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 VERIZON WIRELESS

Verizon Wireless hereby responds to the Commission's Public Notice seeking comment on concerns and issues related to intentional interruptions of Commercial Mobile Radio Service by government authorities for the purpose of ensuring public safety.[1] In the Public Notice, the Commission recognizes the important role that wireless communications play in protecting public safety, but notes that wireless networks can be used in ways that put public safety at risk – such as to trigger an explosive device or organize violent activities. It notes, further, that the intentional wireless service interruption of the BART system in California last summer drew criticism. It therefore seeks comment on a number of legal and policy questions surrounding intentional wireless service interruptions.[2]

Verizon Wireless shares the Commission's concerns regarding any intentional interruption of wireless service. Wireless service interruption for public safety reasons should only be considered as a last resort. Wireless customers and the carriers that serve them need to know that the risks and benefits of ordering an interruption have been thoroughly considered,

---

[1] Public Notice, *Commission Seeks Comment on Certain Wireless Service Interruptions*, GN Docket No. 12-52, DA 12-311 (rel. Mar. 1, 2012).

[2] *Id.,* at 2.

along with potential alternatives, and need government authorities to speak in a single, clear and consistent voice. Fortunately, the Department of Homeland Security's National Communications System (NCS), working with carriers and government officials, has already developed an "Emergency Wireless Protocol" (EWP) -- a shutdown and restoration process for commercial and private wireless networks during emergencies.[3] The Commission should embrace the EWP as the protocol for considering and requesting a wireless network shutdown and subsequent restoration.

I. WIRELESS SERVICES PLAY A CRITICAL ROLE IN TIMES OF EMERGENCY.

In deciding whether to request that wireless carriers shut down their networks in response to a perceived public safety threat, government entities must consider the critical role that wireless services play in times of emergency. Public safety officials and first responders often rely on commercial wireless networks to communicate during and after an emergency. Wireless voice services are extensively used at all levels of government to connect with other agencies that are not on the same public safety network. Wireless mobile data terminals, whether using 3G and/or 4G networks, are widely used by police, fire departments, EMTs, HAZMAT teams, and others for accessing databases, EMT telemetry, and other essential data services. Many emergency services providers rely on Wireless Priority Service (WPS) to gain access to commercial wireless radio channels when networks are congested.[4]

---

[3] *See* National Security Telecommunications Advisory Committee, 2009-2010 NSTAC Issue Review at 155 (2010), *available at*: http://www.ncs.gov/nstac/reports/2009%20-%202010%20Issue%20Review%20(FINAL).pdf ("EWP Summary").

[4] *See* http://www.fcc.gov/encyclopedia/wireless-priority-service-wps.

Wireless consumers likewise depend on wireless services during times of crisis. As noted in the Public Notice, about 70 percent of all 911 calls are placed from wireless devices.[5] In addition, the recently-launched Commercial Mobile Alert Service (CMAS, also known as Wireless Emergency Alerts or WEA), provides a means of sending alerts to wireless consumers about events that threaten public safety.[6] Wireless services are also frequently used by members of the public or victims of an attack to get information about what is transpiring, communicate with family and friends, or provide critical information about the event to law enforcement or first responders. Government officials must understand and consider the important role wireless services play during an emergency in determining whether and to what extent to request a shutdown of wireless networks.

II. INTERRUPTING WIRELESS SERVICES MUST BE CAREFULLY CONSIDERED BECAUSE IT COULD CAUSE MORE HARM THAN GOOD.

In considering whether to request a wireless network shutdown, the government must consider all of the implications of interrupting wireless services. First, given the propagation characteristics of wireless signals, which vary depending on the frequency bands used, geography and environmental conditions, in order to prevent any usable commercial wireless signal from reaching any particular geographic area, it is likely that cell sites located several miles away from the target area must be turned off. As such, any wireless network shutdown is likely to impact communications in areas well beyond the target area.

Second, smartphones, tablets, computers, and other wireless communications devices are increasingly able to access and communicate using wireless signals, such as Wi-Fi, emanating

---

[5] Public Notice at 1.

[6] *See* http://www.fema.gov/emergency/ipaws/cmas.shtm.

from sources other than commercial wireless networks. Accordingly, shutting down commercial wireless networks may not prevent all devices from being used for nefarious purposes.

Third, government officials must carefully weigh the benefits and detriments of asking wireless carriers to shut down service. In particular, officials must consider the extent to which wireless services may be used to assist in the response to an event and consider those benefits prior to ordering a shutdown. For example, during the Mumbai terrorist attacks in November of 2008, the terrorists relied upon mobile communications to coordinate the attacks. However, those same airwaves were used during the attacks by victims to provide public safety officials with information about the attacks and even to escape the attackers.[7] While shutting down wireless networks in that case may have deterred the terrorist activities, it might also have prevented victims from communicating with law enforcement to provide valuable information about the attack and from escaping the terrorists.[8]

III. WIRELESS CARRIERS NEED A UNIFORM NATIONWIDE PROCESS FOR CONSIDERING INTENTIONAL SERVICE INTERRUPTIONS.

Verizon Wireless understands that there may be some cases where shutting down wireless service to an area is necessary. In such cases, wireless carriers need a process for ensuring that the decision to shut down the network has been appropriately vetted and that the request comes from a single, reliable source. That process should have several important

---

[7] *See* 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/.

[8] After shutting down wireless service in the New York City tunnels in 2005 in reaction to the London subway bombings, the head of the New York City Port Authority stated that if he knew when he made the decision what he knows now, he would not have shut down wireless service in the tunnels.

elements. First, there should be a single nationwide process for considering whether to seek a shutdown. Multiple processes among the various (Federal, State, local) jurisdictions will inevitably lead to confusion and inconsistent requests where multiple authorities may be involved.[9]

Second, wireless customers and the carriers that serve them need to know that the decision to seek a service interruption has been made after considering as many of the costs and benefits of a shutdown as can be considered given the exigency of the situation. In particular, the decision should be based on consideration of the nature of the threat, the likelihood that shutting down commercial wireless service will be effective in addressing the threat, the availability of other, less-intrusive means of addressing the threat, and the negative impacts to consumers, victims, law enforcement and first responders associated with shutting down commercial wireless service to the area.

Third, wireless carriers need a process where the request comes from a single, trustworthy source. Carriers should not be put in the position of having to sort through multiple communications from multiple government entities. The same single source should also be responsible for letting the carrier know when it is safe to restore service to the area. The existence of a single process with each of these elements will eliminate doubts and confusion and will lead to a much quicker execution of the network shutdown.

---

[9] This concern is not hypothetical. As the Public Notice mentions, there is currently legislation pending in at least one State, California, contemplating a separate process for wireless (and wireline) network shutdowns in that State. Public Notice at 2, note 6.

IV. THE FCC SHOULE EMBRACE THE EMERGENCY WIRELESS PROTOCOL AS THE SINGLE NATIONAL PROCESS FOR ORDERING WIRELESS SERVICE INTERRUPTIONS.

The Department of Homeland Security's National Communications Service has already developed a wireless service interruption protocol, the EWP, that should embraced as the single national process for considering whether to ask carriers to interrupt service. The EWP was developed by the NCS working with members of the National Coordinating Center (NCC), including Verizon Wireless and other carriers.[10] Under the EWP, the NCC serves as the central point for coordinating any actions leading up to and following the termination of wireless service. Any decision to shut down wireless service will be made by State Homeland Security Advisors, their designees, or representatives of the DHS Homeland Security Operations Center. The NCC will receive the request to shut down wireless service, ask the requesting entity a series of questions to determine if shutdown is necessary, then, if a shutdown is determined to be necessary, notify the affected carriers in the area of the decision. It will follow a similar process to restore service.[11]

The FCC should embrace the EWP as the single nationwide process for considering, requesting and terminating a wireless network service interruption. The EWP 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 vetted and comes from a single reliable source. To date, the EWP has been tested in DHS exercises, but not used in an actual emergency. In addition, some

---

[10] The NCC is a joint industry-Government operation whose mission is to assist in the initiation, coordination, restoration, and reconstitution of industry and Government national security and emergency preparedness (NS/EP) telecommunications services or facilities during natural disasters, armed conflicts, and terrorist attacks.

[11] *See* EWP Summary.

Federal, State and local officials may have not yet been briefed about or trained to implement the EWP.

V. CONCLUSION

Wireless service should only be interrupted as a last resort when it is determined that shutting down wireless networks is the best and only way to address a perceived threat to public safety. Any reqeust for a wireless service interruption should come from a single reliable source and should be made after carefully considering the negative ramifications of a shutdown and potential alternatives. The Emergency Wireless Protocol is a process developed to ensure that a decision to order a shutdown has been carefully considered, fully vetted and comes from a single agency. The FCC should embrace the EWP as the single nationwide process for considering and implementing a wireless network service interruption.

Respectfully submitted,

VERIZON WIRELESS

By: _____

John T. Scott, III
Andre J. Lachance
VERIZON
1300 I Street, N.W.
Suite 400-West
Washington, D.C. 20005
(202) 589-3760

Michael E. Glover
Of Counsel

Attorneys for Verizon Wireless

Dated: April 30, 2012