**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Commission Seeks Comment on Certain Wireless Service Interruptions | ) | GN Docket No. 12-52 |
| | ) | |

**COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®**

CTIA – The Wireless Association® ("CTIA") hereby submits these comments in response to the Commission's Public Notice regarding concerns and issues related to intentional interruptions of wireless service by government authorities for the purpose of ensuring public safety.[1] CTIA agrees with Chairman Genachowski's statement in the wake of the San Francisco's Bay Area Rapid Transit system ("BART") August 11, 2011 decision to shut off the transit system's underground cell phone network[2] that "communications networks that are open and available are critical to our democracy and economy" and that "[f]or interruption of communications service to be permissible or advisable, it must clear a high substantive and procedural bar."[3] Although CTIA commends the Commission for raising these concerns, it is

---

[1] Commission Seeks Comment on Certain Wireless Service Interruptions, Public Notice, GN Docket No. 12-52 (Mar. 1, 2012) ("Public Notice").

[2] Michelle Cabanatuan, *BART Admits Halting Cell Service to Stop Protests*, San Francisco Chronicle (Aug. 13, 2011), *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/08/12/BAEU1KMS8U.DTL.

[3] News Release, *FCC Chairman Julius Genachowski's Statement on BART Policy Adoption* (Dec. 1, 2011), *available at* http://www.fcc.gov/document/fcc-chairman-julius-genachowskis-statement-bart-policy-adoption.

In response to widespread criticism of the shutdown, the transit agency's board of directors adopted a new "extraordinary circumstances" blackout policy under which temporary wireless service interruptions are only acceptable where there is strong evidence of imminent unlawful activity that threatens Public Safety. Mike Anderson, *BART Adopts New Cell Phone Blackout Policy*, MSNBC (Dec. 1, 2011), *available at* http://usnews.msnbc.msn.com/_news/2011/12/01/9149242-bart-adopts-new-cell-phone-blackout-policy.

not necessary for the FCC to undertake a substantive proceeding on these issues at this time, given that protocols for wireless service interruptions are already in place.

CTIA recognizes that restricting wireless service may be an appropriate action in particular high-risk crises where authorities determine that an interruption of wireless service is necessary to promote the public's safety. In these extremely rare instances, CTIA supports the use of existing protocols for dealing with emergency situations, and stresses that the considerable risks implicated by disabling wireless service during emergency situations generally weigh against taking such action. While more can be done to ensure that Public Safety officials – particularly those at the state or local level – are made aware of the procedures available to them in emergencies, the Commission need not undertake a time-consuming process to develop new procedures at this time.

## I. PAST PRACTICES AND PRECEDENTS.

The Commission seeks comment on what policies and rationales have been developed by public agencies to support or provide guidance on wireless service interruptions.[4] As the Commission acknowledged in the Public Notice, there is an existing protocol in place for authorities to initiate a request for service interruption during emergencies. The National Communications System's Standard Operating Procedure 303, "Emergency Wireless Protocols" ("SOP 303"), outlines a shutdown and restoration process for use by commercial and private wireless networks during national crises. This process was developed under the President's National Security Telecommunications Advisory Committee, in coordination with representatives from the FCC, the Department of Homeland Security, the Federal Bureau of Investigation, the New York Department of Homeland Security and other government

[4] Public Notice at 3.

representatives, as well as private sector stakeholders. CTIA supports the continued use of and reliance on this protocol during emergencies.

Under SOP 303, the National Coordinating Center ("NCC") is the focal point for coordinating actions leading up to and following the termination of wireless connections. A designated Federal, state, or local law enforcement official or member of government will submit a request to the NCC, which will ask a series of questions of the requesting official to determine whether the shutdown is necessary. The NCC will then notify carriers in the affected area and coordinate the reestablishment of service as soon as possible once the shutdown is no longer required.

The development and implementation of SOP 303 involved substantial government and industry stakeholder participation, with the wireless industry supporting the procedures adopted. CTIA is a strong advocate for stakeholder-developed solutions to wireless Public Safety issues, and believes that the processes that went into creating SOP 303 have made it a particularly effective means for dealing with emergency situations. CTIA therefore supports the use of existing protocols such as SOP 303 for dealing with situations where wireless service interruption is necessary to achieve a Public Safety goal. There is no need for the Commission and industry stakeholders to undertake a complicated, burdensome process to explore alternative means.

While SOP 303 has the support of the wireless industry and has been closely reviewed by government stakeholders, CTIA believes that improved communication and education regarding SOP 303 with Public Safety entities, particularly at the state and local level, will be beneficial. This educational effort will help make Public Safety representatives aware of the options available to them and the steps to be taken in the event an emergency necessitates a wireless

service interruption. Rather than address this issue through a Commission proceeding or through a broad education campaign, the NCC should provide this information to the appropriate contacts within the affected Public Safety entities on a "need to know" basis only. This will help ensure that relevant authorities know how to avail themselves of SOP 303 in the event of an emergency, and will help facilitate a coordinated response to the situation, without widely distributing a procedure with significant homeland security sensitivity.

CTIA also supports the use of a single protocol by local, state, and Federal agencies. The Public Notice suggests that some states and/or localities may seek to establish their own procedures for effectuating a wireless service interruption, separate from the existing Federal protocol.[5] It is unclear whether these plans would require a Public Safety authority to follow only the state or local procedure, or adhere to SOP 303 in addition to the state or local procedure. CTIA is very concerned that the development of multiple protocols would not only waste resources, but would (more dangerously) sow confusion and delay during situations where coordination and efficiency is paramount. The mere existence of multiple procedures at the state or local level undermines the Public Safety goals of these programs.

## II. RISKS IN INTERRUPTING WIRELESS SERVICE.

As CTIA has demonstrated in past proceedings, any interruption of wireless service, particularly in a potential emergency situation, carries significant Public Safety risks. It is for this reason, for example, that CTIA and its members have been so concerned about the use of wireless jammers in prisons and in other contexts.[6] And service interruptions – even to aid in response to a national emergency – always create the potential for adverse consequences. As the

---

[5] Public Notice at n. 6.

[6] *See, e.g.*, Petition to Deny of CTIA – The Wireless Association, WT Docket No. 09-30 (Mar. 13, 2009).

Commission noted in the Public Notice, 70 percent of 9-1-1 calls now originate from wireless phones.[7] It is undisputed that wireless technologies have played a critical function in protecting Public Safety, and a service interruption could result in a 9-1-1 call not being connected, communications among authorities being thwarted, and non-9-1-1 critical communications by individuals left unconnected – and all this presumably during the most dangerous or hazardous situations.

The 2008 terrorist attacks in Mumbai demonstrate the important role that wireless connectivity can play during a national crisis. During the attack, mobile phones often became the sole source of information to the Public Safety officials arriving on the scene, as well as the source of contact for victims, with SMS messages sent to friends and family asking for help and updates leading to critical information for those caught in the violence.[8] In one case, a film crew trapped in a hotel received a text message with floor plans that enabled the crew to find its way to safety.[9]

SOP 303 allows authorities to consider issues such as those raised by the Mumbai attacks, as the protocol requires that various questions be answered by the party making the request to determine whether cellular service disruption is the correct response based on the nature of the threat. For this reason, CTIA supports the approach outlined in SOP 303, as it enables authorities to balance the benefits of maintaining wireless service for potential victims of an emergency against the harms that could be perpetrated by maintaining connectivity.

---

[7] Public Notice at 1.

[8] Timon Singh, *How Social Media Was Used During the Mumbai Attacks*, Next Generation Online (Nov, 26, 2009), *available at* http://www.ngonlinenews.com/news/mumbai-attacks-and-social-media/.

[9] *Id.*

## III. SCOPE OF INTERRUPTION.

The Commission has expressed concern that the scope of a service interruption would preclude other emergency communications, such as 9-1-1 calls and wireless emergency alerts. CTIA stresses to the Commission that during a full wireless service interruption, no 9-1-1 calls can be made in the affected area, and wireless customers in the affected area will not receive wireless emergency alerts. The existing protocol helps minimize the scope of interruption by ensuring that these service interruptions are rare and that they are promptly ended once the emergency has passed.[10]

## IV. CONCLUSION.

For the reasons outlined above, CTIA has significant concerns about any interruption of wireless service, but recognizes that in certain emergency situations a service interruption may be necessary to prevent or stop a life-threatening emergency. However, instead of expending resources on developing new policies that could possibly create confusion and delay, relevant

---

[10] *See* NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, 2009-2010 NSTAC ISSUE REVIEW 155 (2010), *available at* http://www.ncs.gov/nstac/reports/2009%20-%202010%20Issue%20Review%20(FINAL).pdf ("The NCC will also ask the requestor a series of questions to determine if the shutdown is a necessary action. After making the determination that the shutdown is no longer required, the NCC will initiate a similar process to reestablish service.").

Federal officials should ensure that existing procedures are made known to other Federal, state, local law enforcement and homeland security officials so that these carefully-developed procedures can efficiently be put into action when needed.

Respectfully submitted,

By: */s/ Brian M. Josef*

Brian M. Josef
Assistant Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

CTIA – The Wireless Association®
1400 16th Street, NW, Suite 600
Washington, D.C. 20036
(202) 785-0081

Dated: April 30, 2012