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."[1] 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[2]

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).[3]

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)

---

[1] *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")*.

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

[3] 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.[4] 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).

[4] *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.[5]

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.

[5] 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.