TESTIMONY OF MICHAEL ALTSCHUL,
GENERAL COUNSEL, CTIA – THE WIRELESS ASSOCIATION®
before the
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE
"STOPPING FRAUDULENT ROBOCALL SCAMS: CAN MORE BE DONE?"
JULY 10, 2013

Good morning Chairman McCaskill, Ranking Member Heller, and members of the Subcommittee. On behalf of CTIA – The Wireless Association®, thank you for the opportunity to participate in this morning's hearing to explore ways to protect consumers against unlawful robocalls.

Like our customers, wireless carriers are also victims of robocall campaigns by unscrupulous "boiler-room" operators seeking to sell extended car warranties and the like that violate the protections in the Telephone Consumer Protection Act (TCPA). At CTIA, we and our members understand consumer annoyance over these calls and repeatedly have pledged our full cooperation to efforts by the FCC and the FTC to bring enforcement action against these serial violators of the TCPA. In cases where they can locate and identify the source of these messages, our carrier members have vigorously brought suit against the perpetrators, and the industry has cooperated with the FTC in its investigation and prosecution of TCPA cases.

CTIA was proud to support initial adoption of the Telephone Consumer Protection Act in 1991. At that time, there were roughly seven million wireless subscribers in America, and nearly every wireless subscriber also had a landline phone. Today, there are more than 326 million wireless subscriber connections in the United States, including connections for advanced communications devices like smartphones and tablets that access increasingly ubiquitous wireless broadband services. The U.S. wireless industry now leads the world in delivering next generation wireless services. Wireless has evolved from a niche voice service to the primary

source of broadband communications for millions of Americans. Consumers' mass migration to wireless-only service also is a testament to the attractiveness of wireless prices. According to the Bureau of Labor Statistics' Wireless Price Index, the effective monthly cost of wireless service to consumers has fallen more than 40% since December 1997.

At the same time, because of the real reduction in the price of a wireless call, the popularity of rates plans that offer "buckets" of minutes and unlimited calling on nights and weekends, innovative devices and applications, and the added convenience that wireless offers to consumers who value personal and untethered communications, a substantial portion of the population has moved or is moving to "cut the cord" and rely completely on their wireless phones as their only means of communication. Currently more than 35% of U.S. households are "wireless only" for their voice service, and the percentage is significantly higher in some regions and among certain segments of the population.

Of particular significance for today's hearing, the continuing trend to adoption of wireless service as the primary source of communications for millions of Americans, and the changes that have flowed from innovative rate plans and the greater affordability of wireless service, justify a fresh look at the TCPA's treatment of pre-recorded calls to mobile devices.

For instance, given the shift in the way consumers use their mobile devices the TCPA's disparate treatment of informational calls that depends upon whether a company is calling a wireline or wireless phone number -- or, increasingly, a number associated with an interconnected VOIP provider that simultaneously forwards the call to a customer's wireline and wireless numbers -- is increasingly out of date. As currently enacted, the TCPA requires the "prior express consent" of the called party for even informational calls to wireless phones if the calls are prerecorded or use an autodialer; non-commercial informational calls to residential

phones are not similarly restricted. This disparity creates challenges for companies and government agencies that want to provide legitimate informational calls to individuals who are not reachable in any other way and who may value such calls to receive timely information such as notification about a data breach, fraud alert, change in flight time, or other time-sensitive account information.

Even where a consumer has given prior express consent to one entity to receive autodialed calls on her mobile device, that consent would not apply to informational calls from other entities about that purchase. For example, I may have given LL Bean consent to call me on my cell phone when I ordered a new shirt, but that would not permit UPS to notify me about scheduled delivery times. Similarly, I may have given the auto dealership consent to call my cell phone when I purchased my car, but that consent may not extend to the auto manufacturer that wants to later call me about a safety recall.

A key adjustment to the TCPA that would help resolve this issue would be clarification of the statutory definition of an "automatic telephone dialing system" (ATDS), at least as it applies to delivery of informational calls. The TCPA defines an ATDS as "equipment which has the capacity to store or produce telephone numbers to be called, using a random or sequential number generator" and the ability "to dial such numbers." The Federal Communications Commission and some courts have interpreted this definition to include equipment that dials numbers from a list of customer phone numbers that are neither random nor sequential. The equipment simply aids the calling party by automating the process of dialing these intentionally selected numbers. This expansive interpretation potentially leaves wireless customers unable to receive desirable informational messages, like a fraud alert from their bank, while there remain no restrictions on sending the same alert message to the dwindling number of consumers that

maintain a landline phone. A welcome clarification to the TCPA would allow use of ATDS to send informational messages to wireless phones, so long as they are not used to dial numbers sequentially or randomly.

Another outmoded aspect of TCPA implementation is the fact that the Federal Communications Commission continues to catalog consumers' TCPA reports as "wireless complaints," suggesting they are complaints about wireless service, when the complaints are in fact about violations of the TCPA and FCC rules by telemarketers calling consumers on their wireless phones. As I noted at the outset, wireless carriers have taken numerous steps – including bringing lawsuits against robocallers – to protect their customers against unlawful calling campaigns. At CTIA, we understand consumer annoyance over these calls and repeatedly have pledged our full cooperation to efforts by the FCC and the FTC to bring enforcement action against these serial violators of the TCPA.

Yet while wireless carriers are doing what they can to identify and shut down TCPA violations, the FCC continues to misleadingly catalog consumers' TCPA reports as "wireless complaints." We believe it is unfair for the FCC to continue to count TCPA complaints, which are about calls that originate outside of the wireless network and have nothing to do with wireless carriers' behavior, as "wireless complaints." The FCC's refusal to properly characterize these consumer complaints significantly and misleadingly expands the apparent rate of consumer complaints about wireless services. This is important since absent inclusion of TCPA-related complaints, the total number of complaints about wireless service received by the FCC has been declining significantly, dropping from 12/1000ths of one percent of industry subscribership in 2005 to slightly more than 7/1000ths of one percent today. To ensure accurate reporting, we

believe the FCC should disaggregate TCPA data from its quarterly and annual wireless complaint data and report it separately.

Let me turn now to the question of whether technical solutions can help address the problem of unlawful robocalls. While the recent effort by the FTC to use a contest to identify a technical solution that would allow consumers to automatically screen and reject unwanted robocalls produced some interesting proposals, the limited information available to CTIA and the public about these proposals suggests the FTC and others should approach implementation cautiously.

Each of the three winning entries in the contest, including one submitted by two engineers at Google, relies on creation of a "blacklist" database of numbers identified as associated with robocall spammers. All incoming calls to a consumer would be compared with this database, with calls from blacklisted numbers blocked. The database would also include a "whitelist" of numbers associated with entities that have been identified as associated with "legitimate" callers. While there may be value to these solutions, they raise a number of issues that would need to be resolved before any such system can even be considered for implementation.

- **Identification of Blacklist Numbers.** Each of the proposed systems includes a method for identifying numbers to be included on the blacklist – some using consumer input and at least one using a mathematical algorithm. But there are significant issues with either method. Given the ease with which robocallers using modern equipment can mimic the caller ID of any other phone user, a consumer or an algorithm may think it is identifying an illegal robocaller for the blacklist, when it is actually listing the number of an innocent party. Illegal robocallers can also change the numbers they use (or the numbers they mimic) frequently – even "tumbling" a new legitimate number for each individual robocall – limiting the usefulness of the blacklist. This suggests a need to contact the person or business associated with the number in order to provide an opportunity to object to being placed on the blacklist. Would there be an appeal process? Would there be criteria for moving an innocent customer from the blacklist to the whitelist?
  In addition, one person's unwanted annoying robocall may be another person's important informational message. One consumer may suggest adding a political candidate's

number to the blacklist because he or she is annoyed with the candidate's message, while others may welcome such messages. It is unclear how an algorithm could even distinguish between wanted and unwanted robocalls.

- **Identification of Whitelist Numbers.** Before implementation, rules would need to be worked out and a system administrator appointed to determine how, and on what basis, a robocaller could get its number added to the whitelist. Would there be an appeal process? What would be the criteria for moving a bad actor from the whitelist to the blacklist?

- **Caller ID Spoofing.** Even assuming an accurate database of blacklisted and whitelisted numbers can be compiled and maintained, the ease with which modern equipment and software can allow a caller to hide its identity by spoofing a caller ID would present significant challenges. It would, for example, be relatively simple for an illegal robocall spammer to spoof one or more of the numbers on the whitelist to get its calls through the protection system. While the Truth in Caller ID Act prohibits spoofing of caller IDs for fraudulent or harmful purposes, unlawful robocallers – especially those that are calling from outside the United States – that aren't deterred from violating the TCPA would likely have little concern about also violating the caller ID law. Identifying illegal robocallers that are spoofing caller ID is made significantly more difficult if the robocaller uses modern Voice over Internet Protocol (VOIP) technology, which if routed through a proxy server becomes virtually impossible to trace.

- **Scaling.** Because unlawful robocallers typically use a large number of telephone numbers and change telephone numbers frequently, the database for the blacklist would be very large and continually growing, requiring a significant investment for both acquisition and maintenance of computer resources. Perhaps more significantly, the capacity in both telecommunications and computer resources needed to route to the database for comparison all of the calls robocallers may make to the tens or even hundreds of millions of persons who may sign up for the service would be massive.

- **Administration and Operation of the System.** Any robocall blocking system of the type proposed in the FTC contest would involve a fairly massive administrative and operational effort. It should not be expected that carriers can be the implementing entities. The significant costs of the system aside, a single carrier could reasonably compile and maintain a robocall blacklist that would be associated only with the illegal robocall identification and calling preferences of its own customers. Thus no system operated by a single carrier could be as comprehensive as it would need to be to be effective. In addition, wireless carriers, as legal common carriers, must deliver calls that are placed on their networks. While a subscriber that opted in to the proposed robocall blocking system may be considered to have authorized the blocking, the carrier may not block calls from a legal robocaller on its network, absent specific statutory or regulatory authority to do so.

- **Privacy Issues.** At least one reported robocall solution would require the carrier to allow the solution administrator to screen subscribers' incoming calls to determine whether they are from an illegal robocaller or a legal robocaller or live individual. Even if this

> kind of snooping is authorized by the recipient of the call, such a potentially invasive technology raises serious questions about consistency with the law and rules governing the privacy of customer proprietary network information and a carrier's traditional responsibility to avoid intercepting or divulging the content of communications other than in narrowly circumscribed instances.

We appreciate the efforts of the FTC and others who are exploring technologies that may minimize the transmission of illegal robocalls to our customers. As the foregoing suggests, however, any technical solutions must be subject to careful and complete consideration. Particularly at this early stage of development, it would be premature to impose any technical solution as a mandate.

Finally, whether as part of a technical solution to robocalls or as part of any amendment to the TCPA, nothing should be done to upset the FCC's longstanding conclusion under the TCPA that wireless carriers need not obtain additional consent from subscribers prior to initiating autodialed calls at no cost to their subscribers. These important and beneficial customer service calls may be used to notify customers of billing alerts, low balance alerts on prepaid phones, and usage alerts informing customers of approaching limits for voice, data, or messaging plans. In encouraging wireless carriers to provide this information to their customers, the FCC has consistently recognized the benefits of such calls between wireless carriers and their customers and recognized that Congress had no intention of hindering these communications. Any new solution to illegal robocalling, whether technical or through increased enforcement, should not upset this key communication between wireless providers and their customers.

On behalf of CTIA, thank you for your consideration of these suggestions. We look forward to working with you to address these and related matters as the Subcommittee moves forward with its work.