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

In the Matter of	)	
	)	
Wireless E911 Location Accuracy Requirements	)	PS Docket No. 07-114
	)	
E911 Requirements for IP-Enabled Service Providers	)	WC Docket No. 05-196
	)	

JOINT COMMENTS OF

CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, and SUN MICROSYSTEMS, INC.

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

Lee Tien
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Dated: August 20, 2007

TABLE OF CONTENTS

I. THE WORLD IS EXPERIENCING A DRAMATIC SHIFT IN HOW PEOPLE COMMUNICATE, AND THE EMERGENCY RESPONSE SYSTEM SHOULD ADAPT TO AND EMBRACE THE NEW TECHNOLOGICAL PARADIGM RATHER THAN RESIST IT. 2

A. Internet-Based Communications Are Radically Different Than Communications Over the Public Switched Telephone Network. 2

B. Public Safety and Security Will be Enhanced by the Broad Availability of New Low Cost Communications Technologies – Even If They Are Not Able to Determine and Transmit Location Information.....5

II. IF THE COMMISSION IMPOSES "AUTOMATIC LOCATION" REQUIREMENTS ON INTERCONNECTED VOIP SERVICE, IT WOULD EFFECTIVELY PROHIBIT THE USE OF A BROAD SWATH OF TECHNOLOGY, AND WOULD SIGNIFICANTLY REDUCE THE COMMUNICATIONS CHOICES AVAILABLE TO AMERICANS. 6

III. THE COMMISSION SHOULD FOCUS ITS ATTENTION NOT ON TRYING TO FORCE NEW TECHNOLOGY TO ACT LIKE OLD TECHNOLOGY, BUT ON RAISING AWARENESS AMONG THE PUBLIC THAT DIFFERENT TECHNOLOGIES HAVE DIFFERENT CAPABILITIES. 8

IV. THERE IS SIGNIFICANT RISK THAT ANY COMMISSION ACTION TO FORCE LOCATION DETERMINATION TECHNOLOGY INTO VOIP AND OTHER IP-BASED TECHNOLOGIES WOULD SERIOUSLY HARM BOTH PRIVACY AND INNOVATION. 9

CONCLUSION 11

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

In the Matter of	)	
	)	
Wireless E911 Location Accuracy Requirements	)	PS Docket No. 07-114
	)	
E911 Requirements for IP-Enabled Service Providers	)	WC Docket No. 05-196
	)	

JOINT COMMENTS OF

CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, and SUN MICROSYSTEMS, INC.

The Center for Democracy & Technology, the Electronic Frontier Foundation, and Sun Microsystems, Inc., respectfully submit these comments on the Notice of Proposed Rulemaking ("NPRM") in PS Docket No. 07-114, CC Docket No. 94-102, and WC Docket No. 05-196, as released on June 1, 2007.

The undersigned strongly support the goals of the emergency 911 system – including the goal of transmitting "automatic location identification" ("ALI") information about someone seeking emergency assistance. But efforts to promote 911 and ALI are not the only ways to increase public safety and security, and more broadly are not the only goals that policymakers should pursue in assessing communications policy. Making 911 and ALI the paramount goal to be pursued will harm innovation and the development of new communications technologies, and by chilling new technologies will ultimately harm public safety. The Commission must avoid sacrificing the continued robust development of Internet and other communications technologies, and instead should look for ways to promote the deployment of 911/ALI without preventing new technologies from emerging.

Further, the Commission must exercise care to avoid causing serious harm to the privacy interests of Americans. A mandate by the Commission requiring or encouraging (even indirectly) the ongoing or routine tracking of users would create significant privacy risks, including both risks of commercial abuse of the location information, and governmental use (and possible abuse) of the information for surveillance purposes. The Commission should act to promote – and not reduce – users' control over their location information, and the goal of providing location information in the e911 context should not destroy privacy outside of that context.

I. THE WORLD IS EXPERIENCING A DRAMATIC SHIFT IN HOW PEOPLE COMMUNICATE, AND THE EMERGENCY RESPONSE SYSTEM SHOULD ADAPT TO AND EMBRACE THE NEW TECHNOLOGICAL PARADIGM RATHER THAN RESIST IT.

Just as the Internet is revolutionizing many aspects of our society, it is dramatically changing how we communicate, and what companies (if any) are involved in our communications. The emergency system needs to adapt to this new reality.

A. Internet-Based Communications Are Radically Different Than Communications Over the Public Switched Telephone Network.

When the use of a single short number to call for emergency assistance – 911 – was first proposed and then deployed in the late 1960s and 1970s, the communications marketplace was very different than it is today, and the emergency calling system was built upon assumptions that no longer hold true. The challenge for the emergency calling system in general – and the Commission in particular – is to adapt the emergency system to the new realities in communications, rather than to perpetuate no longer valid assumptions.

When the 911 system was created, there was in most places only a single telephone company – AT&T – and even after the break up of that company, there has been only one

predominant *local* telephone company in any given locality (whether it be one of the "former Bell companies," or an independent local provider). And thus, there was usually only one main company in any given area that needed to interact with the emergency response system. Thus, critically, there was only one company that needed to integrate with the system to deliver "automatic location identification" ("ALI") to public service answering points ("PSAPs"). Even with the advent of wireless carriers, there are still only a limited number of carriers in the PSTN that must provide ALI to PSAPs, and for the most part all of those carriers own or at least directly manage their own networks.

Real-time (or near-real-time) person-to-person communications over the Internet take place in a radically different environment than in the PSTN, with at least three key differences:

- there is no real limit on the number of companies that can provide real time communications services, and providers no longer have to be large or locally-based companies;
- companies can and do provide real time person-to-person communications capabilities without any need to own the network on which the communications travel, and without any technical or business reason to enter into contractual agreements with network owners; and
- users can engage in real time person-to-person communications without any company involvement at all (beyond basic access to the Internet).

Moreover, there is a dramatic diversity of additional vital information that in the Internet context could be conveyed to a PSAP – including among others visual images of the emergency site, historic or real-time medical data, and additional contact information relevant to the emergency (including additional information that can help emergency responders locate someone in need of help).

The emergency system faces a choice – will it be ready to receive emergency communications from the full diversity of available communications tools on the Internet (even

if the emergency communications do not arrive with an automatic or certified location), or will it refuse to receive communications that fall outside of the traditional PSTN model of emergency calls? Outside of the Internet context, the emergency system already receives communications without automatic location delivery – from satellite phones, for example – but it is unclear whether the emergency system will be willing to open up to the full range of Internet communications.

The Commission faces a related choice – will it facilitate (or at least not hinder) the creation of wholly new ways to communicate (including to communicate in emergency situations), even if those communications cannot carry "automatic location" information, or will it discourage (intentionally or not) the development of communications capabilities that do not meet an idealized conception of PSTN emergency calls (with fully "automatic" location generation and transmission)?

New and emerging communications services available on the Internet are a case in point: they are very different than any PSTN-based communication, they can be offered by providers that are wholly unconnected to users' access networks, and they can be deployed at a low cost. One can easily imagine circumstances in which such services would be the most readily available technology to use to request emergency assistance, such as the case of a teenager with computer access but no phone in her room at home, and who hears an intruder break in to the house downstairs. The emergency services community should want to be able to receive an emergency message from the teenager – even if the teen must provide her location by voice or text input.

Policy makers – both the Commission and Members of Congress – should acknowledge that new IP-based communications tools (including tools we have yet to invent) will not look or

act like traditional phone calls on the PSTN, and may not have the same characteristics or capabilities as traditional phone calls. In particular, not all new technologies will be able to interact with the emergency system in the same way as phone calls. In some cases, the changes will improve the ability of citizens to reach response authorities, but in other situations the changes may be not be helpful (such as not being able to create or transmit "automatic" location information over all technologies). Both the emergency systems and the using public itself must understand and adapt to the different capabilities offered by new communications technologies.

B. Public Safety and Security Will be Enhanced by the Broad Availability of New Low Cost Communications Technologies – Even If They Are Not Able to Determine and Transmit Location Information.

Although the availability of location information for many (but far from all) emergency calls on the PSTN has certainly assisted emergency response agencies and increased public safety, the lack of location capability in a communications technology does not mean that the technology *harms* public safety and security. Any technology that increases the availability and affordability of real-time person-to-person communications will *increase* the ability of the public to report emergencies or suspicious activities, and in the vast majority of the cases such reporting can be completely effective without *any* "automatic" location determination or transmission.

Again, it is easy to hypothesize a new communications technology that could be low-cost and could become almost ubiquitous – a very small, very low cost device that can transmit and receive text (similar to IM or SMS), without being a part of a cellular phone, and for a very low monthly service fee. Although cell phones are increasingly widely deployed, such a low-cost device might be even more widely deployed (especially by parents for their children). Such a ubiquitous communications capability would enhance public safety *even* if it lacked the ability to be located in any sort of automatic way.

Our society has already made this exact type of calculation with regard to, for example, some university dormitory settings. Many such facilities (as well as companies, schools, etc.) use "multi-line telephone systems" ("MLTS") that are able to provide (for example) telephone service in each dorm room. But as the Commission is aware, many of these systems *cannot provide detailed location information*. Nevertheless, the availability of those phones certainly increases the ability of students and others to contact emergency service centers (as well has providing a broad range of non-safety-related societal benefits). The lack of location capability has not kept our society from deploying MLTS systems.

Although location information is without question a desirable objective in the emergency system, it is not, and should not be, an absolute requirement for communications tools to be deployed and used. As detailed more fully below, in the Internet context, location information will often not be available, and the Commission should be cautious to avoid harming the development of such technology – even if it lacks location information.

II. IF THE COMMISSION IMPOSES "AUTOMATIC LOCATION" REQUIREMENTS ON INTERCONNECTED VOIP SERVICE, IT WOULD EFFECTIVELY PROHIBIT THE USE OF A BROAD SWATH OF TECHNOLOGY, AND WOULD SIGNIFICANTLY REDUCE THE COMMUNICATIONS CHOICES AVAILABLE TO AMERICANS.

In Paragraph 18 of its NPRM, the Commission indicates that it has tentatively decided to impose an automatic location requirement on "interconnected VoIP" services. Such an action would be a serious mistake, one that would have harmful consequences in terms of both market competition and technological development. The Commission should step back from its tentative decision.

Many VoIP services offer the ability to use a "softphone" – a piece of computer software used on ordinary personal computers, enabling users to make and receive voice communications

without any dedicated or extra hardware whatsoever. An ALI requirement would effectively prohibit such software (and with it, some VoIP services that *only* use softphones). This would be significantly harm competition in the VoIP and voice marketplaces, and would ultimately *reduce* the ability of VoIP users to contact emergency providers at all (because some service providers would be confined to permitting only VoIP-to-VoIP calls, without reaching the PSTN. It would not be rational for the Commission – in the name of *promoting* public safety – to *reduce* VoIP users' ability to contact emergency service providers.

Beyond softphones, even many VoIP services that use a hardware device to connect to the Internet would be unable to provide ALI, because there is no reliable and ubiquitous way for a computer device to determine its only location (especially since most VoIP usage takes place indoors, where GPS technology is ineffective). By imposing an ALI requirement, the Commission would erect obstacles that may well be insurmountable for many non-network-based VoIP providers, who would have little choice but to withdraw from the market. This would significantly reduce the competitive choices available to Americans, and would chill the technical and market development of additional competitive services.

Not only would an ALI requirement be harmful to competition and innovation, it would also be grossly unfair, in light of the fact that many other types of voice communications do *not* have comparable obligations. For example, satellite telephone service is permitted by the Commission even though it cannot provide ALI service. Similarly, MLTS service discussed above lacks ALI requirements. Moreover, even some CMRS/cell providers do not provide ALI service. Unless the Commission is to adopt a rule that would prohibit those services as well (something which we do not propose or support), it would be arbitrary and capricious for the Commission to effectively prohibit a broad range of VoIP services. This is especially true in

light of the fact that the vast majority of interconnected VoIP service customers do in fact receive e911 service with appropriate location transmittal – but such location information is not "automatically" determined and thus would not meet the Commission's tentative requirement.

The Commission must reject its tentative decision to impose an ALI requirement on VoIP providers. At most, the Commission could create a multi-stakeholder task force (including privacy and public interest advocates) to investigate the technical and other options to facilitate location reporting for emergency calls in the VoIP context.

III. THE COMMISSION SHOULD FOCUS ITS ATTENTION NOT ON TRYING TO FORCE NEW TECHNOLOGY TO ACT LIKE OLD TECHNOLOGY, BUT ON RAISING AWARENESS AMONG THE PUBLIC THAT DIFFERENT TECHNOLOGIES HAVE DIFFERENT CAPABILITIES.

User expectations are vitally important in the area of emergency communications and new technologies. Although most Americans may assume that calls to 911 sent over the PSTN carry location information, communications users must understand that different technologies have different capabilities, and that – for example – the most effective way for location to be sent in many VoIP services is for the user to register the location with the VoIP provider. Rather than taking steps to prevent Americans from using new services that cannot mimic every aspect of the PSTN, the Commission should instead seek to educate users about the differences in the technologies.

And, any educational efforts or requirements should be imposed on an even-handed basis, so that (for example) users of satellite telephone service, MLTS services, and non-ALI-capable CMRS/cellular services should be alerted to the limitations of those services in the same manner that VoIP providers convey limitations to their users. It is arbitrary to impose notice requirements on VoIP providers when those same requirements do not apply to all other service providers that can reach the PSTN.

If Americans are only allowed to use technology that acts "just like the old telephone system," they will be deprived of a broad range of options and benefits that new technology can provide. Instead of pursuing such an approach, the Commission should work to expand users' understanding of the benefits and limitations of the different communications technologies available to them.

IV. THERE IS SIGNIFICANT RISK THAT ANY COMMISSION ACTION TO FORCE LOCATION DETERMINATION TECHNOLOGY INTO VOIP AND OTHER IP-BASED TECHNOLOGIES WOULD SERIOUSLY HARM BOTH PRIVACY AND INNOVATION.

In both the instant and previous NPRMs[1], the Commission has raised the question of whether it should mandate any particular technologies to perform location determination. Whether such a mandate would be desirable in the context of CMRS/cellular service is beyond the scope of these comments, but in the VoIP/IP-based contexts, such a mandate would create serious threats to both privacy and technical innovation.

Those risks have been discussed in two previous submissions to the Commission, and those submission are incorporated herein:

- Joint Comments of Center for Democracy & Technology, Computer & Communications Industry Association, Electronic Frontier Foundation and pulver.com, submitted on August 15, 2005, in WC Docket No. 05-196 (available at http://www.cdt.org/digi_tele/20050816CDTe911.pdf); and

- Ex Parte Letter and Attachment submitted by the Center for Democracy & Technology on May 17, 2007, in WC Docket 05-196. A copy of this submission is attached hereto.

Both documents raise significant concerns about the risk to privacy of a mandate to include location determination technology in IP-enabled devices, and those concerns are equally

[1] *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), *published* 70 Fed. Reg. 37,307 (June 29, 2005).

applicable if the Commission were to impose a strict requirement that cannot be met using current location technology (and thus might effectively require the use of some of the more privacy-invasive approaches being touted by various vendor).

Briefly, the critical issues raised in those two documents include:

- The Commission should not impose any sort of location mandate that would require networks to proactively track users of VoIP and other IP-based voice services. Instead, the Commission should encourage solutions that, for example, only determine a user's location at the time of an e911 call.
- More generally, the Commission should avoid imposing any requirement that would serve to deprive users of control over their own location information. As a specific example, users who have communications devices (such as cell phones) that contain GPS technology should be able to turn off the GPS capability except during an actual emergency.
- The Commission must not exceed its statutory authority, which does not authorize the Commission to impose a design mandate on general purpose computing devices, even if they are capable of voice communications to the PSTN (as indeed most computers are). Such action would exceed the Commission's authority and would in any event be bad policy.

CONCLUSION

For the foregoing reasons, the Commission should step back from imposing location obligations on interconnected VoIP services, and should at most assemble a multi-stakeholder task force to study the options and challenges raised by emergency calling in the Internet context.

ON BEHALF OF

CENTER FOR DEMOCRACY & TECHNOLOGY (www.cdt.org)
ELECTRONIC FRONTIER FOUNDATION (www.eff.org)
SUN MICROSYSTEMS, INC. (www.sun.com)

Respectfully submitted by,

/s/

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

Lee Tien
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Dated: August 20, 2007

CENTER FOR DEMOCRACY & TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

May 17, 2007

By Overnight Delivery and Electronic Submission

The Honorable Kevin J. Martin, Chairman
The Honorable Michael J. Copps, Commissioner
The Honorable Jonathan S. Adelstein, Commissioner
The Honorable Deborah Taylor Tate, Commissioner
The Honorable Robert M. McDowell, Commissioner
Federal Communications Commission
445 12th Street, S.W.
Washington DC 20554

Re: **EX PARTE** Letter and Attachment Concerning "Auto-location" in the VoIP and IP-Enabled Emergency Contexts – WC Docket No. 05-196

Dear Commissioners:

The Center for Democracy & Technology (CDT) respectfully submits this *ex parte* letter to urge the Commission not to issue any mandates concerning E911 location technology in the VoIP and IP-enabled contexts without first soliciting comment and input on the harm to privacy, security, and innovation that could flow from an ill-considered mandate on location.

We understand that the Commission may soon take further steps in the above proceeding concerning emergency services in the VoIP context. As we detail in the attached report, "Balancing the Location Needs of E911 with Privacy and Innovation," we believe that the current record is wholly inadequate for the Commission to take further action at this time to require that VoIP-capable or IP-enabled devices have any certain type of location determination technology. Although the Commission's 2005 NPRM invited comment on privacy, only two sets of comments (including CDT's) addressed the topic, and in any event the 2005 NPRM did not seek comment on any detailed possible rules.

In particular, rather than issuing any rules at this time, we urge the Commission to articulate in detail in an NPRM or FNPRM any technologies or requirements that it is actively considering and to solicit comment on the innovation, privacy, and security implications of such technologies or requirements and of location mandates in regards to VoIP and IP-enabled devices in general.

There are very significant potential harms to both innovation and privacy that could flow from any mandate concerning location technology in the VoIP and IP-enabled contexts. We strongly urge the Commission to invite comments focused on those harms and risks.

We hope to have a further opportunity to discuss these issues with you. We appreciate your attention to our concerns in general and the attached report in particular.

Respectfully submitted,

/s/

John B. Morris, Jr.

cc: Ms. Marlene H. Dortch (by electronic submission)
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

CENTER FOR DEMOCRACY & TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Balancing the Location Needs of E911 with Privacy and Innovation

The Location Information Needs of E911 Emergency Communications in the VoIP and IP-Enabled Contexts Can Be Addressed Without Damaging Innovation or Creating an Orwellian Surveillance Society

May 2007

EXECUTIVE SUMMARY

It is vital that our 911 emergency response system move into the 21st Century and be able to receive emergency calls from Voice-over-IP (VoIP) and other "IP-enabled" technologies that are flourishing on the Internet (which utilizes the "Internet Protocol," or "IP"). It is also important that VoIP services that directly compete with cell phones and ordinary home telephones should be able to deliver "enhanced 911" communications in which the location of the caller is delivered to the emergency response centers (or PSAPs, "public service answering points").

This transition, however, raises some critical questions about (1) which VoIP and "IP-enabled" services or devices should be required to provide location information to PSAPs, and (2) what are the characteristics of the location information that is provided.

The answers to these questions could pose very serious threats to (a) the ability of citizens to protect the privacy and security of their location information, and (b) the ability of industry and academia to continue the extraordinary level of innovation that has marked the last 15 years of Internet growth. On the privacy front, some location determination technology would create an on-going regime of surveillance that would radically reduce privacy. On the innovation front, requirements that *all* IP-enabled devices be "automatically" locatable would certainly hamstring the ability of technologists to innovate and develop new modes of communication.

These questions have been discussed in recent years in a variety of technical and policy forums, and both Congress and the Federal Communications Commission (FCC) are considering taking action on these questions.

Unfortunately, neither Congress nor the FCC has paid sufficient attention to these risks to innovation, privacy, and security. In Congress, the Senate Commerce Committee recently passed S. 428, the "IP-Enabled Voice Communications and Public Safety Act of 2007." In

addition to addressing immediate regulatory obstacles to E911 services for VoIP calls, the bill also directs the National Telecommunications and Information Administration (NTIA) of the Commerce Department to develop a "national plan" for this transition. The bill does not, however, adequately address the privacy and innovation issues. We urge Congress to add an additional provision to the NTIA mandate, following Paragraph H in Section 5 of S. 428:

> (I) analyze (a) whether and how users of IP-enabled devices will be able to protect the privacy and security of their location in non-911 contexts, and (b) the impact of the E911 transition on future innovation in the IP-enabled context.

The Federal Communications Commission is looking at similar issues in its proceeding on *IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers*. The Commission should wait for the results of the comprehensive NTIA study that the Senate Commerce Committee amendment would require. In any event, the FCC should not take any further action without a more robust and current opportunity for the public to respond to the privacy and innovation implications of any rules or location determination technologies it may be considering. The record in the on-going FCC proceeding is wholly inadequate to assess these vital issues. Before any final rules concerning location determination in the VoIP or IP-enabled contexts are adopted, the FCC should issue a Notice of Inquiry or a Further Notice of Proposed Rulemaking setting out in detail what location technologies and requirements the Commission is considering adopting, and inviting comment on the privacy, security, and innovation implications of those proposals.

Ensuring a robust and effective E911 system in the Internet age is vital. But that goal can and should be achieved without destroying privacy or harming the ability to innovate. It is critical that these important issues be fully considered before any final rules are enacted.

DISCUSSION

Both Congress and the Federal Communications Commission are currently considering actions to promote the transition of the 20th Century emergency communications system to the Internet age. This transition is vital to maintain a robust emergency response capability, and a broad range of companies and technical standards organizations is working to ensure that the transition goes smoothly.

The advent of the Internet and the diversity of ways to communicate over the Internet promises to radically and positively transform our E911/emergency response capability. If properly implemented, Internet communications will dramatically increase the amount and relevance of information available to a "public service answering point" (PSAP) in an emergency. Digital and IP-enables services will allow a 911 caller to immediately transmit a picture of a car accident to the emergency services dispatchers. Someone with a heart condition can have his or her pacemaker communicate through a cell phone in the event of a heart attack. The value and potential of these new communications are enormous, and without question VoIP

and other Internet based communications must be able to communicate with the E911/emergency system.

The integration of VoIP and IP-enabled services into the E911 system, however, should not – and need not – come at the price of harm to privacy or security or hindrances on innovation. At the same time that Congress and the FCC take steps to open the emergency system to VoIP and other new technologies, they must be very cautious to not harm the also-important policy goals of privacy and innovation. As detailed below, decisions about integrating IP-enabled services with the E911 system can – if not carefully made – create serious risks to both privacy, security and innovation. Some location determination technology could easily be converted to create a surveillance society, and some location technology requirements being considered could seriously inhibit the future development of new communications technology.

Two specific questions raise the greatest policy concerns for both privacy and innovation:

1. What devices should be subject to a government mandate to work with the 911 system?

2. What should those devices be required to do?

As described below, both Congress and the FCC have taken steps toward answering these questions, with Congress to date taking a more cautious and tentative approach, and the FCC appearing to be considering a more aggressive – and thus riskier – approach.

The possibility of a "Big Brother" location tracking system arises in the broader context in which technology has overtaken the constitutional and statutory protections for information about individuals' whereabouts. Current legal standards for access to location information are inadequate to safeguard privacy rights.

Congress and the FCC should tread carefully in this area, and should not rush to adopt any broad requirements or mandates without first explicitly receiving input on the privacy, security and innovation issues raised by possible E911 mandates.

Background on Congressional Consideration of these Questions

In April 2007, the Senate Commerce Committee considered and passed S. 428, the "IP-Enabled Voice Communications and Public Safety Act of 2007." In additional to addressing some immediate regulatory obstacles to E911 services for VoIP calls, the bill also directs the National Telecommunications and Information Administration (NTIA) of the Commerce Department to develop a "national plan" for a transition to a robust emergency calling system. At markup, the Committee put aside an earlier draft that would have required *all* IP-enabled devices to be locatable "automatically." However, when the Committee adopted the provision calling for an NTIA study, it did not require NTIA to analyze the privacy, security or innovation impact of any proposed E911 rules for VoIP services. Such a requirement should be part of the task assigned to the NTIA by the legislation.

Background on the FCC's Proceeding Proposing an Auto-Location Mandate:

In June 2005, the FCC ordered certain VoIP carriers to provide E911 emergency service. At the same time, it issued a "Notice of Proposed Rulemaking" in which it stated that it "intend[s] in a future order to adopt an advanced E911 solution for interconnected VoIP that must include a method for determining a user's location without assistance from the user as well as firm implementation deadlines for that solution."[2] Specifically, the FCC indicated that it was inclined to:

> require *all* terminal adapters or other equipment used in the provision of interconnected VoIP service sold as of June 1, 2006 to be capable of providing location information automatically, whether embedded in other equipment or sold to customers as a separate device[3]

The Commission made clear that its "auto-location" mandate would likely cover even ordinary desktop and laptop computers (which can easily provide VoIP voice communications without any additional equipment).[4]

In August 2005, the Center for Democracy & Technology, the Electronic Frontier Foundation, the Computer & Communications Industry Association, and Pulver.com filed joint comments opposing this proposal, raising concerns about both privacy and harm to innovation. See http://www.cdt.org/digi_tele/20050816CDTe911.pdf. We are aware of only one other set of comments that addressed privacy.

There has been some concern that the FCC would move forward with an "auto-location" mandate. Moreover, there has been concern that the Commission would put its stamp of approval on a "radio-frequency-based" (RF) technology for location determination that will seriously harm privacy and innovation instead of selecting a far more privacy friendly handset- or network-based location determination technologies.

Under the more privacy-friendly approaches, a user's VoIP device discloses its location only *at the time it makes a 911 call* and there is no need or requirement for any network or service provider to track on a continuing basis the location of any users. The user remains in control of location information – which the user's device obtains from whatever network it is using to connect to the Internet or from GPS technology – and can (in a non-emergency context) send his or her location only when the user chooses. The Internet Engineering Task Force (IETF)

---

[2] *In the Matters of IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers, First Report and Order and Notice of Proposed Rulemaking*, ¶ 2, at 2, WC Dockets No. 04-36, 05-196 (released June 3, 2005), *published* 70 Fed. Reg. 37,307 (June 29, 2005) ("*First Order and NPRM")*.

[3] *First Order and NPRM* ¶ 57, at 34 (emphasis added).

[4] In footnote 77 of the same document, the Commission specifically refers to "a personal computer with a microphone and speakers, and software to perform conversion (softphone)" as included in the range of equipment that can support VoIP services. *First Order and NPRM* ¶ 24 n.77, at 14 n.77.

(with active CDT participation in the "geopriv" working group) has been working on this privacy-friendly approach for the past 5 years.

In stark contrast, the RF-based approaches to location determination require that a service provider track the location of *all* users *all of the time*. By constantly tracking users, the service provider is able to inform the emergency service agency (a "PSAP," or "Public Safety Answering Point") of a given user's location if the user calls 911. RF-based approaches are being pushed at the FCC by a few service providers that are seeking to market the technology for location-based advertisement and other commercial purposes.

Any specific technology mandate from the FCC would raises serious concerns about privacy, security and innovation. The RF-based approach is particularly troublesome.

Threats to Privacy

Fundamentally, there are three basic approaches to the control and transmission of location information: (1) the user (or the user's phone or other device) controls who can know the user's location (except in 911 situations, when disclosure would be automatic); (2) a network or service provider externally determines a user's location on an ad hoc and as needed basis, and is able to transmit it (with or without the user's permission) to a third party; or (3) a system of on-going tracking is established so as to be able to transmit the user's location in the event of a 911 call. At least some of the approaches being considered by the FCC would inhibit the ability of users to control their location information (as in approach 1), and instead would give private service providers information about customers' location (as in approaches 2 and 3). Both approaches 2 and 3 take the information away from the user (where it can be most directly protected) and give it to a third party service provider that may or may not have any direct contractual relationship with the user. It appears that the FCC has seriously considered RF-based technology that might take approach 3, requiring the on going tracking of users.

A mandate or strong endorsement by the FCC to implement an approach that requires the network or other third party to provide location information in an E911 context could directly undermine years of technology development focused on the transmittal of, and protection of, location information. Since 2001, the "GeoPriv" working group of the Internet Engineering Task Force ("IETF") has been developing technology to bind a user's location information with user-created location privacy rules.[5] A key focus of this working group has been to enable a user to directly control the transmittal of his or her location information, rather than having to rely on (and trust) whatever transient access network the user might be utilizing at the time, while also ensuring that location information is delivered to the 911 PSAP in an emergency context. By maximizing user control, the technology can minimize the abuse of location information (by, for example, access networks that seek to profit by selling users' location information without their consent, for unsolicited advertising and other purposes).

[5] *See* GeoPriv Charter, http://www.ietf.org/html.charters/geopriv-charter.html. The Center for Democracy and Technology has been an active participant in the GeoPriv working group since its inception, and has co-authored a number of the technical documents produced by the group. *See, e.g,,* RFC 3693, "Geopriv Requirements," *available at* http://www.ietf.org/rfc/rfc3693.txt; RFC 3694, "Threat Analysis of the Geopriv Protocol," *available at* http://www.ietf.org/rfc/rfc3694.txt.

A mandate by the FCC requiring or encouraging an RF-based system of on-going tracking of users would create even more privacy risks, including risks of commercial abuse of the location information, and governmental use (and possible abuse) of the information for surveillance purposes.

The FCC should not endorse or otherwise promote any of these approaches without a full and open discussion and debate about the serious privacy implications raised by the approaches.[6]

Threats to Innovation

The FCC's proposed adoption of an auto-location mandate would also pose a severe threat to innovation, in two ways. First, if the FCC selects one type of location-determining technology (such as a RF-based system) or sets requirements that only one technology can meet, the mandate would chill the development of competing technologies and could entrench a particular technology (and the service providers that offer that technology) to the exclusion of new services and technologies yet imagined.

More fundamentally, the proposition that *all* VoIP-capable devices (or even worse, all "IP-enabled" devices) *must* be able to be automatically located will chill the development and deployment of new types of communications services. Many of the Internet's most useful services – including VoIP – 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. Yet none of those services are likely to have the look and feel of traditional telephone system, even if they have a way of ultimately connecting to traditional telephones. If the Commission imposes E911 mandates on such new and emerging services, it will likely stop them in their tracks (at least, stop their development and use in this country).

To take an example no longer confined to the comic pages, it is certainly possible that we will soon see widely deployed some form of Dick Tracy's wrist communicator, yet such devices because of size and battery constraints may not be able to support GPS or other locating technology. Moreover, such devices may end up utilizing as yet unallocated spectrum, and therefore may not ride on top of existing wireless networks with triangulating capabilities. And such devices may move seamlessly from one type of network to another. And it is certainly possible that such devices will not have the ability to be "automatically" located. But surely such devices could be beneficial to users, and beneficial to public safety. If the Commission, however, mandates that *all* IP-based voice services be fully E911 compatible, then this type of new technology may never be introduced or get off the ground in the first place.

---

[6] Related to but distinct from concerns about harm to privacy are concerns that an ill-considered FCC mandate could harm the ability of users to protect their location information from security attacks. Any requirement that *every* IP-enabled device be locatable, or that an always-on location tracking system be implemented, will certainly harm the ability of a battered wife to prevent a batterer from discovering location, or a corporate executive to prevent a competitor from discerning valuable information from the executive's location. As with privacy, the FCC should not promulgate any rules for VoIP or IP-enabled devices or services without a full opportunity to assess the security concerns.

The Broader Context

These questions and developments are occurring in the context of a much broader debate about the weak privacy protections afforded location information under current law. By turning portable computer devices and cell phones into tracking devices, a FCC auto-location mandate would allow government tracking by remote computer of individuals' precise locations over prolonged periods of time and would create a treasure trove of information available to commercial entities for targeted advertising, or subject to subpoena in civil litigations (such as, for example, a divorce case). Current legal standards for access to location information are inadequate to safeguard privacy rights against indiscriminate surveillance of individuals' movements and activities.

While location information can be valuable for legitimate law enforcement and intelligence purposes and can be used to provide useful commercial services to individuals who wish to receive them, location tracking reveals sensitive information that deserves legal protection from unwarranted and unwanted disclosure. Location information can reveal a person's acquaintances and physical destinations such as medical clinics, government services buildings, and commercial establishments. Such data may imply – correctly or incorrectly – additional information about the individual, including preferences and associations. Informational privacy about one's movements in society implicates the constitutional right to travel and the freedom to associate. Without assurance that one's movements are not arbitrarily being watched and recorded by the government and other third parties, full exercise of these liberties will be chilled.

Current law does not set explicit standards for government location tracking. Although there is a federal statute governing tracking devices (18 USC § 3117), the statute does not provide a particular standard for approving governmental use of a tracking device. Congress did make clear that the standard for government acquisition of location information is higher than the standard for non-content, transactional information under the pen/trap law (a certification by the government that the information likely to be obtained is relevant to an ongoing investigation), but it stopped short of stating precisely what that standard is.

In CDT's view, given the power of location technology to locate people in non-public places, the government acquisition of location information should be allowed only pursuant to a search warrant issued on a finding of probable cause to believe that a crime has been, is being, or is about to be committed and that the surveillance will result in information pertinent to its investigation. The lack of sufficient standards for governmental access to, and use of, location information, coupled with the amount of location information that the FCC mandate would make available, gives government agents too much discretion and creates a qualitatively new threat to personal privacy.

The law is equally unclear in the commercial context. Although Congress has prohibited telecommunications carriers from disclosing wireless location information for commercial purposes except with the prior express approval of the customer, this limitation applies only to "telecommunications carriers" and not to other entities that collect or use location information from VoIP devices in the course of providing location-based services.

Specific Policy Recommendations

S. 428, the "IP-Enabled Voice Communications and Public Safety Act of 2007," should be amended before passage to direct – as part of its "national plan" – the National Telecommunications and Information Administration (NTIA) to specifically consider and analyze the impact of any proposed E911 mandates on innovation, privacy and security. We urge Congress to add an additional provision to the NTIA mandate, following Paragraph H in Section 5 of S. 428, requiring the agency to:

> (I) analyze (a) whether and how users of IP-enabled devices will be able to protect the privacy and security of their location in non-911 contexts, and (b) the impact of the E911 transition on future innovation in the IP-enabled context.

The Federal Communications Commission is looking at similar issues in its proceeding on *IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers*. The Commission should await the outcome of Congressional action on S. 428 and the results of any NTIA study, but in any event it should not take any further action without a more robust and current opportunity for the public to respond to the privacy and innovation implications of any rules or location determination technologies that the FCC is considering.

The record in the on-going FCC proceeding is wholly inadequate to assess these vital issues. Over the past two years, the FCC has received numerous ex parte briefings and sales pitches on a wide variety of technologies that might be used to track location. The public has received no indication of which of those technologies the FCC is seriously considering, and thus the public has not had a sufficient opportunity to assess and comment on any of those proposals. The FCC's Notice of Proposed Rulemaking in mid-2005 was wholly lacking in details about what the Commission would adopt. Based on the current record, the public has simply not had an adequate chance to raise the serious risks to privacy and innovation that are discussed here.

The FCC should not issue final rules concerning location determination on this inadequate record. Instead, the Commission should issue a Notice of Inquiry, a new NPRM or at most a Further Notice of Proposed Rulemaking setting out in detail what location technologies and requirements the Commission is considering and inviting comment on the privacy and innovation implications raised by those proposals.

Conclusion

The location information needs of E911 emergency communications in the VoIP and IP-enabled contexts can and should be addressed, but this need can be met without damaging the ability of our country to innovate and without creating an Orwellian surveillance society or otherwise harming our citizens' ability to protect the privacy of their location information.

For further information contact John Morris at 202-637-9800 or jmorris@cdt.org.