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

In the Matter of	)	
	)	PS Docket No. 10-255
Framework for Next Generation 911 Deployment	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology respectfully submits these brief comments on the Notice of Inquiry in the *Matter of Framework for Next Generation 911 Deployment*, PS Docket No. 10-255, as released December 21, 2010.[1] We applaud the Commission for a forward-looking inquiry about the 911 system, one that looks beyond the legacy 911 system to the potential of a "NG911" IP-based emergency system. We urge the Commission to act to promote an effective and technologically advanced emergency reporting and communications system, based on open technical standards and facilitating broad access to the emergency system. In doing so, however, the Commission must exert great care that its rules do not retard technological progress in the emergency system, and do not stifle innovation and consumer choice in technology more broadly. We look forward to working with the Commission to promote an effective and advanced emergency system.

[1] *In the Matter of Framework for Next Generation 911 Deployment,* PS Docket No. 10-255 (released Dec. 21, 2010) ("NOI").

INTRODUCTION AND OVERVIEW

The goal of promoting technological innovation and the offering of advanced services applies both in the emergency context and more broadly. In the emergency context, the Commission should avoid actions that would discourage developers and providers of new IP-based services from seeking to connect those services into the NG911 system. By setting very high or rigid requirements for services to be able to communicate into the NG911 system, the Commission might inadvertently reduce the ability of future technology users to connect to the emergency system. If the NG911 system has such specific requirements that only a few "new" services can comply, then in 10 or 15 years we may find ourselves right back where we are today – with an outdated emergency system that has been left behind by advancing technology.

At the same time, the Commission should also be concerned about innovation and deployment of non-emergency technology, and thus should seek to avoid imposing emergency-focused mandates that have the result of hindering the development of valuable *non*-emergency technology. The development of robust emergency communications in the IP context need not prevent new modes of communications from emerging. As one example (discussed more fully below), in NOI ¶ 52, the Commission poses the question of whether is should require that *every* Internet connected consumer device with "suitable" user interface be able to connect into the NG911 system. Yet a requirement of that type would very likely have the result of *discouraging* the creation of some new, innovative communications devices in the first place. Thus, as the Commission appropriately works to promote the move to NG911, it should also be sensitive to not chill the development of innovative technologies.

The Commission has correctly focused on consumer expectations as it assesses the move to NG911. Consumers today assume (sometimes incorrectly) that their legacy wireline or cellular telephone is "fully e911 capable." But as we move away from the legacy world with one

or two communications technologies to a world with thousands (or more) of services that allow users to communicate, it will be vital for consumers to understand that *some* of those new services will in fact be "fully NG911 capable," but that some services may *not* be as fully capable of connecting to the emergency system. The Commission should certainly act to make it easy for new IP-based technology to integrate into the NG911 system – by (for example) ensuring that the needed PSAP databases and other system resources are widely and affordably available to innovative new services. But the Commission should not go so far as to impose mandates on new technologies that they *must* connect into the system. It is vital that consumers be told and understand the differing capabilities of differing services and technologies.

Finally, as the Commission makes plain in its NOI, it already appreciates that there are serious potential privacy concerns raised by aspects of the emergency system. As discussed below, it is vital that the Commission be cautious to ensure that users maintain control over their private information, and that the NG911 system (and technology deployed to support the system) not be allowed to reduce user control over information about themselves or their location.

SPECIFIC COMMENTS

The following are comments and concerns in response to specific questions and discussions in the NOI, presented in the basic order in which they arise in the NOI.

Paragraphs 38 & 47 concerning transmission of medical information: Allowing emergency responders to receive electronic medical information (generally, as discussed in NOI ¶ 38, or in the disabilities context as discussed in ¶ 47) could be invaluable, and could enhance their ability to respond to an emergency. It is absolutely essential, however, that *any* transmission of medical information be at the full discretion of the person(s) involved. In some contexts, it may be appropriate for permission to transmit health information be given on a

blanket basis in advance of any emergency calls, but in most contexts it would be much better if the person placing the emergency were able to decide *at the time of the call* whether to transmit health information with the call.

A simple hypothetical can illustrate the concern. If an individual with a particular medical condition contacts the NG911 system about him- or herself, it may be helpful to have medical information transmitted. But if that same individual contacts NG911 to report a car accident that he or she witnessed, the personal medical information is absolutely irrelevant to the emergency. Indeed, if the user's choice is binary – to always transmit medical information or to never transmit it – it is quite likely that (a) some users would choose to "never" transmit information just to guard against privacy invasions, and (b) other users who do choose to "always" transmit sensitive medical information would hesitate to call for emergency help when they are a mere bystander. Both scenarios are sub-optimal, and could be avoiding by ensuring that users have maximum control over their own personal information.

Paragraphs 40, 49 & 54 concerning what formats PSAPs "should" accept in the NG911 system: A familiar adage in the Internet Protocol context is that networks and servers should "be liberal in what you accept, and conservative in what you send,"[2] which teaches in part that robustness and interoperability will be enhanced if systems are able to receive information in a range of formats, and even if the information is not precisely formatted. To promote innovation and to maximize the chance that new, innovative technologies will seek to interface with the NG911 system, it is desirable for PSAPs to adhere to the first part of this adage: "be liberal in what you accept." It will certainly be appropriate for the NG911 system to focus its efforts on the most common communications protocols. But at the same time, the system should

[2] Braden, R., ed., "Requirements for Internet Hosts -- Communication Layers," RFC 1122, October 1989.

also encourage PSAPs to be willing and able to receive emergency communications even if they arrive through less common protocols and without all of the precise assurances and information that the PSAPs might normally prefer.

Moreover, the NG911 system should not act as a significant barrier to new technology – if the NG911 technology will *only* interact with protocols or services A, B, and C, then innovative alternatives X, Y, or Z may have a harder time getting acceptance and market share. If on the other hand the NG911 system remains open to new communications services, then it will both keep pace with technology and will not serve to discourage new innovation.

Section IV.A.3 (¶¶ 41-43) concerning "SMS for Emergency Communications": The NOI raises a number of questions about the use of SMS in the NG911 context. As a threshold matter, we question whether great effort should be made to retrofit the legacy SMS system with new capabilities. SMS is not an IP-based technology, and it appears that more robust IP-based texting technologies may supplant SMS as consumers' preferred texting technology.

More generally, as suggested in ¶ 43, SMS could serve as a good jumping off point for consumer education about the limitations of communications technologies. Today, most consumers expect phones to be e911 capable, but they do not expect the same of SMS messages. Rather than seeking to make *all* "modern" technologies (including SMS) NG911 capable – a goal that is either unobtainable or obtainable only at the expense of chilling the development of new technologies – the Commission should focus its attention on consumer education to make sure that there is broad public understanding that some voice and text technologies are (or will be) fully NG911 capable, but that some voice and text technologies, like SMS, are not and will not be fully integrated into the NG911 system (even though in some cases they may still be usable as a fall-back method to reach emergency responders).

If the Commission seriously considers technical proposal to retrofit NG911 capabilities into SMS technology, it should carefully consider privacy concerns that might arise. Any proposal that location information be transmitted with an SMS message must ensure that location information is transmitted *only* in the emergency context or by the specific choice of the user. A requirement that SMS message *always* reveal location (even if only to service providers involved in the chain of transmission) could have some very serious privacy implications.

Paragraph 52 asking whether "every" capable consumer device should be required to be NG911 capable: The NOI asks whether "every consumer device with Internet or cellular connectivity and a suitable user interface have the ability to request emergency assistance?" Although broad ability to contact emergency services is of course a desirable goal, it should certainly not be mandated by the Commission (even if, as is doubtful, the Commission has the authority to do so).

Many of the Internet's most useful services began as experimental products often released to the public without charge and without guarantee. Some of those services – such as instant messaging – already include voice capabilities, and certainly more voice-capable services will emerge. On the hardware side, as more unlicensed spectrum is made available, we will likely see similar innovation in consumer devices. If the Commission imposes mandates on such new and emerging services and devices, it will likely stop them in their tracks, or certainly slow their development and raise their costs.

To take an example from the comic pages, it is certainly possible that we will see deployed some form of Dick Tracy's wrist communicator, yet such devices (because of size and battery constraints) may not be able to support location technology needed for full NG911 capabilities. Moreover, such devices may use new spectrum or mesh technology, and thus may

not ride on top of existing wireless networks with triangulating capabilities. It is certainly possible that such devices will not be fully NG911 capable. But surely such devices could be beneficial to users, and beneficial to public safety.

One does not need to look into the future to envision an example of a valuable device that could be threatened by an overly broad mandate to connect to the NG911 system. Today, many e-readers (such as the Kindle and its competitors) contain keyboards and rudimentary browsers that can use WiFi and/or 3G connections. Such devices, therefore, are "consumer device[s] with Internet or cellular connectivity and a suitable user interface," but their cost might go up significantly if (for example) they had to be locatable in an emergency context. In the future it might be the case that connected e-readers *without* NG911 capability could be affordable by every high school student in the country (thereby eliminating overly heavy book bags), but that adding NG911 capability might raise the cost and put the devices out of reach of many students. As valuable as the NG911 system will be, a mandate on every connected device could have serious societal consequences outside of the emergency context.

Paragraph 53 asking whether WiFi "hot-spot" providers should be required to participate in the NG911 system: This paragraph raises very similar issues to those discussed immediately above with regard to NOI ¶ 52. While the Commission can certainly encourage an open and innovative NG911 system that can facilitate broad compatibility with the emergency system, there could be serious societal consequences arising from a mandate that all hot-spot operators take certain actions (again, even if, as is doubtful, the Commission has the authority to do so). We broadly benefit from the availability of free or low-cost Internet connections available at libraries, coffee shops, municipalities, and others who provide Internet access, and

mandates could make such services too expensive to provide. The Commission should be very hesitant to impose mandate on the huge diversity of small providers of Internet access.

Section IV.D.4 (¶¶ 74-75) raising privacy concerns: As the Commission notes in NOI ¶ 61 and elsewhere, in many states 911 call records are subject to disclosure. As IP-based applications and services make more and more information (including medical information, video and still images, etc.) potentially available to PSAPs, serious privacy concerns are raised. These concerns may suggest that the disclosure laws may need to be revisited and possibly modified. This is a serious issue that may warrant a separate inquiry by the Commission (including to consider the Commission's possible authority to address the concern). As noted above with regard to ¶¶ 38 & 47, a failure to protect the privacy of those who reach out to the NG911 system may discourage some from "making the call" in the first place.

And, because location information is highly sensitive and there are strong temptations for commercial abuse of such information, to the extent the Commission requires or urges service providers to determine location information, it should also impose accompanying obligations on those providers to ensure that the location is not used outside of the emergency context without the express consent of the users.

Section IV.D.5 (¶ 76) concerning location capabilities: Although NOI ¶ 76 is not clear on this point, in the past[3] the Commission asked whether *all* devices capable of communicating with NG911 services (which would include all ordinary desktop and laptop computers) should be required to be "automatically" locatable. There are very serious privacy and innovation concerns raised by this proposal. These concerns were extensively addressed in the *Joint Comments of*

[3] *See In the Matters of IP-Enable Services and E911 Requirements for IP-Enabled Service Providers, First Report and Order and Notice of Proposed Rulemaking*, WC Dockets No. 04-36, 05-196 (released June 3, 2005), at ¶ 57 ("IP-Enabled E911 Proceeding").

Center for Democracy & Technology, Computer & Communications Industry Association, Electronic Frontier Foundation and Pulver.Com[4] filed in the prior proceeding, and we urge the Commission to review those comments.

CONCLUSION

We urge the Commission to promote a robust NG911 system, but at the same time to promote and protect innovation and privacy. We look forward to working with the Commission on these issues.

Respectfully submitted by,

/s/

John B. Morris, Jr.
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, DC 20006
(202) 637-9800

Dated: February 28, 2011

[4] *Joint Comments of Center for Democracy & Technology, Computer & Communications Industry Association, Electronic Frontier Foundation and Pulver.Com*, IP-Enabled E911 Proceeding (filed Aug. 15, 2005).