Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Petition of Public Knowledge et. al for Declaratory Ruling Stating Text Messaging and Short Codes are Title II Services or are Title I Services Subject to Section 202 Nondiscrimination Rules	))))	WT Docket No. 08-7

To: The Commission

OPPOSITION OF CTIA – THE WIRELESS ASSOCIATION®

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Brian M. Josef
Assistant Vice President, Regulatory Affairs

CTIA – THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036

November 20, 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Twilio frames its Petition as an effort to curb what it calls the "blocking" and "throttling" of messaging traffic but in fact, Twilio is asking the Commission to invalidate consumer-protection measures that prevent massive quantities of unlawful and unwanted mobile messaging spam from reaching and harming consumers. Wireless provider messaging practices are designed to protect consumers, not restrict them, and in the past Twilio has recognized the value of these measures. Its call to subject mobile messaging to Title II common carriage requirements is the wrong policy and wrong on the law. At its core, Twilio's request is for the Commission to require mobile operators to cease using spam filters and to instead deliver every message that seeks to defraud, trick, and abuse end-user customers. Such regulatory maneuvering directly serves Twilio's interests, as the company's business model clearly reflects that the more traffic Twilio sends, the more profit Twilio generates. In the world Twilio seeks, Americans' mobile phones and messaging services would be subject to as much frivolous and exploitive content as Americans' email inboxes are. The Commission should place the needs of consumers over the demands of those that seek unfiltered, high-volume messaging models (including spammers). It must, in other words, deny Twilio's Petition.

The mobile messaging marketplace has grown exponentially since the service was first introduced. In all of 2000, Americans sent a total of roughly 170 million messages. Wireless provider-offered messaging now accounts for more than *two trillion* messages per year, and over-the-top ("OTT") messaging applications have been wildly successful. Today, the total messaging volume of a *single* app, WhatsApp, is 50 percent larger than the messaging volume of the entire wireless provider-offered text messaging market.

Mobile messaging's huge popularity is due in part to its status as a largely spam-free and trusted communications environment. But with messaging's popularity comes the constant risk of unwanted and unlawful communications. As one security solutions provider observed of the messaging ecosystem, "[a]lways-on communications, inherent trust in the channel, high open rates, and six billion subscribers are not lost on those with ill intent." Wireless providers work relentlessly to ensure that messaging benefits consumers and does not subject them to spam or otherwise harmful traffic. In the context of person-to-person ("P2P") messages, sent using ten-digit telephone numbers, providers employ robust spam filtering software, "account fingerprinting" techniques to identify accounts that are sending high volumes of messaging traffic with little or no voice or data usage, and other tools. With P2P traffic, any genuine wireless consumer can send a message to another user without concern that the message will be denied because of its content.

Wireless providers developed the Short Code program to facilitate the delivery of lawful, albeit high-volume, Application-to-Person ("A2P") traffic while ensuring that users remained protected from massive quantities of unwanted traffic. The Short Code program facilitates easy-to-use A2P messaging while protecting against the spam threat that A2P enables. This program involves a provider-by-provider review process that takes place when a content provider seeks a Short Code. Best practices developed by CTIA are designed to ensure that a campaign does not promote illegal or illicit or otherwise inappropriate content. Notably, a campaign may only send messages to users who have opted to receive such communications and must respect user

decisions to opt out of any future messages. The program calls for regular audits and penalties for violations of the terms of the approved campaign.

These wireless industry efforts to combat spam and unwanted messages have been remarkably effective given the scope of the problem, as the level of messaging spam is minimal in comparison to email. The Commission has taken notice, commending "carrier efforts to implement protections against unwanted text messages" in its recent order under the Telephone Consumer Protection Act ("TCPA") on robocalls and unwanted text messages.

Recently, the messaging environment has faced new opportunities and new challenges arising from cloud-based "hybrid" traffic, which involves automated systems sending huge volumes of messages via ten-digit phone numbers rather than Short Codes. Such traffic is not subject to the content review and pre-approval associated with the Short Code system, and may be caught by traditional P2P spam filters. The threat of unwanted or harmful traffic delivered via hybrid business models is real, and Twilio itself has been a conduit for spammers to exploit wireless consumers. Indeed, it is precisely *because* Twilio and other hybrid providers offer ten-digit mass-messaging as an alternative to Short Code program review that they are appealing to bad actors.

For the past year, under CTIA's auspices, the messaging community (including Twilio) has been working to address whether and how cloud-based messaging traffic under a hybrid model can be integrated into the existing ecosystem without exposing consumers to greater risk of spam and unwanted or harmful messages. Consistent with the consensus-based, inclusive industry processes that have governed messaging from its earliest days, the messaging industry formed several working groups charged with addressing the issues presented by hybrid traffic. This is a far better course than pursuit of Title II.

The result Twilio seeks – Title II classification of messaging and Short Codes – would upend efforts to restrict unwanted messages and protect consumers. If wireless provider-offered messaging were a common carrier service, providers would be hamstrung in their efforts to filter unwanted traffic and provide a curated A2P experience for their end users, unleashing a flood of unwanted and/or unlawful traffic. Provisions such as Section 201 and 202 of the Communications Act ("Act") could preclude mobile providers from halting traffic that is unwanted by consumers, but not *per se* illegal. It could also chill wireless provider filtering and curating efforts by threatening to subject providers to intensive inquiries as to whether a choice to transmit one message but not another constituted unreasonable discrimination. This result risks unleashing a Pandora's Box of new mobile messaging threats, creating consumer "text fatigue" and thus diminishing – not enhancing – the medium's utility, including its role in notifying consumers of critically important events.

Grant of the Petition also would subject competing messaging services to disparate regulation. Twilio asks the Commission to subject only a single subset of messaging providers – mobile providers – to the strictures of Title II. Given the similarities among wireless provider-offered and OTT messaging, IM, and email, any effort to treat messaging differently than these services for regulatory purposes would inevitably lead to arbitrary line drawing and distort the natural development of the marketplace.

The Commission must also reject Twilio's Petition as a matter of law. Twilio asks the Commission to subject "short-code-based services" to common carrier regulation under Title II, but its arguments reflect a fundamental misunderstanding of Short Codes, which are not a communications service at all. When a mobile provider sells access to a Short Code, the product being sold is an addressing, billing, and marketing tool, and *none* of these functions involves the transmission of information. Accordingly, Short Codes are neither telecommunications nor a telecommunications service.

Likewise, the Commission must reject Twilio's contention that SMS and MMS are telecommunications services subject to common carrier obligations under the Act. The characteristics of mobile messaging necessarily make it an information service under the Act, not a telecommunications service. Much like other asynchronous services such as email and voicemail, in which users send messages that are stored until the recipient accesses them, mobile messaging involves data storage and computer processing that changes both the form and content of messages. These core information-service functions cannot be separated from messaging's transmission functionality. Furthermore, because messaging is an information service and does not make "interconnected service" available to the public switched network, it cannot be a commercial mobile radio service ("CMRS"). Nor is mobile messaging the functional equivalent of CMRS. None of the precedent that Twilio cites alters these conclusions.

Finally, there is no legal basis for mandating direct interconnection between messaging providers. Information services are not subject to interconnection requirements of any kind, and even telecommunications service providers are only required "to interconnect directly *or indirectly* with the facilities and equipment of other telecommunications carriers."

For these policy-based and legal reasons, the Commission should deny Twilio's Petition.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Petition of Public Knowledge et. al for Declaratory Ruling Stating Text Messaging and Short Codes are Title II Services or are Title I Services Subject to Section 202 Nondiscrimination Rules	))))	WT Docket No. 08-7

To: The Commission

OPPOSITION OF CTIA – THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association® ("CTIA") hereby opposes the Petition for Expedited Declaratory Ruling filed by Twilio Inc. and placed into the above-referenced docket.[1]

I. INTRODUCTION.

The messaging environment has changed and grown dramatically since its inception, but one thing has remained constant: Wireless providers work relentlessly to ensure that messaging benefits consumers and does not subject them to spam or otherwise harmful traffic. Mobile network operators currently have the flexibility to address these risks, and their efforts have helped make messaging the most popular and trusted communications medium: In 2014, Americans sent over 2 *trillion* individual SMS and MMS messages.[2]

Twilio's call for Title II classification of SMS (text messaging), MMS (multimedia messaging) – and even the distinct Short Code system used to manage and facilitate certain high-

[1] Petition for Expedited Declaratory Ruling of Twilio Inc., WT Docket No. 08-7 (filed Aug. 28, 2015) ("Petition").

[2] Dr. Robert F. Roche & Kathryn Malarkey, *CTIA's Annual Wireless Industry Indices: Annual Wireless Survey Results: A Comprehensive Report from CTIA Analyzing the U.S. Wireless Industry*, CTIA, at 144 (Sept. 2015) ("Roche & Malarkey").

volume messaging – would eliminate core protections that safeguard consumers and risks forcing wireless providers to deliver millions of unwanted, uninvited, harassing, obnoxious, and outright unlawful messages to their customers. There is no mystery as to why Twilio, which earns more revenues the more messages its commercial customers send, would benefit from the regime it seeks. What *is* unclear is why the Commission would undermine consumer interests by opening the floodgates to a tidal wave of unwanted messaging traffic.

Further, Twilio's call to classify wireless provider-offered messaging services as telecommunications services would create arbitrary distinctions between those offerings and the wide range of wildly popular third-party messaging offerings that are substitutes for these services. These include competitive over-the-top ("OTT") messaging services, Instant Message ("IM") platforms, and even email, none of which would be subject to Title II's demands even under Twilio's proposal. This result would further disserve customers by artificially privileging some messaging offerings over others, placing a heavy thumb on the competitive scale. In any case, Twilio's request for classification has no basis in the law: Even under the terms of the *2015 Open Internet Order*,[3] messaging services are integrated information services, not distinct telecommunications offerings. And Short Codes are not communications services at all, much less telecommunications services.

CTIA believes that technological advances in messaging, as elsewhere, hold much promise for consumers, but they also pose new threats. New mass-messaging technologies and falling prices have provided spammers an increasingly strong platform to work from, and they

[3] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) ("*2015 Open Internet Order*").

have eagerly exploited these new capabilities – including, notably, the services offered by Twilio itself – to distribute phishing scams and other harmful, unwanted, and unlawful traffic.

As the mobile messaging marketplace evolves, CTIA has brought together the different parties that constitute the messaging ecosystem – including Twilio – to identify ways to introduce new business models while continuing to safeguard U.S. consumers from unwanted or unlawful messaging traffic. Even if the FCC had authority to grant Twilio's Petition, this is a far better course than Title II. CTIA therefore urges the Commission to keep consumers at the heart of its mission, and to deny Twilio's Petition in full, along with the Public Knowledge petition also at issue in this proceeding.

II. WIRELESS PROVIDER MESSAGING PRACTICES ARE DESIGNED TO PROTECT CONSUMERS, NOT RESTRICT THEM.

The fundamental premise of Twilio's claim – that wireless providers manage access to messaging offerings in a way that harms consumers – could not be further from the truth. Since the inception of mobile messaging, wireless providers have built upon the utility of messaging offerings while protecting consumers from unlawful and unwanted traffic. These efforts continue today as the messaging ecosystem, including wireless providers, works together to identify new messaging opportunities and preserve a marketplace that is remarkably effective in limiting the waves of spam and other pernicious traffic that characterize (for example) email.

When mobile messaging first arose, all traffic was sent from one wireless consumer to another – commonly known as "person to person," or "P2P," messaging – using ten-digit telephone numbers. With P2P traffic, any genuine wireless consumer can send a message to another user without concern that the message will be denied because of its content. As a practical matter, the pure P2P environment poses little risk of high-volume spam as no human can send 1 message per second, much less thousands of messages per second.

Automation, however, changed things, bringing high-volume traffic to the messaging world. Mass messaging (often referred to as "application-to-person," or "A2P") technologies enable commercial enterprises and other entities to send thousands of messages per second. As discussed further below, many commercial message campaigns advance consumer welfare and reflect lawful, appropriate uses of messaging on Twilio and other messaging platforms. But mass messaging technologies also open the risk of massive volumes of unwanted and unlawful messages. They facilitate the transmission of spam, phishing attempts, links to viruses and other malware, obscene or otherwise pornographic photos, and commercial traffic that a user has not agreed to receive.

The fact that most P2P and A2P messaging traffic is largely desired by consumers and lawful is not an accident, nor is it the result of restraint on the part of bad actors. Rather, it is due in large part to very active efforts undertaken by wireless providers. As described in more detail below, P2P spam filters help to prevent much of the malicious automated traffic from getting to consumers. The Short Code program, likewise, facilitates the delivery of lawful A2P traffic while ensuring that consumers remain protected from massive quantities of unwanted traffic. Although the Twilio Petition attempts to characterize these wireless provider efforts as "call blocking,"[4] its website provides a far more accurate assessment:

> Carriers want to protect their subscribers from spam, and will only grant bulk messaging capabilities to applications that they've screened and approved. This is why there are traffic limits for long codes, and an approval process for short codes.[5]

[4] Petition at 2 *et al.*

[5] Laura Schaffer, *Short Codes, Big Lessons: Make The Most Of Your Short Code*, TWILIO BLOG, (Dec. 3, 2014), https://www.twilio.com/blog/2014/12/short-codes-big-lessons-make-the-most-of-your-short-code-nt.html ("Twilio Short Code Blog").

Just four months ago, the Commission commended provider efforts to protect consumers against unwanted messages, noting that it has been "encouraged by carrier efforts to implement protections against unwanted text messages …."[6]

New "hybrid" business models, like certain Twilio lines of business, have arisen for the delivery of mobile messages, presenting new opportunities for enhancing consumer welfare – but also exposing new risks. These hybrid models typically involve the transmission of high-volume A2P messages, but do so through means traditionally used to send P2P traffic – ten-digit telephone numbers – not through the Short Code system. Some contain mechanisms to prevent spam abuse, but they are the exception. Hybrid traffic often is not subject to the type of content review that limits spam in the Short Code environment.

To be sure, Twilio is the source of much legitimate traffic,[7] and while much of its marketing focuses on its ability to send automated and high-volume messages with Short Codes "send[ing] up to 30 messages per-second,"[8] it also states, "[i]f you need to send more than 30 messages per-second please contact our sales team."[9] The company's business model clearly establishes that the higher the volume of traffic Twilio sends, the more profit Twilio generates.[10] With these policies and incentives in place – and no apparent checks against spam – it is no

---

[6] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, et al.*, Declaratory Ruling and Order, 30 FCC Rcd 7961, 8021 ¶ 119 (2015) ("TCPA Declaratory Ruling and Order").

[7] *Twilio Short Code Blog* (stating that Twilio is the largest holder of Short Codes in the industry, the fastest growing provider of Short Codes, and the provider with the most active Short Codes).

[8] Twilio, What are the limits on outbound calls and SMS messages per-second? https://www.twilio.com/help/faq/twilio-basics/what-are-the-limits-on-outbound-calls-and-sms-messages-per-second (last visited Nov. 19, 2015).

[9] *Id.*

[10] Twilio, Messaging Pricing, https://www.twilio.com/sms/pricing (last visited Nov. 19, 2015).

surprise that Twilio has attracted some bad actors in addition to legitimate customers. In February 2014, Cloudmark reported news of "an SMS phishing attack aimed at the customers of several large mobile providers in the US," in which malicious messages were sent through Twilio via traditional P2P mechanisms to "[m]ore than a quarter of a million mobile users."[11] Investigation revealed that more than 90 percent of the numbers involved were provisioned by Twilio. Recipients of the fraudulent messages were urged to click on a link provided in the message to receive an account credit or a discount on services from their wireless provider. Those who did were asked to sign on using their pre-established user ID and password – information that the party behind the attack could then use to take control of the account.[12] Perhaps needless to say, this type of attack would almost surely have been prevented if the traffic at issue had been subject to the Short Code review process. Indeed, one observer asked rhetorically why "spammers love Twilio so much," and then answered: "[I]t's because they use long codes for messaging"[13] – *i.e.*, they send mass messages through the P2P system, which does not involve any *ex ante* content review. It was not Twilio's first experience serving as the conduit for spam: It had previously been sued for transmitting unsolicited long-code text

[11] *SMS Phishers Exploit Twilio and ow.ly to Steal Mobile Account Logins*, CLOUDMARK SECURITY BLOG (Feb. 13, 2014) (emphasis omitted), http://blog.cloudmark.com/2014/02/13/sms-phishers-exploit-twilio-and-owly-to-steal-mobile-account-logins/ ("Cloudmark Article"). *See also* Derek Johnson, *SMS Spammers Exploit Twilio – Send 385,000 Spam Text Messages*, TATANGO (Feb. 13, 2014) http://www.tatango.com/blog/sms-spammers-exploit-twilio-send-385000-spam-text-messages/ ("Johnson").

[12] *See* Cloudmark Article.

[13] *See* Johnson.

messages from GroupMe[14] – ironically, one of the very companies whose success Twilio cites as a rationale for granting its Petition.[15]

Thus, as Twilio and others have sought to develop hybrid A2P messaging models, challenges have arisen that threaten the current, spam-limited messaging environment that consumers enjoy today. As described below,[16] CTIA and wireless providers have sought to address those challenges in a way that safeguards consumers while enabling Twilio to pursue a business model of facilitating mass A2P messaging. Among other things, earlier this year CTIA initiated a dialogue between all of the players in the messaging ecosystem, including Twilio, to refine best practices and otherwise find industry-based solutions. Now Twilio asks the Commission to sharply curtail wireless providers' efforts to combat unwanted messaging traffic – to impose traditional Title II common carriage regulation on SMS, MMS, and Short Codes and to eliminate the Short Code review process that prevents a tidal wave of malicious traffic from flooding the messaging ecosystem. Even if Twilio's Petition were not bankrupt as a matter of law – which, as discussed below, it is[17] – the Title II framework that it seeks would upend each wireless provider's efforts to limit unwanted traffic in the messaging ecosystem. The Commission should ensure that, as the marketplace evolves, wireless providers remain capable of protecting consumers from an onslaught of unwanted and/or objectionable traffic.

At its core, Twilio's requested relief is to require mobile operators to cease using spam filters and deliver every message to consumers that seeks to defraud, trick, and abuse end-user

---

[14] *See generally* Derek Johnson, *Twilio Continues to Send SMS Spam, Even After Lawsuit*, TATANGO (Apr. 9, 2012), http://www.tatango.com/blog/twilio-continues-to-send-sms-spam-even-after-lawsuit/.

[15] *See* Petition at 5.

[16] *See infra* Parts III & IV.

[17] *See infra* Part VI.

customers. It would subject Americans' smartphones to the same degree of frivolous and exploitive content that many Americans' email inboxes are subject to today, and would effectively inhibit the ability of banks to alert customers that they've been defrauded, schools to announce closings or provide notice of emergency measures, or airlines to update flight status. This may benefit Twilio, and those that wish to misuse the messaging platforms, but it is hard to see how this is in the public interest.

III. SMS IS MASSIVELY POPULAR BUT SPAM AND OTHER UNWANTED OR HARMFUL MESSAGES PUT THE MESSAGING ECOSYSTEM AT RISK.

A. Messaging is Increasingly the Most Popular and Trusted Way to Communicate.

Messaging has become today's most popular way to communicate. According to a 2015 Pew Research Center study, "[t]ext messaging is the most widely-used smartphone feature," and "is also the most *frequently-used*."[18] Back in 2000, roughly 170 million messages were sent the entire year; by 2001, on average more than 252 million texts were sent *per month*.[19] And by 2011, volumes were nearly 1000 times greater, reaching over 193 *billion* messages per month. In 2014, Americans sent over 2 *trillion* individual SMS and MMS messages.[20] Of course, beyond wireless provider-offered messaging, OTT messaging apps have been wildly successful. In 2014, OTT texting apps surpassed SMS in terms of volume.[21] Today, the total messaging

---

[18] *U.S. Smartphone Use in 2015*, PEW RESEARCH CENTER, at 8, 33 (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. Nearly all of the smartphone owners in the Pew survey (97 percent) used text messaging during the study period, and they used their devices for texting more than email or Internet use or calling.

[19] Roche & Malarkey at 135-36.

[20] *Id*. at 144.

[21] *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications*, Policy Statement and Second Further Notice of Proposed Rulemaking, 29 FCC Rcd 1547, 1550 ¶ 6 (2014) ("*911 Policy Statement & Second FNPRM*") ("In mid-2013, the six most popular

volume of a *single* app, WhatsApp, is 50 percent larger than the messaging volume of the entire SMS market.[22]

Reliance on messaging, moreover, is likely to become even more pronounced over time. A 2014 Gallup poll concluded that texting is the main method of communicating for Americans under 50.[23] In 2012, the latest year for which statistics are available, smartphone users aged 18 to 24 sent approximately 67 texts every day, compared to 18 texts per day for users aged 45 to 54.[24] Another Pew Research Center study found that for 58 percent of teens with smartphones, texting is already their primary method to keep in touch with close friends.[25]

Notably, Americans view messaging as a highly accessible – and trusted –medium, and this trust is largely due to the fact that "the majority of text messages are clean of any harmful content."[26] Network security provider Cloudmark reports that the SMS "open rate" is more than 90 percent and that texts are generally opened within 15 minutes of receipt – email, in contrast,

---

mobile chat applications averaged nearly 19 billion messages each day, compared to 17.6 billion SMS messages.").

[22] *See* Benedict Evans, *WhatsApp sails past SMS, but where does messaging go next?*, BENEDICT EVANS (Jan. 11, 2015), http://ben-evans.com/benedictevans/2015/1/11/whatsapp-sails-past-sms-but-where-does-messaging-go-next.

[23] Frank Newport, *The New Era of Communication Among Americans*, GALLUP (Nov. 10, 2014), http://www.gallup.com/poll/179288/new-era-communication-americans.aspx.

[24] *See* Alex Cocotas, *CHART OF THE DAY: Kids Send a Mind Boggling Number of Texts Every Month*, BUSINESS INSIDER (Mar. 22, 2013), http://www.businessinsider.com/chart-of-the-day-number-of-texts-sent-2013-3.

[25] *How Having Smartphones (or not) Shapes the Ways Teens Communicate*, PEW RESEARCH CENTER (Aug. 20, 2015), http://www.pewresearch.org/fact-tank/2015/08/20/how-having-smartphones-or-not-shapes-the-way-teens-communicate/ (also finding that 73 percent of teens have a smartphone).

[26] *Global Security Insights for Mobile: 6, Ultimate Network Defence – Fighting the Rising Tide of SMS spam*, ADAPTIVE MOBILE, at 2.

has an open rate of 20-25 percent within 24 hours of receipt.[27] Consumer reliance on texting, and its remarkably high open rate, are due in large part to the very low incidence of unwanted messages. Of course there is some element of SMS spam, but messaging is far less "polluted" than email, which as consumers all know has far more prevalent spam and pernicious, unwanted traffic: By some estimates, two-thirds of email is spam and only one percent of SMS is spam.[28]

Commercial entities and other organizations have seized on messaging as a means to break through the noise and reach consumers. For example, A2P traffic facilitates communications from airlines needing to contact their customers, many of whom may, at the time the message is sent, already be on their way to the airport and thus fully reliant on mobile devices.[29] Financial institutions rely on text messaging to alert consumers of potential fraud.[30]

---

[27] *SMS Spam Overview: Preserving the value of SMS texting*, CLOUDMARK, https://www.cloudmark.com/en/s/resources/whitepapers/sms-spam-overview (last visited Nov. 17, 2015).

[28] *See e.g.*, Maria Vergelis, *et. al*, *Kaspersky Security Bulletin. Spam in 2014*, Securelist (Mar. 12, 2015), https://securelist.com/analysis/kaspersky-security-bulletin/69225/kaspersky-security-bulletin-spam-in-2014/ (reporting spam amounted to 66.76 percent of email in 2014, with U.S. being targeted by 9.8 percent of the world's malicious emails, the largest share of any country). By contrast, it has been reported that 1 percent of SMS marketing messages are spam. *See* Aline Doherty, *SMS Versus Email Marketing*, BUSINESS2COMMUNITY (July 28, 2014), http://www.business2community.com/digital-marketing/sms-versus-email-marketing-0957139#!bth7SG#CcOT53BPhyU6jqFi.97.

[29] *See* Dan Butcher, *How Travel, Tourism, and Hospitality Companies Can Use SMS*, NEUSTAR 4-5, https://www.neustar.biz/enterprise/docs/whitepapers/digital-marketing/how-travel-tourism-and-hospitality-companies-use-sms.pdf (offering several case studies on airline uses of SMS) (last visited Nov. 19, 2015); *see also* QUANTITATIVE PROBLEM SOLVING METHODS IN THE AIRLINE INDUSTRY: A MODELING METHODOLOGY HANDBOOK 348-50 (Cynthia Barnhart & Barry Smith eds., 2012) (explaining the value of regular communications, including text message, to consumers in handling small disruptions like delays, and not just major irregularities); Hilary Howard, *Google Offers Flight Information by Text Message*, N.Y. TIMES (Apr. 8, 2007), http://www.nytimes.com/2007/04/08/travel/08transgoogle.html (highlighting the utility of flight status updates via text for on-the-go travelers as early as 2007).

[30] *See, e.g.*, U.S. Senate Fed. Credit Union, SMS Guardian: For Your Piece of Mind – Text Alert Fraud Prevention, https://www.ussfcu.org/services/sms/ (last visited Nov. 18, 2015) (allowing

Content providers use A2P interfaces to facilitate "two-factor" authentication by sending access codes to a consumer's pre-established phone number to be used in conjunction with a preset password or other means of identification.[31] Messaging is also used by doctors' offices, concert venues, online retailers, and others to inform or remind consumers of appointment times, upcoming events, scheduled deliveries, and so on.[32] And A2P offerings enable customers to contribute funds to aid recovery efforts following earthquakes, tsunamis, and other natural disasters, with charges being billed through the mobile provider.[33] These are just a few of the ways that A2P messaging has expanded opportunities and provided value to consumers. So long as the messages described here are lawful and delivered with the customer's consent, they both

---

users to voluntarily sign up for fraud protection text alerts, including the ability to cancel a charge or stop the alerts simply by responding); Honor Credit Union, Debit Card – Text Fraud Alerts, https://www.honorcu.com/security-center/debit-card-text-fraud-alerts (also offering users the chance to text "NO" in response to a received alert, cancelling the fraudulent transaction 24/7).

[31] *See, e.g.*, Chase, What is Multifactor Authentication?, https://m.chase.com/?nodeid=1&itemid=2 (last visited Nov. 18, 2015) (explaining the importance of two-source identification for secure login, and the availability of text message second-factor authentication); *see also* Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 268 (2013) (arguing generally that "direct online accessibility to data requires strong authentication").

[32] *See, e.g.*, Talksoft, About Us: Patient Reminder Systems from Talksoft, http://www.talksoftonline.com/about.shtml (last visited Nov. 18, 2015) (offering doctors a patient reminder system including text messages); CenturyLink Center, Sign Up to Receive Text Alerts, http://www.centurylinkcenter.com/index.php?src=forms&ref=Text-Alerts (last visited Nov. 18, 2015) (offering users the chance to sign up for text message alerts about upcoming events).

[33] *See, e.g.*, American Red Cross, Text Message Donations, http://www.redcross.org/support/donating-fundraising/donations/text-messaging (last visited Nov. 18, 2015) (explaining different causes cell subscribers can donate to via text, including texting "REDCROSS" to 90999 to donate $10 to disaster relief, or "PREVENT" to the same number to help fund vaccinations against measles); *see also* SMS Tsunami Warning, What is SMS Tsunami Warning, http://www.sms-tsunami-warning.com/ (last visited Nov. 18, 2015) (on the preventative side, offering a free subscription service that sends SMS messages alerting vulnerable populations to seismic activity and potential tsunamis).

reflect the benefits of, and further promote, the utility of the unpolluted mobile messaging environment.

The Commission too has recognized Americans' growing reliance on messaging, adopting requirements for the provision of messaging to Public Safety Answering Points for 9-1-1 emergency calls.[34] In so doing, the Commission recognized the "unique value" that texting capabilities afford to the public, including the millions of Americans with hearing and speech disabilities.[35]

Thus, messaging has assumed an increasingly prominent role in Americans' lives precisely because it is a trustworthy medium largely free from the harms imposed by unwanted and unlawful content.

B. Spam and Unwanted Messaging Are a Significant and Growing Risk to the Messaging Ecosystem.

Today's messaging environment, given its popularity, presents a potential growth market for bad actors: "[A]lways-on communications, inherent trust in the channel, high open rates, and six billion subscribers are not lost on those with ill intent."[36] As the New York Times reported, "[w]hile SMS is less plagued by spam than e-mail, it's not without its bottom feeders."[37] It went on to note, however, that "the vast majority of the messages will never even get through, or

---

[34] *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications*, Second Report and Order and Third Further Notice of Proposed Rulemaking, 29 FCC Rcd 9846 (2014).

[35] *Id.* at 9847 ¶ 1, 9852-53 ¶¶ 13-14.

[36] *SMS Spam Overview, Preserving the value of SMS texting*, CLOUDMARK, https://www.cloudmark.com/en/s/resources/whitepapers/sms-spam-overview (last visited Nov. 18, 2015).

[37] Mark Cohen, *Text Message Marketing*, N.Y. TIMES, Sept. 23, 2009, http://www.nytimes.com/2009/09/24/business/smallbusiness/24texting.html.

through for long, before the cellphone carriers cut [them] off."[38] Wireless providers work extremely hard to minimize and/or prevent unwanted messaging traffic, but the risks are growing.

Earlier this year, Symantec issued its 2015 Internet Security Threat Report and observed that "[t]he threat landscape is continually evolving" and, "[a]s more users rely on their mobile devices, more spam, scams, and threats are tailored to these devices."[39] Specific to messaging, Symantec noted the following:

> SMS is far from a new technology; it's older than the smartphone itself. However, we've seen significant growth in this area of the mobile landscape when it comes to how scammers and attackers carry out their campaigns. SMS and other mobile messaging technologies are readily being used as a means to deliver all kinds of scam campaigns, such as adult content, rogue pharmacy, phishing and banking scams, payday loan spam, fake gifts, etc.[40]

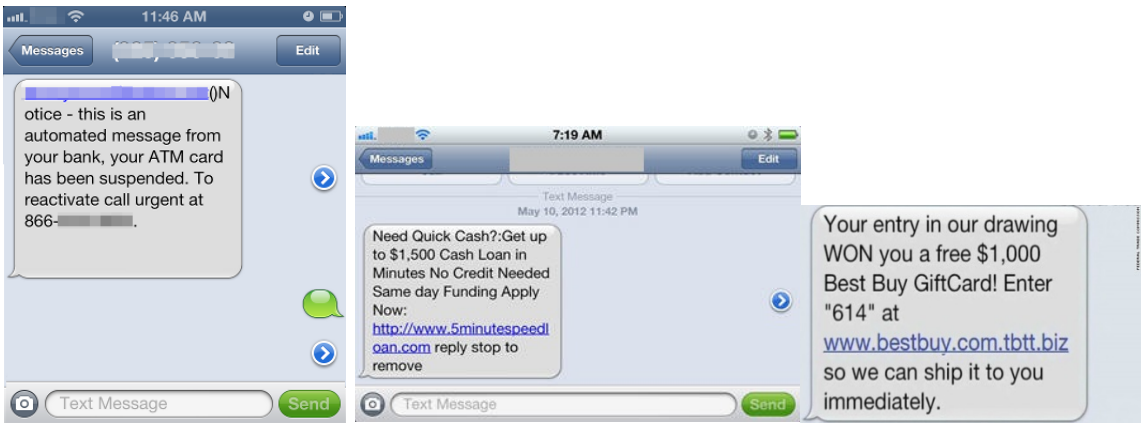
Just a few examples provide a sense of how these scammers are reaching out to messaging subscribers:

[38] *Id*.

[39] Symantec, Internet Security Threat Report, Vol. 20, at 23 https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf ("Symantec Report").

[40] *Id*.

Examples of Scam Campaigns in SMS Spam[41]



These campaigns may seek direct payments from consumers or access to their financial accounts, or they may seek sensitive personal information that can be sold to third parties.

Federal and state law enforcement agencies have taken notice. The Federal Trade Commission ("FTC"), for example, cracked down on entities that bombard consumers with hundreds of millions of unwanted spam text messages making misleading or false promises. In March 2013, the FTC charged 29 defendants with sending more than 180 million unwanted text messages to consumers in schemes promising free gifts or prizes. The FTC found that "[c]onsumers who clicked on the links in the messages found themselves caught in a confusing and elaborate process that required them to provide sensitive personal information, apply for credit or pay to subscribe to services to get the supposedly 'free' cards."[42]

---

[41] Jerome Segura, *SMS Scams: How to Defend Yourself*, MALWAREBYTES UNPACKED (July 30, 2013), https://blog.malwarebytes.org/intelligence/2013/07/sms-scams-how-to-defend-yourself/; WASH. STATE OFFICE OF THE ATT'Y GEN., *Washington Attorney General Targets Text Spammers* (Dec. 10, 2012), http://www.atg.wa.gov/news/news-releases/washington-attorney-general-targets-text-spammers; Lisa Sylvester, *Those Spam Text Messages are a Scam*, CNN: THE SITUATION ROOM WITH WOLF BLITZER (Mar. 8, 2013, 11:03 AM), http://situationroom.blogs.cnn.com/2013/03/08/those-spam-text-messages-are-a-scam/.

[42] FTC Press Release, *FTC Cracks Down on Senders of Spam Text Messages Promoting "Free" Gift Cards, Defendants Were Responsible for More than 180 Million Spam Text Messages* (Mar.

As part of the *TCPA Declaratory Ruling and Order* adopted earlier this year, the FCC reiterated that Section 227 of the Act applies to both voice calls and SMS.[43] The FCC went on to find that massive growth in the use of wireless devices "serves only to increase the number of wireless consumers potentially impacted by the use of autodialers and, thus, the governmental interest in protecting wireless consumers from the costs and privacy intrusions of unwanted voice calls and text messages."[44] CTIA's own comments in the TCPA proceeding recognized the growing challenges of unwanted messages but described in detail provider efforts to limit spammers: "[C]arriers routinely use robust spam filtering software that detects when a large volume of spam is sent from a single phone number, or identifies texts that invite a customer to click on a link to a website."[45] Citing CTIA's comments, the FCC noted spammers' unrelenting efforts but commended "carrier efforts to implement protections against unwanted text messages."[46]

State attorneys general have been deeply concerned about SMS scams as well. Attorneys general representing at least 25 states have either expressed concern about the growing risk of scams delivered via SMS, provided state residents with tips on how best to handle text message

---

7, 2013), https://www.ftc.gov/news-events/press-releases/2013/03/ftc-cracks-down-senders-spam-text-messages-promoting-free-gift.

[43] TCPA Declaratory Ruling and Order, 30 FCC Rcd at 7970 ¶ 7.

[44] *Id*. at 8021 ¶ 118.

[45] Comments of CTIA – The Wireless Association® on Revolution Messaging Petition, CG Docket No. 02-278, at 10 (filed Nov. 2012) (citations omitted). CTIA also noted other industry initiatives to stem the tide of unwanted messages on mobile devices, including mobile providers' mechanisms to report spammers and block unwanted messages; industry best practices; and providers' legal actions against third parties. *Id*. at 10-12.

[46] TCPA Declaratory Ruling and Order, 30 FCC Rcd at 8021 ¶ 119.

scams, or urged the FCC to take action against spammers.[47] The New York attorney general, for example, noted that some spammers have migrated from online scams via email to exploiting SMS on mobile phones and provided best practices for mobile phone users.[48]

[47] ALA. DEP'T OF LAW, CONSUMER PROT. UNIT, *Alaskans are Warned to Beware of Text Message Scams* (Mar. 29, 2013), http://www.law.alaska.gov/press/consumer_alerts/2013/0313-Smishing.html (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); ARIZ. ATT'Y GEN., *Arizona Attorney General Reminds Arizonans About National Data Privacy Day and Offers Tips to Protect Personal Information* (last visited Nov. 19, 2015), https://www.azag.gov/press-release/arizona-attorney-general-mark-brnovich-reminds-arizonans-about-national-data-privacy (offering consumers tips to avoid unwanted SMS messages); ARK. ATT'Y GEN., *Spam Texts*, http://arkansasag.gov/programs/consumer-protection/my-phone/spam-texts (last visited Nov. 19, 2015) (offering consumers tips to avoid unwanted SMS messages); STATE OF CAL. DEP'T OF JUSTICE OFFICE OF THE ATT'Y GEN., *Leave Me Alone! How to Slow the Flow of Unwanted Communications* https://oag.ca.gov/privacy/facts/other-privacy/leave-me-alone (last visited Nov. 19, 2015) (offering consumers tips to avoid unwanted SMS messages); COLO. ATT'Y GEN., *Phishing Scams are on the Rise* (Sept. 2011), http://www.coloradoattorneygeneral.gov/sites/default/files/uploads/Phishing%20Alert.pdf (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); OFFICE OF THE ATT'Y GEN., STATE OF IDAHO, *Attorney General Lawrence Wasden Warns Idaho Consumers Not to Respond to Fraudulent Banking Messages* (Aug. 22, 2011), http://www.ag.idaho.gov/media/consumerAlerts/2011/ca_08222011.html (offering consumers tips to avoid unwanted SMS messages); ILL. ATT'Y GEN., *Attorney General Sends a Message to Cell Phone Spammers: U R Violating the Law* (Jan. 22, 2007), http://www.ag.state.il.us/pressroom/2007_01/20070122.html (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); OFFICE OF THE IND. ATT'Y GEN., *Do Not Call – FAQs: What About Unwanted Text Messages?*, http://www.in.gov/attorneygeneral/2443.htm#20 (last visited Nov. 19, 2015) (offering consumers tips to avoid unwanted SMS messages); IOWA DEP'T OF JUSTICE OFFICE OF THE ATT'Y GEN., *Beware of Nepal Earthquake Scams* (May 29, 2015), https://www.iowaattorneygeneral.gov/for-consumers/consumer-alert/past-consumer-alerts/beware-of-nepal-earthquake-scams (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); KAN. ATT'Y GEN., *Consumer Corner: Avoiding Telemarketer Tricks* (Apr. 23, 2012), https://ag.ks.gov/search-results-detail/2012/04/23/consumer-corner-avoid-telemarketing-tricks (offering consumers tips to avoid unwanted SMS messages); KY. ATT'Y GEN., *AG Conway Urges FCC to Allow Use of Call-Blocking Technologies by Phone Companies* (Sept. 9, 2014), http://kentucky.gov/Pages/Activity-Stream.aspx?viewMode=ViewDetailInNewPage&eventID={16189290-41EA-4B20-A6ED-51061630ED5D}&activityType=PressRelease (urging the FCC to take action under the TCPA); MD. ATT'Y GEN, *AG Gansler Warns Consumers About Retail Text Message Scam, Phony promise of large gift card is attempt to get user's personal information* (Dec. 5, 2012),

http://www.oag.state.md.us/Press/2012/120512.html (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); MICH. ATT'Y GEN, *Cell Phone Spam Stop Receiving Unwanted Text Messages!*, http://www.michigan.gov/ag/0,4534,7-164-17337_20942-190608--,00.html (last visited Nov. 19, 2015) (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); MINN. ATT'Y GEN., *Beware of Text Messaging Phishing – or "Smishing" – Scams*, http://www.ag.state.mn.us/Brochures/pubtextmessagephishingorsmishingscams.pdf (last visited Nov. 19, 2015) (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); MO. ATT'Y GEN., *AG Koster Urges FCC to Approve Call-Blocking Authority for Phone Companies* (June 17, 2015, 10:09 AM), http://ago.mo.gov/home/news-archives/2015-news-archives/ag-koster-urges-fcc-to-approve-call-blocking-authority-for-phone-companies (expressing concern about the growing risks of SMS spam and urging the FCC to take action under the TCPA); NEB. ATT'Y GEN., *Consumer Alert: Text Message Phishing Scam Targeting Bank Customers* (Apr. 8, 2010, 2:30 PM), http://ago.nebraska.gov/resources/dyn/files/552077z59a468d8/_fn (offering consumers tips to avoid unwanted SMS messages); N.H. DEP'T OF JUSTICE OFFICE OF THE ATT'Y GEN., *New Hampshire Residents Warned About Phone Scam Involving Their Bank Accounts* (July 31, 2013), http://doj.nh.gov/media-center/press-releases/2013/20130731-phone-scam-alert.htm (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); N.Y. ATT'Y GEN., *Stop Mobile Spam: Protect your Mobile Phone from Unwanted Text Message (SMS) Spam*, http://www.ag.ny.gov/internet/stop-mobile-spam (last visited Nov. 19, 2015) (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); N.C. DEP'T OF JUSTICE OFFICE OF THE ATT'Y GEN., *Consumer – Telephone and Do Not Call – Text Messaging*, http://www.ncdoj.gov/Consumer/Telephone-and-Do-Not-Call/Text-messaging.aspx (last visited Nov. 19, 2015) (expressing concern about the growing risks of SMS spam and offering consumers tips to avoid unwanted SMS messages); OR. DEP'T OF JUSTICE OFFICE OF THE ATT'Y GEN., *Watch Out! The Text Message Scam is Back!* (Apr. 4, 2013, 10:43 AM), http://www.doj.state.or.us/consumer/pdf/scam_alert_04-04-13.pdf (offering consumers tips to avoid unwanted SMS messages); PA. ATT'Y GEN., *Consumer Protection Rights & Resources for Consumers of All Ages*, https://www.attorneygeneral.gov/uploadedFiles/MainSite/Content/Press/brochuresPublications/bcp_book.pdf (last visited Nov. 19, 2015) (offering consumers tips to avoid unwanted SMS messages); TEX. ATT'Y GEN., *Beware of Text Message Spam: "Smishing"*, https://www.texasattorneygeneral.gov/alerts/alerts_view_alpha.php?id=222&type=1 (last visited Nov. 12, 2015) (offering consumers tips to avoid unwanted SMS messages); WASH. ATT'Y GEN., *Washington Attorney General Targets Text Spammers* (Dec. 10, 2012), http://www.atg.wa.gov/news/news-releases/washington-attorney-general-targets-text-spammers (expressing concern about the growing risks of SMS spam); W. VA. ATT'Y GEN., *Attorney General Patrick Morrisey Warns Students of Texting Scam from Unknown Numbers* (Aug. 19, 2015), http://www.ago.wv.gov/pressroom/2015/Pages/Attorney-General-Patrick-Morrisey-Warns-Students-of-Texting-Scam-From-Unknown-Numbers.aspx (offering consumers tips to avoid unwanted SMS messages); WIS. DEP'T OF JUSTICE OFFICE OF THE ATT'Y GEN., *Smishing:*

CTIA and wireless providers have been strong proponents of law enforcement efforts to curb illegal and malicious mass-messaging. Wireless providers have taken spammers to court to protect their customers from unwanted and costly commercial messages.[49] CTIA has urged the FCC "to work with wireless carriers to increase enforcement efforts against third parties sending unsolicited commercial messages to wireless customers," and offered the wireless industry's assistance in helping the Commission to "fulfill[] its statutory mandate to enforce these important consumer protection laws."[50]

Legal protections of this type, however, are not alone sufficient. They are post-hoc remedies that can deter bad behavior by those that seek to operate lawfully, but they do not subdue bad actors – especially those outside the reach of American law enforcement. And from the consumer perspective, they cannot undo the harm once unwanted or malicious traffic has been sent. Thus, wireless providers employ an aggressive array of operational protections to safeguard their customers. In this environment, providers require substantial flexibility to respond to each new ploy by malicious content providers.

Phishing by Cell Phone Texts (Feb. 9, 2010), https://www.doj.state.wi.us/news-releases/smishing-phishing-cell-phone-texts (offering consumers tips to avoid unwanted SMS messages).

[48] N.Y. ATT'Y GEN., *Stop Mobile Spam: Protect You Mobile Phone from Unwanted Text Message (SMS) Spam*, http://www.ag.ny.gov/internet/stop-mobile-spam (last visited Nov. 19, 2015).

[49] *See, e.g.*, First Amended Complaint, AT&T Mobility LLC. V C&C Global Enterprises, LLC., No. 02733-TWT (N.D.G. 2006) (AT&T suing multiple companies for allegedly having "inundated AT&T and its subscribers with thousands of commercial electronic messages that were received by AT&T subscribers in the form of text messages"); Complaint & Demand for Jury Trial, Cellco P'ship v. Brown, No. 04-2856 (D.N.J. 2004) (Verizon suing 51 spammers for "inundating…its subscribers with millions of unsolicited commercial electronic messages").

[50] *See, e.g.*, Letter from Steve Largent, CTIA, to Kevin J. Martin, Chairman, FCC, *et al.*, WT Docket No. 08-7, at 2 (filed July 18, 2008); *see also* Letter from Steve Largent, CTIA, to Julius Genachowski, Chairman, FCC, et al. (filed Jan. 25, 2012), attached hereto as Exhibit A.

IV. WIRELESS INDUSTRY EFFORTS TO COMBAT SPAM AND UNWANTED MESSAGES HAVE BEEN LARGELY EFFECTIVE GIVEN THE SCOPE OF THE PROBLEM, BUT NEW BUSINESS MODELS RAISE CHALLENGES.

A. The Advent of Automated Messaging Added New Value But Created Opportunities for Mischief.

Like mobile communications generally, messaging services have evolved with amazing speed in recent decades. Early messaging services did not offer interoperability – a user could only send messages to other customers of the same provider. In 2000, providers developed mechanisms to allow for inter-provider communications. The advent of interoperability generated significant growth in messaging, but the traffic at issue was still P2P.

As explained above, the automation of messaging, the introduction of Short Codes, and the rise of A2P traffic created new opportunities providing value to consumers. But the rise of A2P messaging has, as noted above, unleashed new risks. A single content provider can send thousands of unwanted messages in a matter of minutes. These messages can impose real harms. Phishing-related traffic can be sent to thousands of recipients in the hope that some recipients will reveal financial passwords or other sensitive personal information. Wrongdoers can deposit worms and other malware on the devices of millions of users who unwittingly click on links that appear to be innocent. In all these cases, bad actors are poised to exploit the dark potential of an otherwise beneficial technology. It is this outcome that wireless providers are striving diligently to prevent – thus far, with impressive (though not complete) success. As detailed below, however, the "relief" Twilio seeks would undercut these efforts, exposing users to risks at a level unseen before now.

B. Industry Practices to Combat Spam and Unwanted or Harmful Messaging Are Significant.

Wireless providers have undertaken extensive efforts to block unwanted and unlawful traffic. Notwithstanding the inherent limitations on true P2P messaging (basic human limitations provide what might be the most critical barrier against "mass-casualty" texting), wireless providers have adopted guidelines and developed a series of practices designed to ensure that content providers do not exploit automated ten-digit number messaging to distribute unwanted or harmful content.[51] For example, wireless providers routinely use robust spam filtering software that detects when a large volume of spam is sent from a single phone number, or identifies texts that invite a customer to click on a link to a website. Wireless providers also use "account fingerprinting" techniques to identify accounts that are sending high volumes of messaging traffic with little or no voice or data usage. Further, in 2012 several wireless providers and the GSMA worked with Cloudmark to launch a service that permits consumers to forward mobile spam to "7726" ("SPAM" on traditional telephone keypads) for free.[52] These reports are added to a database, which aggregates messaging spam data across providers' networks and alerts wireless providers so that they can block unwanted messages from the offending senders. It is estimated that these actions will block between *1.3 billion and 1.6 billion* messages in 2015.

As detailed above, the Short Code program was developed to facilitate easy-to-use A2P while protecting against the spam threat that A2P enables. The Short Code program's principal bulwark against abusive A2P messaging is the provider-by-provider review process that takes

---

[51] *See CTIA SMS Interoperability Guidelines*, Version 3.2.2, at 19-21 (Jan. 1, 2015) ("*CTIA SMS Interoperability Guidelines*"), http://www.ctia.org/docs/default-source/default-document-library/sms_interoperability_guidelines_v3-2-2_jan_2015-as-posted.pdf?sfvrsn=2.

[52] GSMA Spam Reporting Service, Cloudmark, http://www.cloudmark.com/en/s/products/cloudmark-gsma-spam-reporting-service (last visited Nov. 18, 2015).

place when a content provider seeks a Short Code. Program review offers a way to bring A2P traffic "inside the tent" – it acts as a means of pre-clearing specific campaigns and messages so that messages do not need to be subjected to aggressive spam filtering in real time.[53]

First, CTIA has developed a basic Short Code code of conduct, set forth in its Short Code Monitoring Handbook ("Handbook").[54] As the Handbook makes clear, the goals of Short Code review are to:

- Provide consumers the best possible user experience;
- Honor consumer choices and prevent abuse of messaging platforms;
- Deliver flexible guidelines that communicate compliance values clearly;
- Enable the short code industry to self-regulate; and
- Facilitate enforcement measures, if necessary, to protect consumers quickly and consistently.[55]

CTIA's best practices emphasize that the program review process is designed to ensure that a campaign is appropriate for the intended audience and does not promote illegal or illicit content, such as depictions or endorsements of violence, adult or otherwise inappropriate content, profanity or hate speech, or endorsement of illegal drugs.[56] The Handbook confirms that "[m]essages must be delivered to a consumer's mobile device only after the user has opted in to receive them."[57]

---

[53] In this sense, Short Code program review might be likened to the Transportation Security Administration's "TSA Pre" program for frequent flyers, under which travelers undergo a rigorous screening process once in exchange for being able to pass through the security line more expeditiously in advance of each specific flight thereafter.

[54] *See* CTIA Short Code Monitoring Program, Short Code Monitoring Handbook Version Number 1.5.2 (Oct. 1, 2015) ("Short Code Monitoring Handbook"), http://www.ctia.org/docs/default-source/default-document-library/ctia-short-code-monitoring-handbook.pdf.

[55] *Id*. at 1.

[56] *Id*. at 4.

[57] *Id*. at 3.

As part of program review, wireless providers generally require content providers to specify the precise messages that will be sent, the frequency with which they will be sent, and other core characteristics of the traffic. Content providers must obtain customers' express consent to receive the messages at issue, via a specified opt-in process, as a condition for approval. Wireless providers also review the content of the proposed messaging campaign to ensure that users will not be sent unlawful, harassing, inappropriate, or otherwise malicious traffic.[58] Moreover, wireless providers vet all would-be Short Code holders to prevent the re-entry of entities that have misused Short Codes in the past.[59] These measures are designed to ensure that Short Codes do not fall into the hands of bad actors likely to abuse A2P messaging capabilities. Provider-specific guidelines also set forth criteria to optimize the consumer experience.[60]

Program review, needless to say, is not without cost. As the discussion above indicates, wireless providers and CTIA undertake significant efforts to ensure that A2P messaging

---

[58] Twilio complains that "if a short code lessee wants to alter its use case," it must again obtain approval and that, following approval, the provider "cannot just send whatever message content might be requested." Petition at 23-24. This, of course, is precisely the point of pre-approval: use of Short Codes frees messaging parties from message-by-message spam filtering only because the campaign has been pre-approved. Twilio's own marketing material explains, "After mobile carriers approve your short code application, you're able to send a large volume of approved SMS messages at once without running into recipient carriers' spam filters." Twilio, Can my Twilio SMS messages be blacklisted as spam?, https://www.twilio.com/help/faq/sms/can-my-twilio-sms-messages-be-blacklisted-as-spam (last visited Nov. 19, 2015). A regime allowing senders to alter campaigns at will would eviscerate the role of the content review and providers' ability to protect consumers.

[59] Likewise, CTIA conducts thorough background checks of any company seeking to lease a Short Code for a messaging campaign, using third-party sources such as Lexis/Nexis, Hoovers, Dunn & Bradstreet, Bloomberg, Reuters, as well as direct follow-up with the applicant itself.

[60] *See, e.g.*, Verizon, Content Policies for Verizon Networks at 5-6, http://www.verizon.com/about/sites/default/files/Verizon_Content_Policy.pdf (last visited Nov. 16, 2015).

campaigns comport with consumer interests. These efforts have been successful in limiting spam in the messaging marketplace, but they impose financial and other costs. Even aside from the large sums that individual wireless providers invest in spam prevention, CTIA itself invests significantly to maintain the curated, monitored messaging environment. The program review process can be time-consuming – admittedly sometimes more time-consuming than content providers would like – but is critical to ensure that this platform is not misused.[61] As Twilio itself explains, the Short Code program enables "mobile carriers [to] confirm that your business is not sending spam, and that your app provides ways for users to stop receiving messages. After mobile carriers approve your short code application, you're able to send a large volume of approved SMS messages at once without running into recipient carriers' spam filters."[62]

Although the front-end content review process is a critical piece of wireless providers' efforts to prevent abuse of A2P messaging, it is not the only piece. Rather, the Short Code program is subject to extensive and ongoing monitoring as a particular campaign progresses. A campaign must limit messages to users who have opted into receipt of such communications, but

[61] CTIA, wireless providers, and others are currently engaged in efforts to improve the speed of the review process by developing "best practices" for content providers' campaigns that will be acceptable by most or all providers. Some earlier steps have already improved the process. CTIA and the Mobile Marketing Association, which until 2012 had promulgated separate guidelines for acceptable campaigns, harmonized their materials in 2012. The streamlined Handbook, moreover, sets out clear criteria governing audits of Short Code campaigns. Finally, the end of premium Short Codes, which involved third-party commercial entities placing charges on wireless providers' bills, has led to reductions in the time required for individual providers to approve campaigns. CTIA is hopeful that the current work will further streamline the review process to the extent consistent with safeguarding consumers from unwanted and unlawful messaging.

[62] Twilio, Can my Twilio SMS messages be blacklisted as spam?, https://www.twilio.com/help/faq/sms/can-my-twilio-sms-messages-be-blacklisted-as-spam (last visited Nov. 19, 2015).

the Handbook also requires Short Code holders to respect user decisions to opt out of any future messages:

> Functioning opt-out mechanisms are crucial for all text messaging programs. Programs must always acknowledge and respect customers' requests to opt out of programs. However, depending on the use case, some short code programs are not required to advertise opt-out instructions. Short code programs must respond to, at a minimum, the universal keywords STOP, END, CANCEL, UNSUBSCRIBE, and QUIT by sending an opt-out message and, if the user is subscribed, by opting the user out of the program. Subsequent text, punctuation, capitalization, or some combination thereof must not interfere with opt-out keyword functionality. . . . Recurring-messages programs must also display opt-out instructions at program opt-in and at regular intervals in content or service messages, at least once per month. Opt-out information must be displayed in bold type on the advertisement. A program may deliver one final message to confirm a user has opted out successfully, but no additional messages may be sent after the user indicates a desire to cancel a short code program.[63]

The Handbook also includes a six-page discussion of monitoring activities with respect to ongoing campaigns, which include weekly audits of such campaigns, a set of standardized penalties for violations ranging from a grace period in which the content provider can cure the defect to – in the case of serious consumer harm – immediate suspension of the campaign, retest procedures for ensuring that violations have been cured, and an appeals process for content providers that dispute an audit's findings.[64]

Thus, while the rise of A2P traffic has greatly expanded opportunities for mischief by spammers and other bad actors, the spam filtering and the Short Code system developed by wireless providers afford consumers a robust defense against unwanted mass-messaging. The

[63] Short Code Monitoring Handbook at 3.

[64] *Id*. at 9-10; *see also id*. at 11-14 (setting out audit standards).

rise of new business models outside the Short Code system's protections poses new and difficult challenges.

C. New Business Models Trying to Develop a Hybrid Form of Messaging Traffic Create New Challenges.

The emergence of cloud-based messaging technology has propelled a new "hybrid" form of traffic into the P2P ecosystem: Commercial traffic that resembles P2P traffic in form – sent using ten-digit numbers – but relies on automated systems rather than human beings to generate content. Because this hybrid traffic is not constrained by human operation, it can easily reach volumes equivalent to those associated with Short Code traffic. These factors can expose mobile consumers to unwanted or unlawful traffic. As Symantec has succinctly put it: "[N]ew mobile platforms and technologies make it easier for scammers to take advantage of the unsuspecting, especially when they are using a relatively trusted medium like SMS."[65]

Hybrid traffic is sent outside the purview of the Short Code system described above, and thus is not subject to the extensive consumer protections employed by mobile providers. First and foremost, scrutiny of hybrid campaigns is much less well developed than in Short Codes. This means that wireless providers have virtually no opportunity to ensure that the traffic being sent will be subject to consumer opt-in, will properly exclude malware and other malicious content, and will be lawful and consistent with customer preferences. Furthermore, as explained above, the Short Code system requires wireless providers to respect consumer opt-out, either in advance of or during a campaign. In contrast, hybrid models do not offer any uniform mechanism for ensuring such consumer protection. For example, if an adult signs up to receive messages from a hybrid-model adult-content service, and then deactivates the associated phone

[65] Symantec Report at 23.

number, the messages could wind up being sent to a minor who subsequently assumes the number. The Short Code system, in contrast, has a robust deactivation / opt-out program in place. The Short Code audit process detailed above also does not apply to hybrid messaging, raising the risk that hybrid messaging campaigns could convert their content without customer approval or wireless provider review and customers could be left unable to opt out.

It is precisely *because* Twilio and others in the messaging ecosystem offer ten-digit number-based mass-messaging rather than Short Codes and the program review process that bad actors are attracted to some of their hybrid model offerings. As one commentator states in explaining "why spammers love long codes": "Spammers don't want to have to comply with stupid rules and audits of those rules, that kind of stuff just gets in the way of spamming. With long codes, no one is watching, so feel free to [ignore] the MMA Best Practices, the mobile carriers, the CTIA, etc."[66]

Hybrid messages sent as ten-digit number traffic *are* subject to the traditional spam filters applied to such traffic, but these filters inevitably disrupt messaging traffic that some cloud-based service providers argue is wanted traffic. For example, under some circumstances, traffic from commercial call centers may use long codes and thus be treated as P2P, but may be blocked by spam filters because it exceeds filters' thresholds for volume, throughput, number of recipients, and/or traffic balance. Put differently, the traffic bears all the hallmarks of spam, and is treated as such. As noted, the Short Code program is meant to "pre-approve" such traffic and thus to ensure that it will *not* be disrupted by P2P spam filters. But without the protections of the

[66] *See* Derek Johnson, *4 Reasons Why Spammers Love Long Codes*, MOBILE MARKETING WATCH (Aug. 17, 2011), http://mobilemarketingwatch.com/4-reasons-why-spammers-love-long-codes-17943/.

Short Code program, wireless providers have no means of protecting their customers except by applying such filters.

Thus, the central tension at the heart of Twilio's Petition is between the desire among some cloud-based service providers to offer their content-provider customers unfettered messaging access to all mobile devices and the equally strong (and important) desire among wireless providers to preserve a spam-limited messaging environment for consumers – one free of spam, malware, scams, unconsented-to, and other harmful traffic. Entities such as Twilio want to be able to use high-volume, ten-digit number messaging to send mass messages without having to obtain the pre-clearance embodied Short Code program review *or* be subject to the in-the-moment review of P2P spam filters.

V. TITLE II CLASSIFICATION OF MESSAGING AND SHORT CODES WOULD UPEND EFFORTS TO RESTRICT UNWANTED MESSAGES AND PROTECT CONSUMERS.

A. Classification of Messaging Services and Short Codes as Telecommunications Services Would Badly Impair Provider Efforts to Protect Consumers.

CTIA explains below why messaging services and Short Codes are not, as a legal matter, telecommunications services. Even apart from these legal barriers, however, classification of messaging services and Short Codes as Title II telecommunications services would undermine consumer interests. Application of a Title II regime would endanger the wireless provider-driven framework that has largely limited spam and unwanted or harmful messaging.

If messaging were deemed a common carrier offering, wireless providers would be hamstrung in their efforts to filter unwanted traffic and provide a safe A2P experience for their end users, unleashing a flood of unwanted and/or unlawful traffic. Provisions such as Section 201 and 202 could well preclude mobile providers from halting traffic that is unwanted by consumers, but not *per se* illegal. It could also chill provider filtering and curating efforts by

threatening to subject providers to intensive inquiries as to whether a choice to transmit one message but not another constituted unreasonable discrimination.

Furthermore, the Commission must be mindful of the many additional costs and uncertainties that would flow from classifying messaging as a Title II service. Because messaging traffic clearly is not broadband Internet access, the 2015 *Open Internet Order*'s forbearance grants would not apply. Thus, any classification of messaging as a telecommunications service would also subject that offering to every Title II provision affecting common carriers, imposing burdens ranging from tariffing to discontinuance regulation to universal service contribution obligations. In all, Title II classification would impose on messaging offerings dozens of statutory provisions and hundreds of codified rules, putting mobile messaging at a clear disadvantage *vis-à-vis* other similar services, such as OTT messaging and email.[67] In addition, messaging would potentially be subject to a whole host of new federal and state obligations, including (to take just one example) state certification requirements.[68]

Ultimately, such a breakdown of the existing system would impose unnecessary obligations, threaten to unleash a Pandora's Box of new mobile threats, risk consumer "text

[67] *See, e.g., 2015 Open Internet Order*, 30 FCC Rcd at 5616 ¶ 51 (purporting to forbear from 30 statutory provisions and more than 700 Commission rules). Indeed, the Commission has not sought comment on whether forbearance is appropriate, calling into question whether it could even move to an order that classified messaging as a telecommunications service while simultaneously forbearing from (for example) tariffing, discontinuance, and universal service contribution requirements.

[68] Minnesota is a case in point. Any person wishing to provide telephone service in that state must obtain commission authorization. However, the relevant statutes do not limit "telephone service" to voice services; rather, "telephone service" can include data. Messaging is undeniably a data service.

fatigue" and thus diminish – not enhance – messaging's utility, including its role in notifying consumers of critically important events.

B. Classification of Messaging Services and Short Codes as Telecommunications Services Would Create Arbitrary Distinctions Among Competing Messaging Services, Distorting Competition.

Grant of the Twilio Petition would undermine the evolution of the messaging marketplace in other ways as well. The messaging environment is populated not only by wireless providers but by third-party providers experiencing growing success in the marketplace. As noted above, in 2014 OTT texting applications surpassed SMS in terms of volume.[69] Moreover, because many Internet-based messaging services employ 10-digit telephone numbers that are indistinguishable from the 10-digit numbers issued to mobile subscribers, consumers lack any way to differentiate a text message sent from a traditional provider-offered service from a text message sent from an Internet-based service.[70] There should be no doubt that consumers view OTT and provider-offered messaging services as substitutes.[71]

Chairman Wheeler has stated that "[a] key component of rules that spur competition is assuring the FCC's rules are technology-neutral."[72] Yet Twilio asks the Commission to subject only a single subset of messaging providers – mobile providers – to the strictures of Title II. Given the popularity of non-provider-offered messaging platforms, a Commission decision to

---

[69] *911 Policy Statement & Second FNPRM*, 29 FCC Rcd at 1550 ¶ 6.

[70] *CTIA SMS Interoperability Guidelines* at 6.

[71] Indeed, the Commission has found that, "from the consumer's perspective, text messaging applications provided by CMRS providers are often indistinguishable from the messaging applications provided by OTT and other providers." *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications*, Report and Order, 28 FCC Rcd 7556, 7602 ¶ 134 (2013).

[72] Tom Wheeler, *Tech Transitions, Video, and the Future*, FCC BLOG (Oct. 28, 2014), https://www.fcc.gov/blog/tech-transitions-video-and-future.

classify provider-offered messaging offerings as telecommunications services, but *not* OTT services like WhatsApp, Apple's iMessage, and others, would actively undercut competitive and technological neutrality. There is no basis whatsoever for subjecting providers representing a minority share of the messaging marketplace to common carrier requirements that do not apply to their highly successful competitors.

The problem does not end with OTT messaging services, however. Mobile messaging, Instant Messaging, and email functionalities have converged to the point that they all serve virtually the same ends. Consumers can send email and IMs to mobile devices even if those devices are not email- or IM-capable, as those emails and IMs can be received as text messages.[73] By the same token, mobile customers can send text messages to email and IM addresses the same way they send text messages to other mobile users, and the message is received as email or IM.[74] Moreover, messaging shares the same vital characteristics as email and IM: just as the storage capability of email and IM is central to those services, marketing data show that the "asynchronous" nature of messaging is not at all incidental, but rather an integral component of why consumers use the service in the first place.[75] Given the similarities among messaging, IM, and email, any effort to treat messaging differently than these services for

---

[73] *See, e.g.*, Albert Aydin, *How to Send Text Messages to Verizon Customers from Your PC*, VERIZON WIRELESS (June 25, 2013), http://www.verizonwireless.com/news/article/2013/06/computer-to-phone-text-messaging.html.

[74] *See, e.g.*, Verizon Wireless, Text Messaging FAQs, http://www.verizonwireless.com/support/text-messaging-faqs/ (last visited Nov. 18, 2015)

[75] *See* Neil Howe, *Why Millennials Are Texting More and Talking Less*, FORBES (Jul. 15, 2015); Ian Bogost, *Don't Hate the Phone Call, Hate the Phone*, THE ATLANTIC (Aug. 12, 2015), http://www.theatlantic.com/technology/archive/2015/08/why-people-hate-making-phone-calls/401114/ ("When asked, people with a distaste for phone calls argue that they are presumptuous and intrusive, especially given alternative methods of contact that don't make unbidden demands for someone's undivided attention.").

regulatory purposes would inevitably lead to arbitrary line drawing and distort the natural development of the marketplace.[76]

The Commission should reject Twilio's proposal that would place the Commission's heavy thumb on the competitive scale and distort the future development of the market.

C. The Commission Should Allow Industry to Support New Business Models While Protecting Consumers.

The Commission should refrain from any classification consideration and instead encourage the messaging industry to continue to reconcile technical and marketplace developments with the overriding importance of protecting consumers. For the past year, consistent with the consensus-based, inclusive industry processes that have governed messaging from its earliest days, the messaging community has been working to address whether cloud-based messaging traffic under a hybrid model can be integrated into the existing ecosystem without exposing consumers to greater risk of spam and unwanted or harmful messages.

In April of this year, under CTIA's auspices, the messaging industry formed working groups charged with the following responsibilities, among others:

- Identifying specific use cases and traffic classes arising from hybrid messaging's growth to allow all service providers to deliver an optimal consumer experience and efficient traffic/network management.

- Developing best practices that every messaging service provider should follow with respect to other service providers to protect consumers from unwanted traffic and other service-related problems.

The working groups are in the process of addressing the issues laid out above. They are committed to the twin goals of continuing to provide high value to consumers and commercial

[76] Perhaps even worse, to cure this problem, the FCC would need to extend common carriage regulation to other similar information services, vastly expanding the scope of offerings deemed "telecommunications services."

users without falling prey to the harms associated with extensive unwanted, inappropriate, or illegal content. Twilio, moreover, has been an active participant in these discussions. Its Petition, however, threatens to derail this process, supplanting a regime that balances and respects the numerous interests at stake (including, most critically, consumer protection) with a heavy-handed Title II approach that would restrict wireless provider efforts to apply the protections that have made messaging so immensely popular and trusted in the P2P and Short Code areas The Commission should reject Twilio's Petition and permit industry to work through collaborative processes to address new technologies and evolving customer demands.

VI. AS A MATTER OF LAW, SMS, MMS, AND SHORT CODES ARE NOT TITLE II COMMON CARRIER SERVICES.

A. As an Initial Matter, Common Short Codes Are Not a Communications Service.

Twilio does not seriously contend that Short Codes are either telecommunications or information service offerings. Nevertheless, it asks the Commission to declare that "short-code-based services" are governed by Title II.[77] Twilio's request is premised on a misunderstanding or misrepresentation of the role played by Short Codes in the marketplace, and should be rejected. A Short Code is simply a number sequence offered to third-party content providers to facilitate A2P messaging over the mobile network. When a mobile provider sells access to a Short Code, the product being sold is not the transmission of messages, but rather an addressing, billing, and marketing tool. Specifically, a customer (usually a commercial or non-profit entity) purchasing access to a Short Code is obtaining the following:

- The ability to have individuals send messages to the customer at an easily-remembered five- or six-digit code. This is the primary function of a Short Code. This function is effectively identical to the assignment of a Uniform Resource Locator ("URL") to an

[77] *See* Petition at 1, n.2.

entity wishing to set up a website. Just as a URL corresponds with a harder-to-remember IP address, a Short Code corresponds with more complex addresses, facilitating communication with the holder of the Short Code.

- The ability to send simultaneous messages to large numbers of individuals who have requested such communications, through the use of *separately priced* messaging services (*i.e.*, SMS and MMS). Short Code campaigns use SMS or MMS messages exchanged between the operator of the Short Code campaign and mobile users who are interacting with that campaign.

- The ability (in the case of a charitable entity or political campaign) to allow message recipients to use the Short Code to make financial donations, which are then billed and collected by the mobile provider through its customer bills.

None of these functions involves telecommunications – *i.e.*, the transmission of information. First, the provision of a mobile address (a Short Code) is not a messaging offering, just as the provision of a URL within the ".com" domain is not the provision of Internet access. In both cases, provisioning this alternative address provides a tool for third parties using connectivity (SMS/MMS in the case of Short Codes; broadband Internet access in the case of a URL). Second, holders of Short Codes benefit from a more sophisticated addressing mechanism for outgoing messages, but the Short Code does not provide them the capability to send such messages. Rather, additional fees are involved for the transmission of Short Codes. The sending of those messages occurs via SMS or MMS, which (as detailed below) are information services. Moreover, the fact that the Short Code message is an information service delivered (like all information services) "via telecommunications" or even (if the Commission were to so hold) over a common carrier telecommunications service does not make it a telecommunications service itself. Information services routinely travel over telecommunications service offerings, and this does not affect their classification.[78] The associated Short Code provisioning is not a

[78] *See Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, 19 FCC Rcd 3307, 3312 ¶ 9 (2004) ("*Pulver Order*") ("[T]he fact that Pulver's server is connected

communications service. Finally, the billing and collection function performed by mobile providers further undermines any claim that Short Code provisioning involves the transmission of information. As the Commission has held, billing and collection are not communications services for purposes of Title II.[79]

Given that Short Codes are not communications services at all, they are neither telecommunications services (which by definition involve the offering of telecommunications) nor information services (which by definition are provisioned "via telecommunications"). Indeed, Short Codes fall outside the scope of the Commission's jurisdiction. Accordingly, the Commission does not have authority to regulate a wireless provider's approval and oversight of Short Code campaigns.

B. SMS and MMS are Information Services within the Meaning of the Act, Not Telecommunications Services.

Twilio is wrong on the law governing SMS and MMS (collectively, "messaging") as well. Under longstanding FCC precedent, the characteristics of messaging necessarily make it an information service. Nothing in the *2015 Open Internet Order* alters these conclusions; indeed, in some cases, that decision confirms that messaging is, at most, an information service.

---

to the Internet via some form of transmission is not in and of itself, as some commenters argue, relevant to the definition of telecommunications. Pulver may 'use' some telecommunications to provide its FWD directory service but that does not make FWD itself telecommunications.").

[79] *See, e.g.*, *Audio Communications, Inc.*, Memorandum Opinion and Order, 8 FCC Rcd 8697 (CCB 1993) (finding that billing and collection for 900 services is not a common carrier service); *The Public Service Commission of Maryland and Maryland People's Counsel Applications for Review of a Memorandum Opinion and Order By the Chief, Common Carrier Bureau Denying the Public Service Commission of Maryland Petition for Declaratory Ruling Regarding Billing and Collection Services*, Memorandum Opinion and Order, 4 FCC Rcd 4000, 4000-01 ¶¶ 6-7 (1989), *aff'd sub nom. Public Service Comm'n of Maryland v. FCC*, 909 F.2d 1510 (D.C. Cir. 1990); *Detariffing of Billing and Collection Services*, Report and Order, 102 F.C.C.2d 1150, 1151-52 ¶ 1 n.2, 1168-69 ¶¶ 32-33 (1986).

1. SMS and MMS Involve Core Information Service Functions.

The Communications Act of 1934, as amended ("Act") defines an information service as providing a "capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing or making available information via telecommunications."[80] As described below, messaging falls within this definition, not the "mutually exclusive"[81] category of telecommunications service.

Data Storage and Retrieval are Essential Features of Messaging. When a user sends an SMS or MMS message, that user is relying on, among other things, the network's ability to store the message until the intended recipient's device is able to receive it. In cases where the device is out of range or has been turned off when the system first tries to deliver the message, a Short Message Service Center ("SMSC") or Multimedia Message Service Center ("MMSC") will temporarily store the relevant message until the recipient's device is ready to receive it, and then forward the message to that device.[82] Further, subscribers have the option to defer the delivery of a message to some later point in the future.[83] And once a message is received, it generally is stored until the recipient chooses to delete it.

In this regard, messaging is similar to services like email and voicemail, which the FCC has consistently held to be information services.[84] Indeed, as noted above, messaging has largely

---

[80] 47 U.S.C. § 153(24).

[81] *See 2015 Open Internet Order*, 30 FCC Rcd at 5776 ¶ 385.

[82] *See CTIA SMS Interoperability Guidelines* at 23.

[83] *See id*. at 35, 40-41.

[84] *See Federal-State Joint Board on Universal Service*, Report to Congress, 13 FCC Rcd 11501, 11538-11539 ¶ 78 (1998) ("*Stevens Report*"); *Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, First Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 21905, 21975-76 ¶¶ 143-45 (1997) ("*Non-Accounting Safeguards Order*").

supplanted voicemail as a preferred data storage technology, particularly among younger users.[85] Like email and voicemail, messaging is an "asynchronous" service because one person can send a message to another person without any need for the other person to be available to receive it at that time. Services that permit asynchronous communications offer "more than a simple transmission path"[86] and fall within the definition of information services.

The *2015 Open Internet Order* does not affect this analysis. That order considered only the caching used in the course of delivering real-time communications over broadband Internet access service ("BIAS"), not features that store a message for an indeterminate period of time while the recipient is out of range or otherwise unable to retrieve the message. In the Order's words, the "caching" at issue there was "'the storing of copies of content at locations in the network closer to subscribers than their original sources,'"[87] often used to facilitate speedy delivery of Internet content. The Commission found that caching as so defined "is simply used to facilitate the transmission of information so that users can access other services,"[88] and that it did not make BIAS an information service. CTIA disagrees with that conclusion, and is appealing it, but even assuming *arguendo* that this logic is upheld, it does not apply to the storage or retrieval involved in mobile messaging. Messaging's storage, in contrast to the caching involved in BIAS, offers the ability to access a communication well after it has been

---

[85] *See, e.g.*, Rachel Rood, *Please Do Not Leave a Message: Why Millennials Hate Voice Mail*, NPR (updated Dec. 4, 2014), http://www.npr.org/sections/alltechconsidered/2014/10/23/358301467/please-do-not-leave-a-message-why-millennials-hate-voice-mail; Teddy Wayne, *At the Tone, Leave a What? Millennials Shy Away from Voice Mail*, N.Y. TIMES (June 13, 2014), http://www.nytimes.com/2014/06/15/fashion/millennials-shy-away-from-voice-mail.html?_r=0.

[86] *Stevens Report*, 13 FCC Rcd at 11538-39 ¶ 78.

[87] *2015 Open Internet Order*, 30 FCC Rcd at 5770 ¶ 372 (citation omitted).

[88] *Id.*

sent, and is an important part of the service purchased by the end user. It does not merely facilitate transmission. Moreover, it has nothing to do with storing content at closer proximity to the end user to facilitate speedy retrieval. Indeed, the content at issue in messaging does not *exist* before it is sent. Nor is the storage function at all incidental: As explained above, many users rely on messaging precisely because it offers storage and allows recipients to access messages minutes, hours, or days after they have been sent.

Changes to Form and Content Occur in Messaging. Both the Act and Commission precedent make clear that services that "change the form or content" of transmitted information are information services.[89] Here, both the form *and* content of SMS and MMS messages are subject to substantial computer processing and conversion that render them information services.

In some cases, messaging changes the *content* of transmitted information. Messaging includes communications sent to and from email and IM platforms, and email and IM protocols use different fields and formats than messaging. To render these systems compatible, the SMS platform must strip out certain information (such as email subject lines), and add other information, such as time, date, status reports, and call-back numbers.[90] This is content modification.

In other cases, messaging changes the *form* of transmitted information. First, messaging providers segment (break up) or concatenate (break up and reconstruct) messages that exceed the

[89] *See* 47 U.S.C. § 153(50) (defining "telecommunications" as "transmission … without change in the form or content of the information as sent and received"); *Stevens Report*, 13 FCC Rcd at 11520-21 ¶ 40 ("[A]n entity is *not* deemed to be providing 'telecommunications,' notwithstanding its transmission of user information, in cases in which the entity is altering the form or content of that information.").

[90] *See CTIA SMS Interoperability Guidelines* at 23.

character limit of SMS.[91] In addition, messaging routinely involves protocol processing to facilitate inter-platform operability.[92] Today, wireless providers offer protocol conversion as part of their messaging services so that customers can send text messages to the customers of virtually any other wireless provider. Within the MMS platform, for example, transcoding is used to resolve any differences in multimedia capabilities between a sender and receiver by converting a single piece of content into the optimal format for a subscriber's device, operating system and/or provider. Further, in cases involving the exchange of messages between an SMS platform and an email or IM platform or vice versa, a provider's network must translate the message from one protocol to another. SMS/MMS messages generally originate or terminate on the mobile device in short message peer-to-peer protocol ("SMPP") or MM7. However, email messages are generally formatted in standard mail transfer protocol ("SMTP") and IMs are generally formatted in Transmission Control Protocol/Internet Protocol ("TCP/IP"). In order for SMS and MMS messages to be sent to email or IM systems, or vice versa, the messages must necessarily be subjected to protocol conversion. When users send SMS messages to an email or

[91] *See id*. at 22:

> The maximum message length varies by the service provider network [and user device]. Segmentation might be necessary to adapt message length according to the networks' capabilities. Each service provider can determine the format of a segmented message separately. It is recommended to append an identifier or order reference to the message. The terminating entity is responsible to segment the incoming message if the terminating carrier is limited in message length. Concatenated messages on the originating side should be put into a single SMPP message by the originating entity.

[92] *See id*. at 21 (stating that the most commonly used protocols are SMPP, EMI/UCP, SMS2000/OIS, and SNPP).

IM account, for example, the SMSC routes the message to an Internet gateway, which will translate the message into the appropriate protocol.

The *2015 Open Internet Order* confirms this analysis. As the Commission recognized there, when an email provider places information into a packet payload it "changes the form or content" of the message, and the service is an information service.[93] This same construct applies equally to messaging: As described above, SMS and MMS offerings engage in at least as much modification in form and content as email does, and the *2015 Open Internet Order*'s recognition of email's continued status as an information service governs here.[94]

Messaging Platforms are Integrated Information Services. The data storage and transformation functions described above are core information-service functions associated with messaging and cannot be separated from its transmission functionality. The Commission has found, and the Supreme Court has agreed, that a service involving both transmission and processing is an information service if offered as "a single, integrated service."[95] As the Commission has held, a service that offers "a number of 'computing capabilities'" and that "use[s]" telecommunications without actually providing it is an information service,[96] whereas a service in which any "enhanced" features are merely "incidental" to an underlying provision of

[93] *2015 Open Internet Order*, 30 FCC Rcd at 5763 n.1005 ("We note that a user may choose an application, such as email, that is a separate information service provided by the BIAS provider. When this occurs, the provider of the information service may place information into the packet payload that changes the form or content.").

[94] *See id.*

[95] *See Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities*, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 4798, 4821 ¶ 36, 4824 ¶ 41 (2002); *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 990 (2005).

[96] *Pulver Order*, 19 FCC Rcd at 3312-14 ¶¶ 9-11.

transmission is not.[97] In applying these definitions, the Commission consistently has focused on what is actually being offered and how consumers understand that offering. "[W]hether a telecommunications service is being provided turns on what the entity is 'offering . . . to the public,' and customers' understanding of that service."[98] Twilio might *like* wireless providers to provision messaging in a manner that offers pure telecommunications, but that is not the service that these providers, in fact, offer. A user cannot purchase or even use the transmission capabilities of messaging without also having access to the storage and processing capabilities discussed above. This basic fact refutes any suggestion that these offerings are not inherently intertwined.

Nor can the functions discussed above be dismissed as falling within the information service definition's "telecommunications management exception."[99] Even assuming *arguendo* that the *2015 Open Internet Order*'s conclusion that caching, Domain Name System ("DNS"), and other functions associated with BIAS are mere "network management,"[100] the same cannot be said of the features that render messaging an information service. In many cases, messaging customers specifically seek the storage and retrieval that render messaging "asynchronous" – more like email or voicemail than like telephone calls or even Internet communications. Likewise, they seek out the ability to send and receive messages whose form and/or content have

---

[97] *AT&T Corp. Petition for Declaratory Ruling Regarding Enhanced Prepaid Calling Card Services*, Order and Notice of Proposed Rulemaking, 20 FCC Rcd 4826, 4830-31 ¶¶ 15-16 (2005).

[98] *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 14853, 14910-11 ¶ 104 (2005). *See also id*. at 14864-65 ¶ 16 ("[W]hat matters is the finished product made available through a service rather than the facilities used to provide it.").

[99] *See 2015 Open Internet Order*, 30 FCC Rcd at 5772 ¶ 374.

[100] *See, e.g., id*. at 5768 n.1037.

been altered to permit communications among different platforms – including different wireless networks, IM platforms, email systems, and so on. Thus, these functionalities are not principally about managing a telecommunications service; rather, the information-processing functionalities are core to the consumer's demand.

Likewise, these characteristics of messaging would not, in pre-Act terminology, have been "adjunct-to-basic" offerings. As an initial matter, prior to 1996, the Commission expressly defined any service that provided "subscriber interaction with stored information" as an enhanced service.[101] In contrast, basic telecommunications transmissions are subject only to delays caused by network congestion or transmission priorities given by the originator.[102] Commission precedent was also clear (and remains clear) that services offering protocol conversion are enhanced services (and, thus, information services): "[G]enerally, services that result in a protocol conversion are enhanced services, while services that result in no net protocol conversion to the end user are basic services."[103]

Furthermore, the *2015 Open Internet Order* again confirms that the enhanced functionalities associated with mobile messaging are not "adjunct-to-basic." According to that decision, adjunct-to-basic services "(1) must be 'incidental' to an underlying telecommunications

---

[101] 47 C.F.R. § 64.702(a). *See also Computer II Final Decision*, 77 FCC 2d 421 ¶ 97 ("[I]n an enhanced service the content of information need not be changed and may simply involve subscriber interaction with stored information."). The Commission has confirmed that all services previously considered enhanced services are information services under the Act. *See Non-Accounting Safeguards Order*, 11 FCC Rcd at 21955-56 ¶ 102. *See also 2015 Open Internet Order*, 30 FCC Rcd at 5735 ¶ 312 ("[I]n *Computer II* the Commission distinguished 'basic' from 'enhanced' services, a distinction that Congress embraced when it adopted the Telecommunications Act of 1996.").

[102] *See Computer II Final Decision*, 77 FCC 2d at 420 ¶ 95.

[103] *Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges*, Order, 19 FCC Rcd 7457, 7459 ¶ 4 (2004).

service—*i.e.*, 'basic' in purpose and use' in the sense that they facilitate use of the network; and (2) must 'not alter the fundamental character of [the telecommunications service].'"[104] As described above, this is not the case with respect to the storage and information-processing capabilities of messaging. Marketing and other data show that users specifically value the storage and retrieval that are central to messaging's functionality – it is precisely because messages will wait for the recipient until it is convenient for him or her to read and respond that so many users have flocked to SMS and MMS.[105] Put differently, it is because messaging differs from real-time telephony – because it *does* "alter the fundamental character of" the offering – that messaging is so popular. The differences between messaging and telephony, therefore, are not "incidental" but rather crucial to messaging's popularity.

To the Extent Short Codes are a Communications Service, They Too Are Information Services. As detailed above, access to Short Codes is not a communications offering at all. But even if Short Codes were deemed a communications offering, they would clearly be information services, not telecommunications services. To the extent Short Codes are viewed as involving telecommunications, they entail at least as much data storage and retrieval as SMS and MMS. Entities sending messages to or from Short Code addresses use SMS and MMS for the transmission of those messages, and all of the storage and retrieval discussed above applies to Short Code-related messages. Further, information retrieval is central to Short Code activity, as companies use Short Codes is to facilitate customers' access to information. Finally, there is even more conversion of messages in the Short Code context than in the typical SMS or MMS

[104] *2015 Open Internet Order*, 30 FCC Rcd at 5766-67 ¶ 367 (internal quotations omitted).

[105] *See, e.g.*, Neil Howe, *Why Millennials Are Texting More and Talking Less*, FORBES (Jul. 15, 2015); Ian Bogost, *Don't Hate the Phone Call, Hate the Phone*, THE ATLANTIC (Aug. 12, 2015), http://www.theatlantic.com/technology/archive/2015/08/why-people-hate-making-phone-calls/401114/.

context, because Short Code messaging campaigns often involve the exchange of sophisticated content containing graphics or other specialized materials, necessitating additional changes in form or content to accommodate the many diverse devices, services, and platforms on which messages are sent and received.

2. SMS and MMS Cannot Be Classified as Commercial Mobile Radio Services.

Twilio's call for common carrier regulation is predicated on assertions that messaging falls within the definition of Commercial Mobile Radio Service ("CMRS") because these services are "interconnected with the public switched telephone network."[106] The Act and the Commission's rules do not support Twilio's position.

As explained above, messaging is an information service. As such, it cannot be CMRS, because the Act demands that information services remain free from common carrier regulation.[107] Furthermore, messaging does not make "interconnected service" available to the public switched telephone network ("PSTN"), as Twilio suggests. For instance, a typical SMS message routed between two different SMS providers travels from a user's mobile device through an originator SMSC and the Internet to a terminator SMSC, and ultimately to the terminating mobile device. The SMSCs are private servers that control, store, and route SMS messages. Even though SMS allows customers to use their phone numbers as an address for SMS, those messages are typically carried via private data links to an ENUM address associated

[106] Petition at 3.

[107] The Act states that "[a] telecommunications carrier shall be treated as a common carrier . . . only to the extent that it is engaged in providing telecommunications services . . . ." 47 U.S.C. § 153(51). Because messaging is not a telecommunications service, Title II common carrier regulation is flatly prohibited.

with the consumer's phone number.[108] Thus, SMS messages use a private network separate from the PSTN and do not interconnect with the PSTN. Finally, as the *2015 Open Internet Order* stated, to be considered CMRS, an "interconnected service" must "provide the 'capability' for access to all other users of the public switched network."[109] Messaging does not provide the ability to reach all users of the public switched network – specifically, the vast majority of wireline customers can neither send nor receive messages via their wireline phones.[110]

Nothing in the *2015 Open Internet Order* changes this analysis. While the *2015 Open Internet Order* indicated that "a service is interconnected even if [it] provides general access to points on the public switched network but also restricts access in certain limited ways,"[111] it nowhere suggested that Congress could have intended the interconnection requirement to cover a service that failed to reach the huge swath of numbers still associated with fixed-line telephones, which numbered approximately 85 million at the end of 2013.[112] That approach would read the

---

[108] *See* Comments of CTIA, WC Docket No. 06-122, at 3-4 (filed June 6, 2011).

[109] *2015 Open Internet Order*, 30 FCC Rcd at 5787 ¶ 402.

[110] *See CTIA SMS Interoperability Guidelines* at 30:

> "While essentially 100% of CMRS handsets can receive and send SMS messages, the ability of non-CMRS TNs to receive or send SMS messages is still developing. This uncertainty around the SMS capabilities of non-CMRS devices and services potentially presents a problem when only a small number of SMS messages addressed to non-CMRS TNs can be successfully delivered."

[111] *2015 Open Internet Order*, 30 FCC Rcd at 5787 ¶ 402 (quoting 47 C.F.R. § 20.3). This is not to suggest that CTIA accepts the *2015 Open Internet Order*'s changes to the longstanding meaning of "public switched network." To the contrary, CTIA disagrees with the Commission's new rules and interpretations in the *2015 Open Internet Order* and is appealing them.

[112] Industry Analysis & Technology Div., FCC, *Local Telephone Competition: Status as of December 31, 2013*, at 1 (Oct. 2014).

"interconnected" requirement out of the statute altogether, and is well beyond the scope of the agency's interpretive discretion.

C. The Precedent that Twilio Cites Has No Bearing on Messaging Classification.

The Petition insists that the Commission's decision should be guided by Twilio's deeply flawed interpretations of the D.C. Circuit's *Verizon* decision, the Commission's *Roaming Reexamination Order*, and a recent consent decree involving billing practices for premium SMS services. There is no merit to any of these assertions.

Verizon v. FCC. Twilio contends that, under the court's holding in the *Verizon* case, the FCC cannot subject messaging to any provision of Title II without classifying messaging as a telecommunications service. According to Twilio, because the FCC has been subjecting messaging to the TCPA under Section 227 since 2003, the Commission must classify messaging as Title II services as a whole.[113] Twilio's argument is baseless. A call may be a call under the TCPA,[114] but that does not make it a telecommunications service under the Act.

As an initial matter, Twilio mischaracterizes the *Verizon* decision. As the Commission is fully aware, the court in *Verizon* held that the Commission cannot impose *per se* common carrier obligations on information service providers.[115] There is no language in the *Verizon* decision that lends support to Twilio's legal theory, and Twilio has cited none.

---

[113] *See* Petition at 26-29.

[114] *See id.* at 18 n.37.

[115] *See Verizon v. FCC*, 740 F.3d 623, 655-58 (D.C. Cir. 2014) (vacating the Commission's rule prohibiting "unreasonable discrimination" by fixed broadband providers on the theory that it "so limited broadband providers' control over edge providers' transmissions that [it] constitute[d] common carriage *per se*" and finding that the no-blocking rules "would appear on their face" to impose common carrier obligations on fixed and mobile broadband providers).

Twilio's attempt to link messaging classification to the Commission's TCPA precedent also misses the mark. The TCPA applies to those making a "call" – not the underlying providers,[116] and, among other things, restricts the use of an automatic telephone dialing system or an artificial or prerecorded voice to make "any call" to wireless numbers.[117] But there is no indication that a "call" for Section 227 purposes is necessarily a "telecommunications service" under Section 153's definition. Indeed, both Congress and the Commission have used the term "call" when referring to services that could be either "telecommunications services" or "information services" under the Act's definitions, both in Section 227 and elsewhere. For example, Section 223 of the Act makes it unlawful to place "telephone calls" that deliver pre-recorded "dial-a-porn" messages,[118] which are information services.[119]

The fact that numerous other Title II provisions apply to entities that do not provision telecommunications services also reveals the fallacy of Twilio's position. Section 255 imposes

---

[116] This fact alone demonstrates that the TCPA and the Commission's TCPA rules provide no justification whatsoever for classifying text messages as Title II services. Section 227 and the Commission's TCPA rules apply to "any person within the United States." 47 U.S.C. § 227(b)(1). They do not generally deal with the regulation of common carriers that provide telecommunications services.

[117] 47 U.S.C. § 227(b)(1)(A)(iii). The Commission has held that the TCPA applies to "both voice calls and text calls to wireless numbers, including, for example, short message service (SMS) calls." *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd 14014, 14115 ¶ 165 (2003).

[118] *See Sable Communications of Cal. v. FCC*, 492 U.S. 115 (1989).

[119] *See Policies and Rules Concerning Operator Service Access and Pay Telephone Compensation*, Third Report and Order, 11 FCC Rcd 17021, 17031 ¶ 116 (1996) ("We recognize that international pay-per-call, including dial-a-porn, services currently are a significant concern for residential consumers. The record in this proceeding, however, does not clearly establish that international blocking for residential consumers would be either technically feasible or economically reasonable or that it would be effective in helping such consumers limit access to international information services."); *Information Providers' Coalition for Defense of the First Amendment v. FCC*, 928 F.2d 866, 869 (9th Cir. 1991) ("Dial-a-porn is a widely understood shorthand expression to describe a telephone 'information service' that offers sexually-oriented messages . . .").

disability-related requirements on manufacturers, but that doesn't make manufacturers providers of telecommunications services under Title II. Sections 273-275 are related to Bell Operating Company provision of manufacturing, electronic publishing, and alarm monitoring services; the fact that these provisions are found in Title II doesn't transform those activities into telecommunications services. Section 224 governs pole attachments by utilities; the fact that it is in Title II doesn't turn the provision of pole attachments by electric utilities into a telecommunications service.

In sum, the proposition that the FCC has defined texts (including Internet-to-phone texts)[120] as "calls" for purposes of the restrictions in section 227 simply isn't relevant to the issue of whether the service through which the "calls" are transmitted is a telecommunications service or not. Statutory provisions addressing "calls" govern calls, and provisions addressing "telecommunications services" govern telecommunications services. The fact that Title II contains provisions of both types (not to mention some addressing other categories of service) does not mean that all such categories are coextensive. Twilio's argument should be rejected.

Roaming Reexamination Order. Contrary to Twilio's claims,[121] the Commission did not decide the regulatory classification of SMS in the *Roaming Reexamination Order*. Rather, the Commission specifically stated that "nothing in this order should be construed as addressing [the] regulatory classification of push-to-talk, SMS or other data features/services."[122] The FCC undertook no analysis of whether SMS is an interconnected service for purposes of Section 332,

[120] *See* TCPA Declaratory Ruling and Order, 30 FCC Rcd 7961.

[121] *See* Petition at 35.

[122] *Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 15817, ¶ 54 n.134 (2007).

nor did it cite a single comment to suggest that it was. Twilio's assertion that the *Roaming Reexamination Order* somehow compels a finding that SMS is a commercial mobile radio service only underscores the weakness of its Petition.

Consent Decree. The Commission should also reject Twilio's mischaracterization of a recent Enforcement Bureau Consent Decree.[123] A Consent Decree is a compromise settlement and does not constitute a finding of law or fact.[124] By its own terms, moreover, the Consent Decree cannot "be used as evidence or precedent in any action or proceeding" other an action to enforce the Consent Decree.[125] But that is precisely what Twilio is urging the Commission to do here, and it is wholly improper.

VII. THERE IS NO LEGAL BASIS FOR MANDATING DIRECT INTERCONNECTION BETWEEN MESSAGING PROVIDERS.

The Commission must deny Twilio's request for mandatory direct interconnection in the messaging space.[126] As an initial matter, there are no legal grounds for imposing interconnection requirements of any kind – much less direct interconnection requirements – on information services. The Commission has never adopted a rule requiring providers of information services to interconnect their offerings, and Twilio can point to no statutory basis for any such mandate.

In any event, the Act does not even mandate direct interconnection for telecommunications services. Rather, Section 251(a)(1) directs "[e]ach telecommunications carrier" "to interconnect directly *or indirectly* with the facilities and equipment of other

---

[123] *See* Petition at 28-29.

[124] *See AT&T Mobility LLC*, Order, 29 FCC Rcd 11803, 11809 (EB 2014).

[125] *Id*. at 11809-10.

[126] *See* Petition at 4, 9 (calling for "fair interconnection" and alleging that wireless providers deny requests for "direct interconnection").

telecommunications carriers."[127] Twilio provides no rationale whatsoever for imposing more stringent interconnection mandates to messaging than are applied even to telephony.

VIII. CONCLUSION.

For the reasons discussed above, the Commission should reject Twilio's Petition.[128]

Respectfully submitted,

/s/ Thomas C. Power

CTIA – THE WIRELESS ASSOCIATION®

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Brian M. Josef
Assistant Vice President, Regulatory Affairs

1400 16th Street, NW, Suite 600
Washington, DC 20036

Its Attorneys

November 20, 2015

[127] 47 U.S.C. § 251(a)(1) (emphasis added).

[128] As CTIA has explained previously, the Commission also should reject Public Knowledge's petition. *See* Comments of CTIA – The Wireless Association®, WC Docket No. 08-7 (filed Mar. 14, 2008); Reply Comments of CTIA – The Wireless Association®, WC Docket No. 08-7 (filed Apr. 14, 2008).).

Exhibit A

July 18, 2008

Chairman Kevin J. Martin
Commissioner Michael J. Copps
Commissioner Jonathan S. Adelstein
Commissioner Deborah Taylor Tate
Commissioner Robert M. McDowell
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: TCPA Related Informal Consumer Inquiries and Complaints;
Ex Parte Submission in WT Docket No. 08-7

Dear Chairman Martin and Commissioners Copps, Adelstein, Tate and McDowell:

The Federal Communications Commission's Consumer & Governmental Affairs Bureau ("CGB") recently released reports describing consumer inquiries and complaints processed during the third and fourth quarters of calendar year 2007.[1] While the CGB Quarterly Reports over the past ten quarters show that wireless complaint rates per million wireless subscribers have fallen in three of the five reported categories, including the important Contract – Early Termination Fees, Billing & Rates, and Carrier Advertising & Marketing categories, more than half of the wireless-related complaints in the last two quarters of reporting were in the "Telephone Consumer Protection Act" ("TCPA") category.[2] Significantly, these TCPA complaints are associated with autodialing, live or recorded telemarketing calls and "unsolicited commercial e-mail messages to cell phones, pagers, and other wireless telecommunications devices," which are all prohibited activities conducted by third parties that victimize wireless carriers and their customers.

As CTIA has previously noted, individual wireless carriers block as many as 200 million text message advertisements each month, and when they can find them,

[1] Quarterly Report on Informal Consumer Inquiries and Complaints Release, News Release (July 2, 2008) *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-283355A1.pdf (last accessed July 18, 2008).

[2] Wireless-related complaints associated with the TCPA numbered 6,489 in the fourth quarter of 2007 – up more that 50% from 4,113 in the third quarter 2007, and up more than ten-fold from the wireless TCPA complaints the FCC received in the fourth quarter of 2006. In contrast, the FCC received 455 complaints regarding Contract Early Termination Fee complaints for the fourth quarter of 2007; a statistically significant reduction from the 507 Early Termination Fee complaints logged a year before in the fourth quarter of 2006. *See* Quarterly Report on Informal Consumer Inquiries and Complaints Release, News Release (July 2, 2008) *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-283355A1.pdf (last accessed July 18, 2008); Quarterly Report on Informal Consumer Inquiries and Complaints Release, News Release (May 9, 2007) *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-272902A1.pdf (last accessed July 18, 2008).

wireless carriers take these spammers to court to protect their customers from unwanted and costly commercial messages.[3] However, even with all the tools at their disposal, carriers cannot stop every call or unsolicited commercial message that violates the TCPA[4] and CAN-SPAM Act.[5] That is why Congress passed the TCPA, and gave the Commission broad authority to enforce it. Accordingly, I am writing to urge the Commission to work with wireless carriers to increase enforcement efforts against third parties sending unsolicited commercial messages to wireless customers. I offer the wireless industry's full assistance and cooperation in assisting the Commission in fulfilling its statutory mandate to enforce these important consumer protection laws.

As I mentioned, wireless carriers are aggressively deploying multiple strategies to protect their customers from unsolicited commercial calls and messages. The number of wireless TCPA complaints would be far greater if not for these efforts. First, wireless carriers are using filters in their networks to help detect and block text messaging spam from third party spammers, often using Internet IP addresses. Carriers are updating their network filters on an ongoing basis to reflect monitoring for new spamming schemes. Second, carriers are offering their customers a variety of text message blocking features that customers can activate via their handset or a wireless carrier's website to block specific email addresses, domain names, or wireless nicknames, or even block text messaging completely.[6] Third, wireless carriers also have brought civil injunction suits against spammers in selected cases. I am pleased to report that wireless carriers are also working together through CTIA to coordinate efforts to combat these attacks on their networks and customers.

But while prophylactic carrier network maintenance and enhanced customer service are helping to protect and minimize prospective harm to wireless subscribers, carrier efforts alone cannot entirely eliminate the problem. As the complaints logged by CGB make clear, this unlawful third party conduct is disruptive to customers' wireless experiences. This conduct also substantially raises carriers' costs of providing customer care, explaining to customers their options in enhancing their protections going forward, investigating customer complaints and issuing credits. More aggressive investigation and prosecution of these complaints is needed to deter the growth of this fraudulent and oppressive third party conduct. Otherwise, those who are guilty of breaking the law will be emboldened by the knowledge they can evade carriers' civil actions by simply disappearing and popping up under a new

[3] Comments of CTIA – The Wireless Association in WT Docket No. 08-7, *In the Matter of Petition of Public Knowledge, et al. for a Declaratory Ruling that Text Messaging and Short Codes are Title II Services or Are Title I Services Subject to Section 202 Nondiscrimination Rules* (Mar. 14, 2008), at 9, *citing* Kim Hart, "Advertising Sent to Cellphones Opens New Front in War on Spam," THE WASHINGTON POST, A1 (Mar. 10, 2008).
[4] 47 U.S.C. § 227.
[5] 15 U.S.C. § 7701 *et seq.*
[6] "Increased Text Usage Has Carriers Battling Spammers", RCR Wireless News (June 4, 2008).

name, with no fear of meaningful FCC enforcement under Section 503 of the Communications Act.[7]

Just as wireless carriers have significantly increased their efforts to combat these third party violations of the TCPA and CAN-SPAM Act, CTIA urges the FCC to similarly strengthen its enforcement efforts in cooperation with carriers. Moreover, as CTIA urged in its Comments in WT Docket No. 08-7, wireless carriers must retain the ability to protect their customers from fraud, spam, and objectionable material. To ensure that carriers can continue these important efforts, the Commission should reject attempts to regulate SMS and Short Code services as Title II services, subject to the Commission's common carrier obligations.

CTIA and its members stand ready to work with the Commission to investigate and prosecute violations of the TCPA and CAN-SPAM Act. We are eager to explore how the wireless industry can partner with the Commission to better protect the nation's 260 million wireless users from unsolicited commercial calls and messages. I welcome any questions you might have and the opportunity to discuss this matter further at your earliest convenience.

Sincerely,

Steve Largent

cc: Aaron Goldberger
Bruce Gottlieb
Renee Crittendon
Wayne Leighton
Angela Giancarlo
Cathy Seidel

[7] 47 U.S.C. § 503.

CTIA
The Wireless Association®

Expanding the Wireless Frontier

Steve Largent
President/CEO

January 25, 2012

Chairman Julius Genachowski
Commissioner Mignon Clyburn
Commissioner Robert M. McDowell
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554

Re: TCPA Violations Associated with Political Campaigns

Dear Chairman Genachowski, Commissioners Clyburn and McDowell:

Just weeks into the primary season, wireless carriers have experienced a significant increase in consumer complaints and inquiries made to their customer call centers regarding unwanted text messages sent by political campaigns. While the exact content of the unsolicited text messages has varied, many of the messages have been accompanied with a web link or a phone number urging the undecided voters to hear the campaign's message.[1] Some consumers have reported receiving unwanted text messages in the middle of the night, between the hours of 11 p.m. and 5 a.m.[2]

As the Commission has clearly stated,[3] *any* autodialed text message sent to a wireless device violates the Telephone Consumer Protection Act ("TCPA").[4] Not only is the sending of

---

[1] "Vote 2012: Political Text Messages Wake Up Eastern Iowans," KCRG-TV9 (January 5, 2012) *available at* http://www.kcrg.com/news/local/Political-Text-Messages-Wake-Up-Eastern-Iowans-136341073.html (last accessed January 6, 2012).

[2] *See id.*

[3] http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email.

[4] 47 U.S.C. 227. Although political messages are exempted from the prohibitions applicable to "telephone solicitations," section 227(b)(1)(A)(iii) of the TCPA makes it unlawful for *any* person to make *any* call from any automatic telephone dialing system to *any* telephone number assigned to a CMRS customer (other than a call made for emergency purposes or made with the prior express consent of the called party). Moreover, the Commission explicitly has stated that the TCPA applies with equal measure to "both voice calls and text calls to wireless numbers including, for example, short message service (SMS) calls." *See* In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order, 18 F.C.C.R. 14014, 14115 (July 3, 2003).

autodialed text messages disruptive and potentially costly to wireless customers, it also is burdensome to carriers who must expend substantial resources to handle customer inquiries and complaints.

Wireless carriers seek to protect their customers by prosecuting third parties who violate the TCPA. As CTIA previously has indicated to the Commission, carrier efforts alone simply cannot stop every autodialed or unsolicited text message sent to a consumer's wireless device.[5] In cases where they can locate and identify the source of these messages, wireless carriers have vigorously brought suit to shut down TCPA violations and the industry has cooperated with the Federal Trade Commission in its investigation and prosecution of TCPA cases. However, as CTIA has noted, these messages are not originated by carriers, but rather by persons who flout the TCPA. Congress granted the Commission broad authority to enforce the TCPA in order to protect wireless consumers.

The recent TCPA violations involving autodialed political text messages are likely to become more prevalent as political campaigns gear up for this year's local, state, and national elections. Accordingly, I am writing to request that the Commission protect wireless consumers from receiving autodialed SMS text messages. As a first step, the Commission can and should issue a Public Notice advising political campaigns of the limitations the TCPA imposes on autodialed political text messages and announcing the Commission's intent to protect consumers by vigorously enforcing the law.

In addition, we reiterate our request that the FCC reconsider how it categorizes its quarterly report on consumer inquiries and complaints. While wireless carriers are doing what they can to identify and shut down TCPA violations, the Commission catalogs consumers' TCPA reports as "wireless complaints." We believe it is unfair for the FCC to continue to count these instances, which have nothing to do with wireless carriers' behavior, as "wireless complaints." By way of example, in the first six months of 2011 (based on the most recent FCC reports), the FCC logged more than 43,000 wireless TCPA complaints, which led the FCC to report that it received 53,644 wireless complaints instead of the real number of just 10,585 complaints from more than 300 million wireless subscribers (which is approximately 5.5 complaints per million wireless subscribers per month (0.00055 percent/month).[6] The FCC's refusal to properly characterize these consumer complaints significantly and misleadingly expands the apparent rate of consumer complaints about the wireless industry, and for this reason, CTIA once again respectfully asks the FCC to disaggregate TCPA data from its reporting of wireless complaints.

---

[5] See letters from Steve Largent to FCC Chairman Kevin Martin, July 18, 2008, letter from Steve Largent to Acting FCC Chairman Michael Copps, May 7, 2009, and CTIA statements available at http://blog.ctia.org/2010/06/02/additional-thoughts-on-the-fccs-consumer-survey/ and http://blog.ctia.org/2010/10/14/ctia-the-wireless-association%c2%ae-statement-on-the-fcc-meeting/.

[6] The FCC's quarterly informal consumer inquiry and complaints reports are available at: http://www.fcc.gov/encyclopedia/quarterly-reports-consumer-inquiries-and-complaints.

Most importantly, CTIA and its members stand ready to work with the Commission in its investigation and prosecution of TCPA violations. We are eager to explore how the wireless industry can partner with the Commission to better protect the nation's wireless users from unsolicited and unwelcome calls and messages.

I welcome any questions you might have and the opportunity to discuss this matter further.

Sincerely,

Steve Largent

Steve Largent