

II. DISCUSSION.

In the *Notice*, the Commission seeks “discussion, analysis, and consideration” of the questions concerning intentional interruptions of commercial wireless service by government authorities. A discussion of these issues is useful to increase awareness of the public interest harms that can result from interrupting commercial wireless service and to educate governmental authorities on the existence of the protocols in SOP 303 to deal with those rare situations where an emergency might necessitate an interruption in wireless service. Yet, the Commission’s inquiry should end there, as the existing SOP 303 protocols make it unnecessary for the Commission to analyze and consider substantive issues associated with government desires to interrupt wireless service.

A. Interrupting Wireless Service Can Do More Harm Than Good.

Comments filed in response to the *Notice* are nearly unanimous that interrupting wireless service should be discouraged. AT&T agrees that interrupting wireless service should be an option of last resort, invoked only in exceptional situations in accordance with a standard set of rules to ensure that the inquiry arises from an authorized government or public safety official and relates to a credible threat. Wireless service is no longer a luxury; it is essential to our daily lives. Americans rely on wireless service more today than ever before and that reliance will continue to grow over the next few years. Shutting off wireless service would impact the ability of the American public to communicate important information to friends and family, to dial 9-1-1 during an emergency, and to assist law enforcement authorities. It would also interfere with the ability of government authorities using commercial wireless service to deal with the emergency that may be present.

Given that reality, interrupting wireless service may place the public at greater risk than the impending threat that leads government authorities to seek a shutdown of the service, and should be carefully considered and used sparingly, only within rigorous and well-defined parameters. In fact, those parameters are already in place with SOP 303. AT&T agrees with CTIA that “it is not necessary for the [Commission] to undertake a substantive proceeding on these issues at this time, given that protocols for wireless service interruptions are already in place.”²

B. SOP 303 Provides the Protocols to Consider Service Interruptions in Response to a Credible Threat.

In 2006, the National Communications System adopted SOP 303, which provides the steps for government authorities to shutdown and restore the nation’s wireless networks in the event of a credible threat to public safety. SOP 303 was developed following a collaborative process with the President’s National Security Telecommunications Advisory Committee, the Commission, the Department of Homeland Security, the Federal Bureau of Investigation, the New York Department of Homeland Security, and other government and private sector entities, including members of the wireless industry. SOP 303 obviates the need for the Commission to engage in a process to consider the substantive questions posed in the *Notice*, all of which were considered in the process leading to the adoption of SOP 303.

SOP 303 provides very well delineated processes for shutting down and restoring wireless service, and as Verizon states, “contains all of the elements that wireless customers and carriers need to ensure that a decision to order a shutdown has been carefully considered, fully

² Comments of CTIA – The Wireless Association®, GN Docket No. 12-52 at 1-2 (filed April 30, 2012).

vetted and comes from a single reliable source.”³ SOP 303 identifies the governmental authorities that are authorized to make a request to interrupt wireless service and provides processes for authenticating those persons, addressing any shutdown request among the appropriate Federal and State agencies, and communicating the need to interrupt wireless service to wireless providers and industry groups if a credible threat is presented. These verification steps insure that requests to interrupt wireless service are subject to rigorous scrutiny, just as they should be. And, this scrutiny provides the consistent and reliable process that gives all participants confidence that wireless service is not interrupted except in situations that would present a real peril to the public interest.

Further, SOP 303 implements a single, nationwide process for evaluating the potential interruption of wireless service, shutting down wireless service, and restoring the service. In the absence of SOP 303, many State and local governments would adopt their own rules and regulations for trying to interrupt wireless service in emergency situations, which would impose an extreme burden on the wireless industry. Requiring the wireless industry to follow a hodge-podge of different rules would, as CTIA observes, “(more dangerously) sow confusion and delay during situations where coordination and efficiency is paramount.”⁴ Moreover, the lack of a uniform process presents the risk that State and local rules and regulations would conflict (or be otherwise inconsistent with) Federal laws or other State laws, creating not only uncertainty about implementation, but potentially putting wireless providers in the untenable position of deciding which rules and regulations apply, e.g. compliance with the rules and regulations of one

³ Comments of Verizon Wireless, GN Docket No. 12-52 at 6 (filed April 30, 2012).

⁴ Comments of CTIA at 4.

jurisdiction would violate the rules and regulations of another jurisdiction. Wireless providers are simply not in the position to make, and do not want to make, these assessments.

All of these substantive issues have been vetted in the SOP 303 process, and it would be counterproductive, and undermine SOP 303, for the Commission to again evaluate in this docket the substantive issues associated with interrupting wireless service when needed to deal with a credible public threat. For these reasons, the Commission should avoid undertaking any substantive review of the issues in this docket and recognize the existing protocols in SOP 303 as the main vehicle to address a credible threat that necessitates an interruption in wireless service.

Dated: May 30, 2012

Respectfully submitted,



Robert Vitanza
Gary L. Phillips
Peggy Garber

AT&T Services, Inc.
208 S. Akard St
Rm 3110
Dallas, TX 75002
(214) 757-3357 (Phone)
(214) 746-2213 (Fax)
robert.vitanza@att.com