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

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

Reply Comments of the Electronic Frontier Foundation

Dated: March 12, 2011

The Electronic Frontier Foundation (EFF) respectfully submits these comments regarding the *Notice of Inquiry in the Matter of Framework for Next Generation 911 Deployment*, PS Docket No. 10-255, as released December 21, 2010. EFF is a nonprofit civil liberties law firm and advocacy organization representing the interests of consumers and innovators in the digital age. Our comments address legal, policy and technological concerns in the NG911 proposed framework.

SUMMARY AND DISCUSSION

The advent of advanced communication technologies beyond voice-centric devices offers an opportunity to update the legacy Emergency 911 system to improve responsiveness and accessibility of emergency services, but the Commission must ensure that the Next Generation 911 will not inadvertently jeopardize consumer privacy or stifled technological innovation. EFF appreciates the Commission's investigation into adopting a framework that will allow consumers to access these critical services through multiple means – including SMS, MMS and real-time text. However, the Commission must consider the privacy and technological ramifications of the proposed system. We have three primary concerns about the transition to next-generation 911 services:

- Consumer medical privacy will be jeopardized unless adequate safeguards are implemented;
- Location sharing and mandatory user authentication would imperil the privacy of online users and hamper online freedom of expression; and
- A technology mandate to implement the NG911 system on all suitable networked devices would chill innovation.

First, the Commission rightly noted the potential ramifications of the NG911 proposal for consumer medical privacy. The Commission requested comment on whether auxiliary data (such as medical history, building floor plans, etc.) should be provided to first responders via PSAPs. The Commission correctly noted that, in most places, 911 call records are subject to public disclosure. If PSAPs receive and transmit sensitive medical

history data, the Commission must establish robust privacy protections to prevent this medical information from becoming public. The Commission should safeguard the medical privacy of callers and should help ensure that sensitive medical history data is specifically exempted from public disclosure.

Second, EFF urges the Commission to respect the wishes of consumers in deciding whether to share locational information or authenticate their identities. Anonymity plays a unique and important role within our society; anonymous and pseudonymous speech has been important in political dialogue from the Federalist Papers to the recent protests in Tunisia and Egypt. Anonymous and pseudonymous speech is also a protective measure for communicating online without revealing one's identity – an important tool for survivors of domestic violence and stalking, individuals suffering from medical conditions such as HIV, political commentators, human rights workers, journalists, whistle-blowers, and even teenagers who seek to explore and question without permanently tying their identity to their expression. We fear that an attempt by the Commission to access and share location information or authenticate identities of online users will unintentionally create a framework that facilitates more routine tracking of individuals' locations and identities, which could jeopardize all types of online anonymous speech. This would creates an architecture of surveillance antithetical to freedom of expression. We strongly object to any attempt to systematically anchor online identities to the offline world and any attempt to mandate online location sharing with emergency services without a consumer's consent.

Third, the Commission should avoid extending mandates for incorporating NG911 into technologies beyond those currently covered under E911. Worldwide, there has been an explosion in consumer electronics that promote information sharing and communication. As technology evolves, it is likely that a wide range of devices will eventually connect to the Internet or with one another via mesh networks, including many devices that have not yet been designed. A technology mandate to incorporate NG911 services into all devices such as laptops, netbooks, handheld computers and tablet computers could increase the costs and complexity in designing new consumer-facing electronics, particularly if those standards are inflexible or complex. This in turn could chill future innovation. Rather than stifle innovation with inflexible and high standards, the Commission should allow technology designers to promote NG911 compliance as a feature and a benefit to their devices. This hands-off approach has been instrumental in creating today's robust technology marketplace, which itself has resulted in the invention of the new modes of communication that have made NG911 possible.

Communications technology has made us steadily safer and safer for over a century by making it ever cheaper and faster to tell people who can help about problems in a timely way. The 911 system is a great triumph that represents an important piece of this puzzle, but another piece is simply making communications cheaper, more reliable, and more ubiquitous. Even communications channels that cannot contact 911 services at all aid public safety by increasing the chance that someone who can help will find out about a problem promptly.

Hence, we should not assume that communications devices all need to be regulated in the same way, or need to have any particular feature or functionality, in order to benefit public safety. Human beings have always showed great ingenuity in using all available channels to summon help in an emergency. They will surely continue to do so, so the core priority should be ensuring that the means of communications are numerous, ubiquitous, and readily comprehensible. New devices do not need any one particular feature to be a net benefit to public safety.

The Commission should also note that new capabilities to locate networked devices will be used for law enforcement and foreign intelligence surveillance, even if such provisions are initially adopted for the purposes of improving emergency services. We saw this scenario unfold with the original E911 rules; to this day, we are contending with legally-controversial cellular telephone tracking by law enforcement.

We look forwarding to working with the Commission to ensure that the next generation of emergency response services will improve the availability and flexibility of emergency responders while protecting the privacy of individual callers and working to promote technological innovation.

SPECIFIC COMMENTS

Sections 52, 53, 55: Should every consumer device with Internet or cellular connectivity and a suitable user interface have the ability to request emergency assistance? Should all devices of a certain class be required to meet the certification criteria?

We support the proposed initiative to allow the public a wider variety of means for contacting emergency services. We also agree with commenters who observe that the more difficult problem is upgrading PSAPs, not end users' devices. End user devices are likely to have rapidly-evolving capabilities, but often PSAPs are not equipped to receive the communications that these devices are already capable of sending. Providing consumers with the ability to transmit several types of media will improve the availability of services, could offer responders important data about an emergency situation, and could improve services to the disabled who may face challenges in communicating with emergency services under the legacy system. However, we urge the Commission not to require new and emerging technologies to offer consumers the ability to request emergency services. Devices, and the software that runs on them, are extremely varied in capabilities, purpose, and user interface. A requirement that all such devices be capable of a particular function could ultimately hamper innovation in the realm of electronics and communication services generally.

Consumer-facing communication services are a market in flux. The availability of Wi-Fi, the development of netbooks, online chat, the network connectivity of consumer devices, and numerous other technologies are in a state of growth and change. Many of the communications technologies we have today were created through innovation and exploration. Regulation of such devices, even well-meaning regulation such as that proposed in NG911, could force emerging technologies to comply with technical and even legal requirements that will be costly and technically challenging. Rather than assist consumers in communicating with emergency services, mandatory requirements stifle innovation and could prevent revolutionary new consumer communication technologies from reaching the marketplace.

What's more, modern digital devices do not all use telephone numbers. Neither do they necessarily connect to the same services or use the same addressing systems, so there is no particular point of emergency contact that users currently expect to be able to reach (like 9-1-1 in the comparatively homogeneous PSTN), nor is there a consistent interface that users would currently expect to use to understand whether emergency services are currently available through a particular network. (Since some networks block or censor particular network protocols or destinations, either for everyone or for some classes of users, it could be quite difficult for a device to determine or reliably explain what kind of emergency capabilities it will have. For instance, users trying to contact emergency services from an airplane over an IP network might find that the ISP has entirely blocked protocols needed to establish a VoIP call.)

Rather than mandatory requirements, the Commission should allow technology creators to offer NG911 accessibility as a competitive advantage. This will improve the accessibility of 911 services, and creators will have an incentive to educate consumers about NG911 compatibility for its marketing advantage.

Section 58. Device-Initiated Services for Emergency Communications. We seek comment on how the deployment of NG911 will facilitate the ability of device-initiated emergency services to reach PSAPs.

Device-initiated emergency service calls must be carefully designed so as not to negate consumers' understanding and control over the circumstances in which emergency calls will be placed. Currently, consumers must proactively contact emergency services in order to request assistance. Alternatively, consumers can use one of the competing services that provide device-initiated emergency service calls – such as burglar alarms on a house or car safety devices, such as OnStar. The OnStar service, for example, will alert a dispatcher if an air bag is deployed in a vehicle, who will then contact emergency services if appropriate and guide emergency responders to GPS coordinates of the car. This service is already available to consumers.

For device-initiated calls to emergency services, it is vital that consumers opt-in to the service. Consumers must be provided with a choice as to how technologies they own collect data and transmit it to third parties, both in emergency and non-emergency situations. Consumers already have this choice with services like OnStar.

Furthermore, consumers should always have the right to deactivate a service. While many consumers will choose to install devices that provide device-initiated calls to emergency services, others may prefer not to have their homes or vehicles sending emergency signals without their consent. We urge the Commission to respect users' choice. For example, a homeowner who burns a cake in the oven may not want to have the fire department signaled after the fire alarm goes off. Such a situation would be not only embarrassing but a wasteful misuse of emergency resources.

59. Social Media for Emergency Communications. To what extent might State and local public safety jurisdictions employ social media tools as a way to interact with the public?

It is unlikely that social media will ever be a primary mechanism by which the public contacts emergency services, nor should people be encouraged to rely on social media for this purpose. At the same time, people will naturally use any available communication channel to get help, such as by asking a friend in an on-line chat to call 911 in an emergency. This is one reason that the increased public use of communications media of all sorts tends to improve public safety even without creating any new formal infrastructure.

However, clear privacy guidelines should be established if emergency services seek to obtain any data from public social media websites. During President Obama's inaugural

address, the Department of Homeland Security monitored a range of public social media sites for threat response purposes. EFF received documents in response to a Freedom of Information Act request describing DHS's use of a "Social Networking Monitoring Center" to collect and analyze online public communication during the inauguration. Notably, DHS considered the privacy implications of this practice and adopted Fair Information Practices Principles[1] to govern the collection, storage and deletion of data. In a state of emergency (such as following an earthquake or during a riot), emergency services may seek to obtain real-time data about breaking events via sites such as Twitter. If emergency responders seek access to such data, we urge them to adopt guidelines based on the Fair Information Practices Principles for how and when such data will be obtained, with an emphasis on minimizing data collection and retention. Emergency service providers should be prohibited from creating false profiles on social networking sites for data collection purposes and should never attempt to access non-public consumer information through social networking sites, as such activity would violate consumer privacy expectations.

Guidelines should be created and reviewed for privacy considerations prior to gathering data through social networking sites. Social media should never be used as a routine mechanism for collecting data.

61. Auxiliary Data. Since this auxiliary data may be considered part of the 911 call record and therefore subject to public disclosure, is there a need to protect the privacy of this data differently than the remainder of the call information?

The ability to transfer auxiliary data to responders, including medical history information, could be a critical component of NG911. However, the Commission rightly notes that there are numerous privacy concerns about this transmission of sensitive data. It is unlikely that PSAP dispatchers would be considered covered entities under federal medical privacy laws. Furthermore, 911 call records are in most places subject to public disclosure, leaving consumers vulnerable to having their personal medical data exposed if it is considered part of the call record.

We urge the Commission to protect the medical privacy of callers. Specifically, medical history data should *not* be considered part of the public call record. Furthermore, any medical data collected by PSAPs should be held to the standards of state and federal privacy laws. It is likely that legal standards will need to be revised to ensure that medical data transmitted via NG911 will adhere to the generally accepted privacy practices. This will ensure that consumers' privacy expectations are not violated by the data handling practices of PSAPs and responders.

Furthermore, we would recommend the Commission adopt standards for consumer notification in the event of a medical data breach.

---

1 See Department of Homeland Security's *Privacy Policy Guidance Memorandum*, December 29, 2008, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

In addition to these comments, we agree with the Center for Democracy and Technology that any transmission of medical data should be made at the discretion of the person(s) involved *at the time the call is made.* The Commission should consider best practices for the security of transmission, reception and storage of this data.

Ensuring full consent of the person(s) involved before transmitting medical data as well as adopting privacy principles to safeguard sensitive medical information can ensure that consumers will feel comfortable contacting and sharing medical information with PSAPs.

75. What privacy concerns will be introduced with the deployment of NG911? What existing or new regulations might be necessary to ensure appropriate privacy controls? How should we address concerns regarding private personal information that may be transmitted as part of an NG911 communication, for example, personal medical information that NG911 can provide to PSAPs and other third parties? How can 911 call takers at virtual PSAPs legally access 911 call data when necessary, while requiring adherence to appropriate confidentiality, disclosure, and retention statutes and rules?

As we noted above, NG911 raises specific privacy concerns. The Commission should consider several important consumer privacy issues:

- **Auxiliary medical data.** Auxiliary medical data transmitted to NG911 PSAPs should not be considered part of the call record available for public disclosure, as the possibility of having personal medical data exposed could prevent consumers from sharing vital information or contacting 911 at all. It is important that auxiliary medical data is only shared at the caller's initiation. It is likely that medical privacy statutes such as HIPAA will need to be amended to cover the transmission of data between users and PSAPs. We also recommend that NG911 adopt a robust data breach notification system.
- **Privacy by design.** While the networking capabilities of NG911 will make it a more responsive and effective emergency system, it is vital that privacy considerations are "baked in" to both the governing policy and technological design of the system. From a policy perspective, this means assigning roles to different responders with varying levels of data access, providing internal audits of security procedures, and educating dispatchers and responders on privacy issues. On a technological level, this means cabining data sets, adopting strong data security protocols and being responsive to the vulnerabilities inherent in any networked system.
- **Minimizing data retention.** While we recommend that NG911 embrace all of the principles outlined in the Fair Information Practices Principles, NG911 should above all endeavor to minimize data retention. By only collecting data that is necessary and discarding data as soon it is no longer necessary (and establishing protocols for ensuring this is done regularly and appropriately) the NG911 system can greatly reduce the potential security and privacy risks of moving into a networked world.

77. Will the deployment of NG911 allow increased security of information through role-based access control and data rights management that limits access to information only to authorized entities? What additional security concerns will be implicated by the transition to NG911 as compared to the legacy 911 security functionality? How can the NG911 network be protected against viruses, cyber attacks, fraudulent or harassing transmissions, and other unwarranted intrusions and interruptions?

Compared to the public telephone network, IP networks may be more vulnerable to denial-of-service attacks that could limit availability of emergency services. They are run by a greater variety of organizations and individuals using a greater variety of equipment, and they may make it cheaper for people to send false calls to the 911 service. Network operators might also have policies that effectively prevent certain kinds of emergency consideration, perhaps as inadvertent collateral damage from the enforcement of other network policies. But, on balance, the number of places where someone can obtain a reliable, usable connection to call for help is increasing steadily.

Some commenters have worried that false calls can be sent over the Internet, whether from within the United States or from another country. This could disrupt a PSAP's operations and prevent it from responding effectively to real emergencies. However, these risks certainly exist today. For instance, a malicious caller currently could abuse telephone relay services for the hearing-impaired, including IP relay services, to place a false emergency call, even in a physically distant area. What's more, PSAP and other emergency dispatch-related facilities also have ordinary 10-digit PSTN numbers, which are generally not secret.[2] For example, if a user wanted to call a PSAP in Idaho, she could look up the PSAP's 10-digit number and dial it from anywhere in the world (or using any VoIP service) and talk to the operator there.

Thus, emergency services are already subject to, and contending with, a range of potential disruptions and abuses. It's not clear whether more Internet connectivity will make these problems worse, but since the Internet and the PSTN are already extensively interconnected today, there will be few, if any, threats that are qualitatively entirely new. Although existing possibilities for disruption might be exacerbated by more widespread awareness of ways to contact emergency services, comparable possibilities usually already exist.

---

2 See, e.g., Minnesota Statewide 9-1-1 Program, “Minnesota 9-1-1 Public Safety Answering Points”, available at http://www.911.state.mn.us/PDF/911_MN_Public_Safety_Answering_Points.pdf (listing direct 10-digit PSTN number for each Minnesota PSAP); Oregon Emergency Management 9-1-1 Program, “PSAP Directory by County”, available at http://www.oregon.gov/OMD/OEM/OR911/docs/psap_directory.pdf (same for Oregon).

Section 76. What, if any, obligations need to be imposed on Internet service providers, residential and enterprise equipment vendors, and other parties to ensure that location information can be discovered, conveyed, and validated?

The Commission's request for location data stems from a need to appropriately deploy resources to the correct location in real emergency situations. While this is an important interest, we urge the Commission not to impose any obligation on Internet service providers, residential and enterprise equipment vendors or any other parties to ensure that location information can be discovered, conveyed or validated.

Real-time location data is extremely sensitive consumer data. A Commission mandate on Internet communication providers to create mechanisms to accurately collect and transmit this data without a user's explicit consent would make it that much easier for consumer location data to be collected and diverted for purposes that have nothing to do with emergency response – or even sold for profit. These systems could also become vulnerable to security exploits or data breaches. The result would be an environment in which consumer location privacy is generally unprotected. We are especially concerned about the many Internet users for whom indiscreet disclosure of location data could jeopardize their physical safety or their work— victims of stalking and domestic violence, judges, police officers, whistle-blowers, investigative journalists, and many others. We instead urge the Commission to act appropriately to encourage systems to provide location discovery as a user-controlled feature without ordering or encouraging service providers to collect and share this data without a user's consent.

Furthermore, ISPs do not necessarily know a user's physical location, as a user may be connecting through a proxy or virtual private network (VPN). Location detection schemes might wrongly inform the ISP that the user is at the proxy's location instead of her real location. It's extremely challenging to ensure that an ISP can distinguish these cases, though devices themselves might be able to distinguish them somewhat by examining their own proxy settings. But in some cases, software on a device doesn't know or can't examine the relevant proxy settings. Thus a mandate from the Commission for ISPs to provide user location data might not only raise serious privacy concerns – it could well be impossible.

While location data can be valuable in the emergency context, our electronic communications systems are most often used for non-emergency communications. Mandates for emergency services will likely bleed over onto the very structure of the Internet and the nature of the record-keeping that ISPs do. When online communications are tied to a specific offline identity and/or a specific location, it can squelch free expression and enable new modes of government surveillance. There is little question that new capabilities to locate networked devices will be used for law enforcement and foreign intelligence surveillance, just as the original E911 mandates have enabled legally-controversial cellular telephone tracking by law enforcement[3]; particularly when the legal

3 Compare, e.g., In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005) (denying law enforcement application to track cell phone without a probable cause search warrant) and In re Application of U.S. for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d

standards and authority for such surveillance are in serious question[4], a broad mandate that all network-connected devices must be locatable would likely have serious implications for Americans' civil liberties and locational privacy. Thankfully, there are efforts in Congress to create clear, strong protections against unwarranted government access to location data, and the Commission should act with great caution in this area unless and until those efforts are successful.[5]

If the Commission does act to encourage ISPs to develop or deploy location capabilities for emergency purposes, these capabilities should be designed and organized to allow the ISP to provide the location information *to the user's device*, not to any third party. Then the user's device can decide, in accordance with the user's wishes, how and when to use this information in the user's interest.

Please see the next Section 80 for additional comments on the importance of protecting online anonymity.

Section 80. We are concerned that unauthorized access to the NG911 network will increase the number of unintentional, prank, or malicious calls to a PSAP. We seek comment on whether such emergency-call-only credentials would be desirable and feasible? If so, how can they be implemented? 81. Even if new authorization procedures can be developed, it may still be necessary for NG911 systems to support emergency communications in some circumstances where the caller cannot be identified. We seek comment on how this problem can be addressed. When would it be appropriate for the NG911 system to support emergency calls without authentication and/or authorization?

These questions, in addition to section 76, deal with whether and how to stop online anonymous speech. The goals of an NG911 system are laudable – to provide consumers with better service, reduce prank calls, and accurately deploy emergency personnel to the correct location. We believe, however, that it is neither wise nor necessary to consider measures that might restrict consumers' First Amendment rights to speak, read and associate anonymously at this time.

The tradition of anonymous speech is older than the United States. Founders Alexander Hamilton, James Madison, and John Jay wrote the Federalist Papers under the pseudonym "Publius," and "the Federal Farmer" spoke up in rebuttal. The U.S. Supreme Court has repeatedly recognized rights to speak anonymously derived from the First Amendment. The right to anonymous speech is also protected well beyond the printed

---

435 (S.D.N.Y. 2005) (granting application).

4 See, e..g., In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 312-13 (3d Cir. 2010) (noting possible Fourth Amendment protection for cell phone location data).

5 See *Digital Due Process: Modernizing Surveillance Laws for the Internet Age* via http://digitaldueprocess.org. Also see *Wyden Calls for Clarity About Legal Procedures Regarding Electronic Devices* via http://www.mycentraloregon.com/news/local/1304380/Wyden-Calls-For-Clarity-About-Legal-Procedures-Regarding-Electronic-Devices.html.

page. Thus, in 2002, the Supreme Court struck down a law requiring proselytizers to register their true names with the Mayor's office before going door-to-door.[6]

These long-standing rights to anonymity and the protections it affords are critically important for the Internet. As the Supreme Court has recognized, the Internet offers a new and powerful democratic forum in which anyone can become a "pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox."[7]

Attempts to force the authentication of NG911 callers (including online “callers”) or mandate the sharing of location information will create an architecture well-suited to inhibit all forms of anonymous and pseudonymous speech. If users must authenticate themselves to contact 911, that same authentication may soon become mandated in other contexts that have traditionally not necessitated authentication, such as setting up an email or instant messaging account.

In our view, mandated authentication is a solution in search of a problem. The Commission’s concern “that unauthorized access to the NG911 network will increase the number of unintentional, prank, or malicious calls to a PSAP” is speculative. Rather than create a systematic structure that could wreak havoc on the ecology of online free expression, we urge the Commission to wait and collect evidence on whether such unintentional, prank or malicious calls *ever materialize as a serious problem.* It is quite possible that the increase in distraction calls during and after the adoption of NG911 services will be mild or nonexistent, or effectively mitigated by means other than authentication. We therefore urge the Commission to collect data on the magnitude of this issue before attempting sweeping changes to Internet architecture to correct what may not be a problem at all.

---

6 See *Watchtower Society v. Village of Stratton*, 536 U.S. 150 (2002).

7 See *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), in which the Court struck down anti-indecency provisions of the Communications Decency Act for violating freedom of speech provisions of the First Amendment.

CONCLUSION

We thank the Commission for the opportunity to submit comments on the NG911 system. While we support the transition to NG911 and the many improvements it will bring to consumers' ability to summon emergency assistance, we urge the Commission to safeguard consumer privacy and shun technological regulation that will hamper innovation in communication technologies. We look forward to assisting the Commission in designing a responsive emergency service that incorporates communications from new technologies while encouraging technological innovation and respecting consumer privacy.

Respectfully submitted by,

/s/

Lee Tien, Senior Staff Attorney
Seth Schoen, Senior Staff Technologist
Rainey Reitman, Activism Director
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Phone: +1 415 436 9333
Fax: +1 415 436 9993