it is already too late. The campaign is likely be over, and/or to have switched to new content and sending addresses.

Orders to block "substantially similar" attacks could place carriers in the difficult position of blocking neither too few nor too many messages. Attackers are adept at varying content, often with no two messages having more than several consecutive words in common. Notice that "substantially similar" content is subjective. What may appear to be "substantially similar" to a

human may be impractical for automated filter technology to accurately classify. Attempts to most accurately match blocking to orders leads to both leakage and overblocking. Precisely blocking illegal clusters of related yet unique messages without blocking wanted messages is complex to implement. Care is needed to prevent overblocking. Further complicating this are questions regarding the appropriate duration of blocks and scope of blocks (e.g., specified content from all phone numbers, or only from certain known-offending service providers). It is difficult to foresee how better results could be obtained from mandated blocking than from flexible, expertly defined voluntary blocking by motivated carriers.

To help increase the effectiveness of defenses, the Commission should instead facilitate collaboration such as intelligence sharing between victims, private industry, telecommunications providers and the government. This will assist with the rapid identification and disruption of illegal messages, while also supporting appropriate government engagement if a service provider is found to act in a complicit or negligent manner. When highly organized criminal activity resistant to technical defense methods (e.g., message filters) is identified, the Commission and other government organizations can and should assist with regulatory and/or criminal enforcement as appropriate.

4. Authentication and Action Against Complicit or Negligent Service Providers

As numerous comments in CG Docket 21-402 state, spoofing the sending phone number is not a significant issue for consumers. The U.S. mobile text messaging and voice telephony ecosystems differ significantly. **Although phone number spoofing is a major issue in voice calling, it is nearly absent in U.S. text messaging.** Nearly all illegal and abusive text messages originate from valid phone numbers sent by a party who has access to the corresponding sending account. There is no need for mandating technologies to identify what is already generally known – that is, the true service provider and customer phone number that originated a text message.

Most service providers, wireless and non-wireless, have effective programs to prevent the sending of illegal messages, including Know-Your-Sender programs, monitoring, and feedback loops. However, there are cases where a potentially negligent (or complicit) service provider sends a disproportionate number of illegal messages. Indeed, M^{3}AAWG member companies

confirm that there are currently some notable entities of this sort. Downstream service providers are willing and able to take actions necessary to protect consumers from those illegal messages. These actions are appropriately rapid and precise, including blocking of messages, message campaigns, phone numbers, and occasionally even blocking a complicit service provider.

We urge the Commission to consider that it is in the consumers' best interests to allow different blocking policies to be applied to different messaging streams in order to optimize blocking accuracy, thus minimizing the delivery of illegal messages and the mistaken blocking of legal and wanted messages.

Service providers that are disproportionate sources of illegal messages are best identified through consumer complaints, which may be accessed via industry referrals to the Commission and/or the Commission's investigative processes.

III. Conclusion

M^{3}AAWG generally supports the FCC's proposals to enhance DNC protections and TCPA consent requirements as outlined in the comments above. M^{3}AAWG urges the Commission to continue to allow the industry the necessary flexibility to rapidly and accurately protect consumers from illegal messaging – flexibility that mandatory blocking notices could erode. With messaging technology rapidly advancing and abuse tactics morphing on what is sometimes a minute-by-minute basis, the messaging industry's defense agility needs to match that of the attackers. It is critical that each defender of the messaging ecosystem be afforded flexibility to ensure that text messaging remains a trusted and reliable medium of communication.

And finally, existing industry originating-provider identification and anti-spoofing methods and processes robustly identify the sources of illegal text messages. Carriers can and do block messages from identified phone numbers and occasionally even complicit service providers in order to protect consumers from illegal messages. Additional originating-provider authentication would not significantly enhance the protection of consumers from illegal and unwanted text messaging. Such mandates might actually encumber or prevent the implementation of more effective industry defense processes and mechanisms.

We encourage the Commission to rely on, promote, and facilitate voluntary industry and consumer action through education; to enact regulations that permit and even empower collaboration wherever possible; and to encourage any actions that can foster increased collaboration.

Thank you for the opportunity to submit these comments. We will be glad to respond to any questions. Please address any inquiries about our comments or work to M^{3}AAWG's Executive Director, Amy Cadagin.

Sincerely,

Amy Cadagin
Executive Director, Messaging Malware Mobile Anti-Abuse Working Group
P.O. Box 9125
Brea, CA 92822
comments@m3aawg.org