December 21, 2015

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Wireless Telecommunications Bureau Seeks Comment on Petition for Declaratory Ruling that Text Messages and Short Codes are Title II Services or are Title I Services Subject to Section 202 Non-Discrimination Rules* (WT Docket No. 08-7)

Dear Ms. Dortch,

Fact Atlas respectfully submits the attached white paper as reply comments to help inform the record in the above-captioned docket.[1] In this proceeding, the Commission is considering whether to subject mobile messaging to Title II regulatory mandates. To inform this discussion, we are supplementing the FCC's record with relevant factual insight into the mobile messaging marketplace, which includes discussion of three broad areas:

Consumer Protection. Messaging is the most frequently used smartphone feature today, with more than 1.8 trillion SMS messages being sent in 2014.[2] It is a highly intimate communications medium that allows consumers to be reached in any number of personal locations and settings. In this environment, where consumers open more than 90 percent of text messages within 15 minutes and trust the legitimacy of those messages, it's easy to see why consumer protection is paramount.

Existing Safeguards. The tremendous level of engagement and growth in the messaging environment is based on the fact that consumers trust SMS to carry only relevant, wanted messages. This trusted forum is no accident. It is instead the result of deliberate efforts on the part of the wireless industry and a light-touch regulatory framework that work together to shield

---

[1] Fact Atlas is a communications firm that connects people with the resources they need to make confident choices about mobile products. We write data-driven white papers, case studies, and reports for the mobile industry. For more information, please visit our website, https://www.factatlas.com.

[2] Pew Research Center, "U.S. Smartphone Use in 2015," April 2015, p. 33, accessed at http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf; mBlox, "Ovum Survey Highlights Impact of A2P SMS Price Strategies on Market Growth," February 2015, available from Reuters, accessed at http://www.reuters.com/article/ca-mblox-idUSnBw195788a+100+BSW20150219#gmKfdBu52pS7j3hU.97.

SMS from spam. As a result, today spam is less than one percent of all SMS traffic in the U.S., compared to email spam, which was reported as 67 percent in 2014. There are a variety of options currently available for businesses to protect the messaging marketplace from abuse, including network spam filters and messaging campaign pre-qualification, which are discussed at length in the paper.

Proactive Solutions. The wireless industry is doing many things right to keep spam rates incomparably low. And as the SMS ecosystem continues to evolve and offer new services, the wireless industry has worked collaboratively to facilitate those new services while remaining vigilant in their ongoing endeavor to protect consumers. These proactive efforts must continue in order to safeguard consumers from spam and abuse while leaving room for continued innovation in the messaging ecosystem.

Fact Atlas appreciates the opportunity to provide insight on this important issue. Any questions regarding the attached paper may be directed to the undersigned.

Sincerely,

/s/ Anna Henningsgaard

Anna Henningsgaard
Founder & CEO
Fact Atlas, Inc.

Choice and Innovation

Safeguarding the SMS Marketplace

A FACT ATLAS WHITE PAPER | December 2015

CONTENTS

01 OVERVIEW

03 NETWORK-LEVEL SPAM FILTERS

09 CAMPAIGN PRE-QUALIFICATION

12 TCPA ENFORCEMENT AND CIVIL LITIGATION

13 CONCLUSION

OVERVIEW

By all measures, SMS is a popular way for people and companies to communicate. Consumers open over 90 percent of text messages within 15 minutes. Compare that with email, which has an open rate of only 20 to 25 percent within 24 hours of receipt.[1] Commercial SMS volumes are growing, hitting 1.8 trillion messages in 2014 with projections to reach 2.2 trillion messages by 2017.[2]

According to Pew Research, 67 percent of cell phone owners check their phone for messages proactively, even when the phone is silent.[3] Text messaging is a highly intimate communications medium, ushering messages into back offices, bedrooms, drivers' seats, and vacation homes. Text messaging is both the most widely adopted smartphone feature and the most frequently used, with 97 percent of smartphone owners using text messaging at least weekly.[4]

This level of growth and engagement would not be possible without safeguards to protect the SMS marketplace from abuse.

Consumer Trust is Essential

SMS draws its commercial appeal from consumer trust. Consumers trust SMS because it almost always carries a relevant, wanted message. Compared with email, voice calls, and the U.S. Postal Service, the SMS inbox is pristine. While spam and abuse volumes have grown in proportion with overall SMS traffic volumes, the rate of SMS spam (less than 1 percent[5]) is a fraction of that of email (reported as 67 percent in 2014,[6] and ranging from 54 to 70 percent on a quarterly basis over the past few years [7, 8, 9]).

This is no accident. Industry and light-touch regulatory efforts have deliberately shielded SMS from professional spamming activities, with great success. Protective measures include:

- Network spam filters;
- Campaign pre-qualification; and
- TCPA enforcement and litigation.

1 Cloudmark, "SMS Spam Overview–Preserving the Value of SMS Texting," 2013, p. 2, accessed at https://www.cloudmark.com/en/s/resources/whitepapers/sms-spam-overview
2 mBlox, "Ovum Survey Highlights Impact of A2P SMS Price Strategies on Market Growth," February 2015, available from Reuters, accessed at http://www.reuters.com/article/2015/02/19/ca-mblox-idUSnBw195788a+100+BSW20150219#gmKfdBu52pS7j3hU.97
3 Pew Research Center, "Mobile Technology Fact Sheet," October 2014, accessed on November 3, 2015 at http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/
4 Pew Research Center, "U.S. Smartphone Use in 2015," April 2015, p. 33, accessed at http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf
5 Cathal McDaid, "Big Spam Hunting," January 2014, Adaptive Mobile company blog http://www.adaptivemobile.com/blog/big-spam-hunting, accessed November 3, 2015
6 Maria Vergelis, Tatyana Shcherbakova, and Nadezhda Demidova, "Kaspersky Security Bulletin, Spam in 2014," March 2015, accessed at https://securelist.com/analysis/kaspersky-security-bulletin/69225/kaspersky-security-bulletin-spam-in-2014/
7 Darya Gudkova and Nadezhda Demidova, "Spam and Phishing in Q2 2014," August 2015, available from Kaspersky, accessed at https://securelist.com/files/2014/08/Spam-report_Q2-2014_en.pdf
8 Tatyana Scherbakova, Maria Vergelis, and Nadezhda Demidova, "Spam and Phishing in Q3 2015," November 2015, available from Kaspersky, accessed at https://securelist.com/files/2015/11/Q3-2015_Spam-report_final_EN.pdf
9 Trustwave, "Spam Statistics," January 2015, Trustwave company website https://www3.trustwave.com/support/labs/spam_statistics.asp, accessed November 18, 2015

Abuse management is a balancing act between empowering businesses to innovate and adding friction for bad actors. It's a difficult calculation to make, and it changes over time. It's also essential for the industry to get this right for SMS. The low rate of spam over SMS correlates with high open rates and positive consumer engagement. Fraud prevention, consumer protection, and innovation thus go hand-in-hand.

A Common Goal

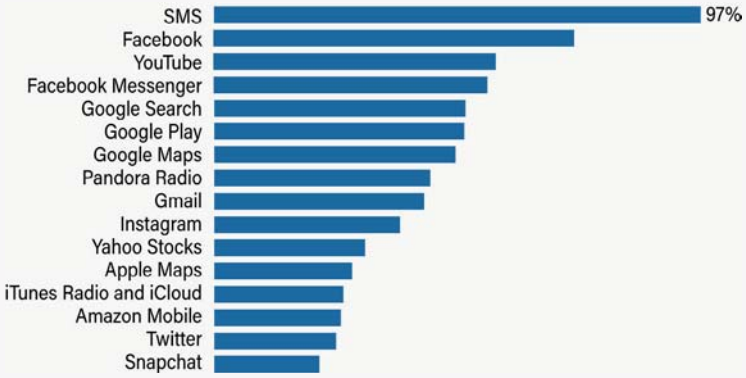
On this issue, regulators and wireless providers are united. Recently, the FCC drew a hard policy line against unsolicited texts and robocalls,[10] but these rules impose damages only after consumer harm is done. The goal of this paper is to open an informed, thoughtful discussion about how, as an industry, we can proactively honor and expand consumer choices around SMS. This requires an exploration of existing safeguards against spam and abuse and reflection on how to make SMS easier for innovative companies to use responsibly.

WHAT IS SMS?

SMS or "short message service" is the technology behind mobile text messaging. SMS works natively on many mobile phones.

SMS looks and acts like other messaging technologies. For example, Apple's iMessage combines internet-based messaging with SMS in the same app. The differences between SMS and an iMessage are almost invisible to the consumer. Most consumers refer to sending SMS or an iMessage as "texting," regardless of which technology they actually use.

Marketers like SMS because it is so widely used. Compare the reach of SMS with the top 15 smartphone apps.[i]



SOURCES: comScore Mobile Metrix, 2015 and Pew Research, 2015

i. comScore, "U.S. Smartphone Subscriber Market Share," June 2015, accessed at https://www.comscore.com/Insights/Market-Rankings/comScore-Reports-June-2015-US-Smartphone-Subscriber-Market-Share

10 Federal Communications Commission [FCC], "Telephone Consumer Protection Act (TCPA) Omnibus Declaratory Ruling (FCC 15-72)," July 10, 2015, accessed at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.pdf

NETWORK SPAM FILTERS

Spam violates consumer choice and causes measurable harm. Virulent spam messages carry unwanted adult content, payday loan scams, and phishing attempts (to name just a few),[11] and high volumes of unsolicited commercial marketing messages degrade network performance.[12] Wireless providers spend millions of dollars to thwart this digital pollution, but spammers only need to convert a small fraction of traffic to profit.

When SMS began to grow in popularity in the early 2000's, two advantages helped shield it from spam. Early price points—upwards of 10 cents per message—were prohibitive for spammers.[13] More importantly, wireless providers had the benefit of watching the rapid growth and negative consumer impact of email spam and took the opportunity to put safeguards in place proactively for SMS. Today, SMS remains relatively free from spam due to the constant and costly efforts of wireless providers and network security companies.

The Evolution of Spam

In their paper "The Economics of Spam,"[14] David Reiley (Google) and Justin Rao (Microsoft) trace the cat-and-mouse game between spammers and email providers beginning in the early 1990's, when professional spammers began automating bulk email delivery. Spam controls evolved quickly, from basic authentication to machine learning, crowd sourcing, and IP blacklisting. The "single most effective weapon in the spam blocking arsenal," IP blacklisting blocks email servers that send unusually high volumes of email.[15]

After two decades of back-and-forth, email providers have claimed victory, but it was hard won. The M3AAWG reports that over 90 percent of all email traffic was "abusive" in Q2 2014.[16] Despite the fact that software from security firms like Symantec can correctly identify and intercept 99 percent of spam emails sent,[17] spam costs Americans approximately $18 billion to $26 billion every year.[18]

The story of SMS spam is a foil for email. Email began its life on the wide-open Arpanet, while SMS emerged in a more limited fashion, enabling communications within each wireless provider's network. The year 2000 introduced cross-wireless provider interoperability for SMS. Once any wireless customer could text any other wireless customer, on any network, SMS blossomed.

With SMS interoperability, consumers quickly adopted asynchronous text messages as a new

11 Symantec, "Internet Security Threat Report," Vol. 20, April 2015, p. 23, accessed at http://www.symantec.com/security_response/publications/threatreport.jsp
12 Nan Jiang, et. al., "Understanding SMS Spam in a Large Cellular Network: Characteristics, Strategies and Defenses," in Research in Attacks, Intrusions, and Defenses, eds. Salvatore J. Stolfo, Angelos Stavrou, Charles V. Wright (Berlin: Springer, 2013), pp. 328-347
13 Justin M. Rao and David H. Reiley, "The Economics of Spam," in Journal of Economic Perspectives, Vol. 26 (3), 2012, pp. 87-110, accessed at http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.26.3.87
14 Ibid.
15 Ibid.
16 M3AAWG, "M3AAWG Email Metrics Program: The Network Operators' Perspective," Report #16, November 2014, accessed at https://www.m3aawg.org/sites/default/files/document/M3AAWG_2012-2014Q2_Spam_Metrics_Report16.pdf
17 Symantec, "Symantec Messaging Gateway for Service Providers," Symantec company website http://www.symantec.com/en/uk/messaging-gateway-for-service-providers, accessed November 18, 2015
18 Rao and Riley, "The Economics of Spam" (see page 3, footnote 13)

way to communicate. Usage soared, going from an average of 0.4 texts per month in 1995 to 35 texts per month in 2000.[19] It wasn't long before companies latched onto this new technology and began automating SMS delivery in bulk. Just ten years after the advent of mass email delivery, SMS faced the prospect of its own spam war.

SMS Spam Protections

Fortunately, the wireless providers were invested in protecting both their customers and their networks' integrity from the outset. As SMS volumes increased, wireless providers put proactive safeguards in place to prevent SMS from reprising email. As SMS spam tactics evolved, wireless providers updated their spam detection algorithms and worked with companies like Cloudmark, Symantec, and Adaptive Mobile to develop sophisticated controls. Spam rates have fluctuated over time, but wireless providers have managed to stay one step ahead of spammers.

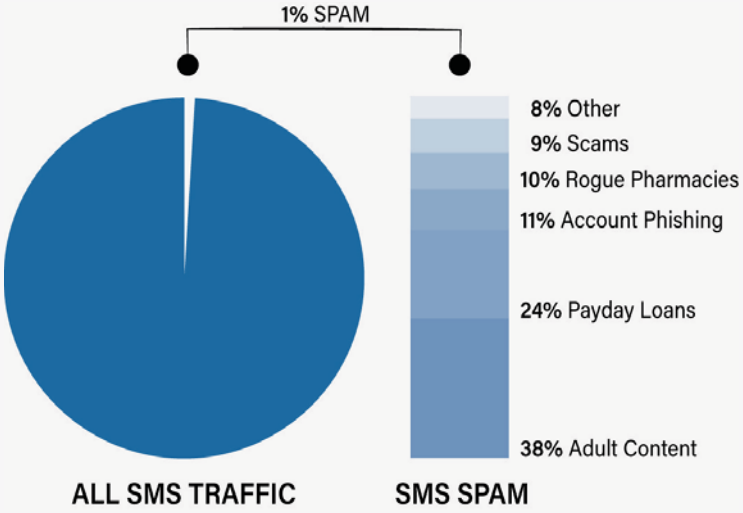
SMS spam is actually more difficult to identify than email spam for a number of reasons:[20]

- Less data to work with and lower overall visibility due to lower overall spam rates;
- Little mobile spam-filtering software compared with email;
- Scarcity of public SMS spam datasets; and
- Limited function of content filters due to short SMS length, idioms, and abbreviations.

SMS SPAM CATEGORIES

Symantec's 2015 Internet Security Threat Report notes that, "an important trend in 2014 was the proliferation of scam campaigns. Although this category was not the most prevalent, it certainly was one of the most dangerous threats using SMS messages."[ii]

Symantec describes scams that con consumers into transferring money or subscribing to paid services, often using classified ads and dating websites. In fact, all of the top spam categories seek to exploit consumers, either by promoting premium subscriptions or stealing data.



SOURCES: Symantec and Adaptive Mobile

ii Symantec, "Internet Security Threat Report," Vol. 20, April 2015, p. 23, accessed at http://www.symantec.com/security_response/publications/threatreport.jsp

19 Christine Erickson, "A Brief History of Text Messaging," September 21, 2012, available from Mashable, accessed November 3, 2015 at http://mashable.com/2012/09/21/text-messaging-history

20 Tiago A. Almeida, José María Gómez, and Tiago P. Silva, "Towards SMS Spam Filtering: Results under a New Dataset," International Journal of Information Security Science, Vol. 2, No. 1, 2013, accessed at http://www.dt.fee.unicamp.br/~tiago/smsspamcollection/IJISS13.pdf

SMS can be routed through many combinations of networks and regions, which complicates tracking. Wireless providers have little time to react to spam in action, but consumers with pay-per-use text plans incur charges for spam as soon as it hits their device. As a result, according to Jiang, et. al., "the focus of the SMS spam defense is to detect and control phone numbers involved in initiating spam (i.e., spam numbers) quickly before they reach a large number of victims."[21]

Spam Profiling & Volumetric Filtering

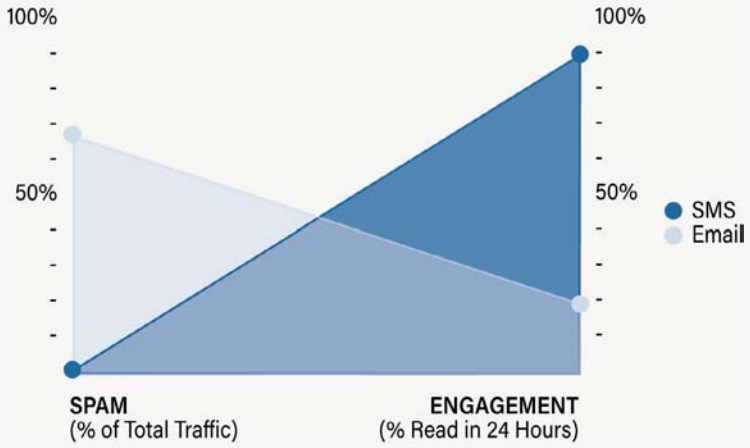
Just as high traffic over a single IP address offered a strong indicator for email spam, high traffic over a single MDN, or 10-digit phone number, correlates strongly with SMS spam. In an analysis performed by the University of Minnesota and AT&T Labs, researchers found that spammers sent far more SMS messages than consumers, while data usage and call minutes on the same spam lines fell below typical consumer usage patterns.[22] Combined with device profiles and other account indicators, this activity footprint can be used to arrest spam while allowing consumer or person-to-person (P2P) traffic to flow freely.

U.S. wireless providers' spam filters work. After years of growth, SMS spam has dropped to less than 1 percent of all SMS traffic in the U.S. today.[23] Compare this with many markets in Asia, where SMS spam exceeds 50 percent of SMS traffic.[24]

NEGATIVE EFFECTS OF SPAM ON ENGAGEMENT

Research has shown that spam exposure leads to significantly lower user engagement, both statistically and in economic terms.[iii] Comparing spam rates for SMS and email with level of engagement reinforces this finding.

Consumers read fewer messages and check messages less frequently when spam levels increase. If SMS spam increases, consumers will find alternative ways to communicate.



SOURCES: Adaptive Mobile, 2014 and Kaspersky, 2015

iii Anirban Dasgupta, et. al., "Impact of Spam Exposure on User Engagement," August 2012, accessed at https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/dasgupta

21 Nan Jiang, et. al., "Understanding SMS Spam in a Large Cellular Network" pp. 328-329 (see page 3, footnote 12)
22 Ibid, p. 337
23 McDaid, "Big Spam Hunting" (see page 1, footnote 5)
24 Cloudmark. "SMS Spam Overview–Preserving the Value of SMS Texting," p. 5 (see page 1, footnote 1)

False Positives & Load Balancing

Any safeguard against bad actors can potentially impact legitimate players. IP blacklists were highly effective at containing email spam, but Rao and Reiley note,[25] "blacklists still routinely cause reliability problems for users trying to send email." Volumetric spam filters for SMS do not impact P2P traffic, but they can impact automated commercial traffic traveling over P2P channels. Commercial marketing traffic can look and act a lot like spam, even if it has a valid opt-in.

As a workaround, many messaging providers engage in load balancing, a practice similar to "snowshoeing" methods perfected by email spammers.[26] For example, messaging provider Twilio offers load balancing as a feature of its Messaging Copilot product. As described on Twilio's website: "Delivery failure increases if you use one phone number to send many messages. [Using Twilio], traffic is distributed across all numbers in a number pool to ensure delivery."[27]

Just because a company engages in load balancing does not mean it is spamming. However, load balancing undermines spam safeguards. It masks the differences between commercial traffic and P2P traffic, making it more difficult for wireless providers to identify and thwart spam.

Instead of masking commercial messaging activity, a better solution is to make legitimate commercial traffic stand out from the noise, to flag it in advance as not-spam. By registering campaigns, service providers can establish a valid "return address" for messages. Combined with strong enforcement controls to prevent known bad actors from jumping back in the pool, pre-qualified campaigns offer the strongest possible safeguard against spam and other abuses.

HOW MARKETERS PROFIT FROM SPAM

The cost to reach consumers varies by advertising channel. In this exhibit, Column 1 shows pricing estimates in the standard advertising industry unit, cost per thousand impressions (CPM). Assuming the average conversion produces profits of $50, Column 2 gives the minimum number of conversions needed, out of one million attempts, for a marketer to profit.[iv]

Advertising Channel	Cost to Reach 1,000 Consumers (CPM)	Conversions Required for Marketer to Profit
Telemarketing	$50 to $250	1,000 in 1,000,000
SMS	$1 to $5	2 in 1,000,000
Webmail Botnet	$0.05	1 in 1,000,000
VoIP to SMS Spam	$0.03	0.6 in 1,000,000

SOURCE: Based on analysis presented in Rao and Reiley (2012)

iv Justin M. Rao and David H. Reiley, "The Economics of Spam," in Journal of Economic Perspectives, Vol. 26 (3), 2012, pp. 87-110, accessed at http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.26.3.87

25 Rao and Reiley, "The Economics of Spam," p. 5 (see page 3, footnote 13)
26 Francisco Pardo. "Global Spam Landscape: Snowshoe Spam," November 2014, available from Symantec, accessed at http://www.symantec.com/content/en/us/enterprise/white_papers/custom-report-spam-outbreak-snowshoe-2014-10.pdf
27 Twilio, "Messaging Copilot," Twilio company website https://www.twilio.com/copilot, accessed November 2, 2015

Promoting Innovation

In the past, there were fewer options for sending bulk traffic over 10-digit phone numbers. However, new technologies and business models have opened a discussion on how to expand this environment. Promising pilots have whitelisted specific numbers for higher volume throughput. For example, the Nordstrom TextStyle campaign uses picture SMS, or multimedia message service (MMS), to connect shoppers with new fashions.[28] In another example, messaging provider Zipwhip has enabled nearly 80,000 landline telephone numbers to send and receive SMS.

Best practices for this environment are still being developed, but the coming year will likely bring exciting advancements for commercial messaging over 10-digit numbers.

WHAT IS SNOWSHOE SPAM?

Digital security firm Symantec has identified snowshoe spam as a growing problem.[v] They introduce the concept with a quote from wisegeek.com:

> *Snowshoes are designed to spread a large weight across a wide area so that the wearer does not break through crusts of snow and ice, and snowshoe spamming distributes a broad load of spam across a varied array of IP addresses… Snowshoe spamming gives more email a chance at getting through.*

Snowshoe spam replicates legitimate marketing messages in format, content, and delivery patterns. Snowshoe spammers even create clusters of fake companies. Once a number is flagged as a source of spam, spammers drop that identity and shift traffic to a new one.

A similar technique can be applied to SMS spam, because it's difficult to track a single originator that is spreading traffic across hundreds or thousands of different phone numbers.

Symantec points out that snowshoe spam campaigns go so far in replicating legitimate marketing, they may include unsubscribe links and headers. SMS spam uses some of these same techniques, and the FTC urges consumers not to text back or click on links in such SMS messages, even to unsubscribe.[vi]

Due to the nature of the snowshoe technique, volumetric spam filters are less effective. Fighting these abusers requires a multi-layered, adaptive approach.

v Francisco Pardo. "Global Spam Landscape: Snowshoe Spam," November 2014, available from Symantec, accessed at http://www.symantec.com/content/en/us/enterprise/white_papers/custom-report-spam-outbreak-snowshoe-2014-10.pdf

vi Alvaro Puig, "Stopping Unwanted Phone Calls and Text Messages," August 2015, FTC blog http://www.consumer.ftc.gov, accessed November 10, 2015

28 Sarah Jones, "Nordstrom simplifies mobile commerce with text message buying," Luxury Daily, May 21, 2015, accessed at http://www.luxurydaily.com/nordstrom-simplifies-mobile-commerce-with-text-message-buying

E2P TEXTING: A CASE STUDY IN INTELLIGENT INNOVATION

A new model for texting called enterprise-to-person (E2P) lets consumers text with landline telephones and 1-800 numbers. E2P texting is conversational, so it's ideal for customer support, reservation reminders, and even non-emergency police lines.

E2P traffic exhibits features of commercial messaging—for example, messages go out to more recipients than a typical consumer's contact list. However, traffic patterns resemble P2P conversations. As a result, E2P traffic presents a challenge for conventional network spam filters.

A pioneer in E2P texting, Seattle-based Zipwhip supports high volume traffic of up to 1,000 messages per second, but only on numbers that follow strict anti-abuse measures.[vii] Zipwhip's platform responds programmatically to the keyword STOP, and it works with a market leading digital security firm to monitor for, and prevent, spam.[viii]

This model for SMS innovation balances valued services with spam prevention and consumer protection. It offers a template for increasing SMS volumes in a careful, intelligent way to benefit consumers.

According to SMS aggregator OpenMarket, 64 percent of consumers prefer texting over voice as a customer service channel,[ix] an ideal use case for E2P texting. Results from early adopters have confirmed that it's a valued service.

In 2013, the National Restaurant Association launched E2P texting on its customer support channels for more than 40,000 members and 500,000 food service establishments. They saw immediate results, including:[x]

- Over 2,000 text conversations per month, leading to 80 percent fewer voicemails;
- Shorter hold times and reduced call abandonment; and
- 4.9 out of 5 customer satisfaction rating for E2P texting.

The market for text services is growing, and success stories like Zipwhip and the National Restaurant Association show that, given the right priorities, innovative companies can balance that growth with consumer protection.

vii Zipwhip, "Zipwhip Toll-Free Texting Now Supports 1,000 SMS/Second," September 2015, available from Reuters at http://www.reuters.com/article/idUSnMKW3XyNra+1d4+MKW20150924#SVhrGF6S8CdbcDXE.97

viii Zipwhip, "Terms of Service" Zipwhip company website http://zipwhip.com/legal, accessed December 20, 2015

ix OpenMarket, "Best Practices for Enterprise-to-Person (E2P) Messaging," July 2015, accessed at http://www.openmarket.com/wp-content/uploads/2015/09/OM-ZW-Best-Practices-for-10-digit-messaging-v1_0.pdf

x Zipwhip, "Zipwhip Transforms National Restaurant Association Customer Support With Toll Free Texting," December 2013, available from Yahoo Finance at http://finance.yahoo.com/news/zipwhip-transforms-national-restaurant-association-141704707.html

CAMPAIGN PRE-QUALIFICATION

Short codes offer an excellent example of pre-qualified campaigns. The process to lease and activate a new short code involves a pre-launch review. This review verifies that campaigns support opt-in and opt-out controls and will not deliver spam or other unsavory or illicit content. Once these are completed, companies are able to send higher volumes of SMS traffic safely. The protections afforded by pre-qualification keep short codes virtually free of spam.

Short codes work natively with SMS. With nearly 92 percent of American adults owning phones that support SMS,[29] short codes offer the cleanest, most ubiquitous digital communication platform available. Because of the underlying compliance framework, short codes offer the most powerful way to reach the widest possible audience. They work seamlessly across smartphones and feature phones alike. The same format works for both Apple's iOS and Google's Android.

Many major brands use a short code: United Airlines, Coca-Cola, Twitter, Uber, Chase, and Wells Fargo, to name a few. Airlines use short codes to deliver flight status alerts. Banks use short codes to deliver fraud alerts. Short codes are a popular vehicle for two-factor authentication, a security practice that sends a temporary password to your mobile phone.

Short Code Fundamentals

Short codes are unique five- or six-digit numbers used to address high-volume SMS campaigns. Businesses or non-profits that lease short codes can use them to send SMS to other text messaging users, but the short code campaigns are administered in a system that prioritizes transparency, customer support, and consent controls for commercial messaging. Each short code supports one or more campaigns, and campaign briefs on file with each wireless provider detail what consumers will experience when interacting with the campaign.

Some service providers lease short codes directly from the Common Short Code Administration (CSCA), which is operated by CTIA and its technology vendor, although many service providers obtain a short code through a reseller. Every company that leases a short code is vetted by CTIA.[30] Vetted companies then submit campaign details to each wireless provider for approval before the short code is activated, or "provisioned," on each wireless provider network.[31]

Independent administration, approval, and activation of short codes enables wireless providers to respond to abuse quickly by suspending a short code without impacting other traffic. With vetting processes in place, known bad actors cannot easily obtain a new short code.

29 Pew Research Center, "Technology Device Ownership: 2015," October 2015, accessed at http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015
30 WMC Global, "CTIA Partner Validation Process," 2014, available from CSCA, accessed at https://www.usshortcodes.com/docs/ctia-wmc-partner-validation-process.pdf
31 Derek Johnson, "SMS Short Codes – What Every Business Needs to Know," January 6, 2015, Tatango company blog http://www.tatango.com/blog/sms-short-codes-what-every-business-needs-to-know, accessed November 3, 2015

A Complex Marketplace

A robust marketplace has formed around short code technologies and services. As providers introduce new capabilities and functionality across wireless providers, the value chain for SMS services grows more complicated. This promotes competition and innovation, which ultimately benefits consumers. However, it also makes the pre-qualification process more complex.

Short codes were originally conceived under a simple framework. A handful of connection aggregators built technology to integrate with wireless provider short code systems.[32] They supported compliance controls, like the universal HELP and STOP keywords, and handled business development for the growing ecosystem. The idea was that different content providers (brands and businesses) would lease a short code from CSCA and plug into connection aggregators to activate it.

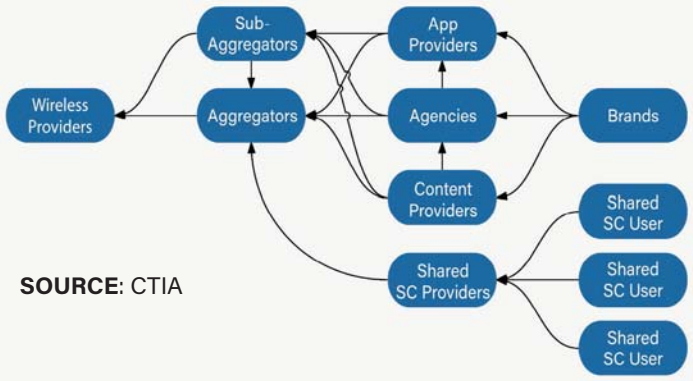
However, some aggregators lacked connectivity across all the wireless provider networks. They sold aggregation services to content providers, but in some cases they had a sub-aggregator relationship. In another example, many major brands hire an agency to manage short codes for them. That marketing agency might work through an app provider for different technology solutions.

To add another layer of complexity, shared short codes introduced an affordable model for smaller businesses like restaurants and doctors' offices that might not need the power and throughput of a dedicated short code. Many short code resellers offer shared leases, effectively subletting different keywords on the same short code to different clients.[33]

SHORT CODE CONNECTIONS

Leasing a short code is easy, but the market for SMS connection services involves a complex web of relationships between multiple wireless providers, dozens of connection aggregators and sub-aggregators, hundreds of intermediaries, and thousands of short code leaseholders.

This diagram shows just some routes companies take to launch an SMS campaign.



SOURCE: CTIA

32 The CSCA lists 11 connection aggregators on its website, http://www.usshortcodes.com/partners/find-a-sms-marketing-partner.php#aggregators-tab
33 Johnson, "SMS Short Codes – What Every Business Needs to Know," (see page 9, footnote 31)

Compliance Policies

The guidlines for running short code campaigns are straightforward and universal; the audit standards are only three pages long. These guidelines used to be more complicated, and for many years industry organizations published two different documents. To alleviate confusion, the Mobile Marketing Association retired the Consumer Best Practices (CBP) document in 2012.[34] Today, all of the Tier 1 wireless providers follow the CTIA Short Code Monitoring Handbook. The latest version, 1.5.2, was published on October 1, 2015.[35]

The stated goal of the Handbook is simple: maintain clarity and consistency and honor consumer choices. All of the requirements in the Handbook roll up under four guiding principles.

- Display clear calls-to-action.
- Offer clear opt-in mechanisms.
- Confirm opt-in.
- Support and acknowledge opt-out requests.

CTIA has the platform to foster broader industry discussions when new policy is developed and released. This is especially important now as the marketplace for SMS grows and evolves. With the introduction of technologies like 10-digit commercial messaging, it will be even more critical to communicate clear, consistent policies and compliance priorities with all stakeholders, old and new.

34 Mobile Marketing Association (MMA), "U.S. Consumer Best Practices For Messaging (Version 7.0)," October 16, 2012, accessed at http://www.mmaglobal.com/documents/us-consumer-best-practices

35 Common Short Code Administration (CSCA), "CTIA Short Code Monitoring Program Short Code Monitoring Handbook," Version 1.5.2, October 1, 2015, accessed November 3, 2015 at http://www.usshortcodes.com/

TCPA ENFORCEMENT AND CIVIL LITIGATION

From the first release of the MMA CBP through to the most recent release of the CTIA Short Code Monitoring Handbook, express informed consent for SMS has been a top priority for the mobile messaging industry. Unlike email, which is based on an opt-out principle, all commercial SMS campaigns require an opt-in. In addition to these industry guidelines, most companies that send SMS must comply with the Telephone Consumer Protection Act (TCPA).

In July of 2015, the FCC sought to address many open questions regarding TCPA. Under TCPA, the baseline for consent to receive SMS marketing is express written consent. In addition, the TCPA restricts autodialed or prerecorded calls and texts to mobile numbers except with the customer's consent

The TCPA allows consumers that receive unsolicited SMS to sue for damages ranging between $500 and $1,500 per violation. When these damages are aggregated in a class action lawsuit, the total costs can be staggering. Over the past year, Capital One settled a TCPA lawsuit for $75 million,[36] Bank of America settled for $32 million,[37] and Gallup settled for $12 million.[38]

The intent of the TCPA is laudable–to protect consumers from unwanted telephone calls, texts, and faxes. Unfortunately, TCPA enforcement and litigation approach suffer from limitations. First, plaintiffs' attorneys have abused the system to impose huge class action lawsuits extorting millions of dollars from businesses for sending transactional communications to reassigned or wrong numbers, even when such communications are sent to people who consented to receive them. Second, TCPA enforcement and litigation are ex post facto remedies, addressing damage only after it is done. While the law has had a chilling effect on new SMS campaigns, it is not sufficient to deter professional spammers.

36 Privacy & Data Security Law Resource Center, "$75M Capital One TCPA Class Deal OK'd; Attorneys' Fees Cut From $22M to $15M," Bloomberg BNA, February 23, 2015, accessed at http://www.bna.com/75m-capital-one-n17179923290

37 Privacy and Security Law Report, "Bank of America $32M TCPA Settlement Receives Final Approval, but Fees Reduced," Bloomberg BNA, September 8, 2014, accessed at http://www.bna.com/bank-america-32m-n17179894572

38 ACA International, "Gallup Agrees to Settlement for Alleged TCPA Violation," August 4, 2015, accessed at http://www.acainternational.org/news-gallup-agrees-to-settlement-for-alleged-tcpa-violation-36468.aspx

CONCLUSION

Giving consumers access to choices means honoring their wishes to receive or opt out of messages, but it also means expanding their access to innovative new services. In the digital environment, spam violates consumers' choices, and too much friction limits innovation. The goal is to strike the right balance of spam protection and abuse prevention to sustain a healthy SMS marketplace.

Today, this goal is achieved through network spam filters, campaign pre-qualification, and, to some extent, TCPA. These protections follow a logical order from proactive and low-friction to reactive and high-friction.

> **Network spam filters** cast the widest net. They are the most affordable and impart the least market friction with the greatest impact. They are best at targeting unsophisticated, widespread abuse that follows predictable patterns.
>
> **Campaign pre-qualification** sets legitimate commercial traffic apart from both P2P and spam traffic. It is highly effective at screening out more sophisticated forms of abuse, adapting to new market conditions, and holding stakeholders accountable.
>
> **TCPA enforcement and civil litigation** has its say after content is delivered. Policy holds specific players accountable for specific instances of abuse. It creates tremendous friction for companies, but the severity of actions and resulting fines establish the highest priority for questions of consent.

The SMS marketplace is healthy. Consumers are engaged. Spam rates are incomparably low. The industry is doing many things right. However, mobile technology and consumer needs are constantly changing and evolving. It is essential for the mobile messaging industry to stay vigilant and proactive in protecting consumers from spam and abuse while fostering innovation

Fact Atlas is a strategic communications firm dedicated to making the mobile landscape easier for companies and consumers to navigate. With proven expertise spanning mobile policy, technology, and business development, the Fact Atlas team delivers data-driven white papers, case studies, and reports.

Fact Atlas was founded by wireless industry veteran Anna Henningsgaard. As a leading expert in mobile compliance, Anna has written widely adopted best practices for commercial SMS, presented before Federal regulators, and facilitated workshops with wireless providers globally. She has worked with the five largest U.S. wireless providers to design and implement compliance programs for a range of third-party content services, including SMS.

This white paper was researched and written with the support of CTIA.

For more information, please visit www.factatlas.com.