

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

In the Matter of)	
)	
E911 Requirements for IP-Enabled Service)	WC Docket No. 05-196
Providers)	

JOINT COMMENTS OF

**CENTER FOR DEMOCRACY & TECHNOLOGY,
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION,
ELECTRONIC FRONTIER FOUNDATION AND PULVER.COM**

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

Daniel L. Johnson
Computer & Communications
Industry Association
666 11th Street, NW
Washington, DC 20001

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

Jonathan Askin
pulver.com
1437 Rhode Island Ave., NW, #109
Washington, DC 20005

Dated: August 15, 2005

TABLE OF CONTENTS

SUMMARY.....ii

I. THE COMMISSION SHOULD PROMOTE BOTH THE DEVELOPMENT OF ADVANCED EMERGENCY TECHNOLOGY AND INNOVATION IN NON-EMERGENCY TECHNOLOGY..... 2

II. NPRM ¶ 57: THE COMMISSION SHOULD BE VERY CAUTIOUS AND LIMITED IN MANDATING AUTOMATIC LOCATION IDENTIFICATION TECHNOLOGY..... 3

A. Automatic Location Identification May Not Be Possible, and a Mandate of Such Identification May in Some Cases Harm Public Safety..... 4

B. Design Mandates on Ordinary Computers Would Exceed the Commission’s Authority and Would in Any Event Be Bad Policy..... 6

C. The Commission Should Promote, Not Discourage or Prohibit, User Control Over Their Own Location Information..... 7

D. The Commission Should Ensure That it Does Not Further the Development of an Orwellian Surveillance Society. 10

III. NPRM ¶ 58: THE COMMISSION SHOULD BE CAUTIOUS IN EXTENDING ANY E911 MANDATES TO IP SERVICES OTHER THAN INTERCONNECTED VoIP SERVICES THAT EMULATE POTS SERVICE..... 11

IV. NPRM ¶ 59: THE COMMISSION SHOULD NOT PERPETUATE THE CONTINUED DEPENDENCE ON THE ARCHAIC EMERGENCY TECHNOLOGY IN USE TODAY, AND SHOULD INSTEAD ENSURE THAT THE EMERGENCY SYSTEM EXPEDITIOUSLY MOVES INTO THE TWENTY-FIRST CENTURY..... 12

V. NPRM ¶ 62: THE COMMISSION SHOULD CREATE STRONG PRIVACY PROTECTIONS AGAINST THE UNPERMITTED USE OF LOCATION INFORMATION IN NON-EMERGENCY CONTEXTS..... 13

CONCLUSION 15

SUMMARY

The undersigned commenters agree on two important broad points: first, that the Commission should act to promote an effective and technologically advanced emergency reporting and communications system, and second, that in promoting such a system, the Commission must be careful not to retard technological progress in the emergency system, or stifle innovation and consumer choice in technology more broadly.

Specifically, the Commission should be very cautious in imposing any requirement for “automatic location identification” in the Internet Protocol-based context. Although automatic identification may be possible in some, but not in all, situations, it is unclear what authority the Commission would have to mandate that automatic location identification be an element of all VoIP-capable devices. Moreover, such a mandate would chill innovation and create significant risks to privacy.

The Commission should also be cautious in extending E911 mandates beyond the interconnected VoIP context, to avoid chilling innovation or driving it overseas. Along the same lines, the Commission should avoid perpetuating the use of the archaic and severely limited technology in use today in the emergency response system, or burden IP-based services with extensive long-term obligations to support the legacy system.

Finally, the Commission should act to protect privacy, and ensure that any new location identification technology that is used in the emergency VoIP context not be also used in non-emergency situations without the express permission of the user. There is a significant risk to privacy raised by location tracking technology, and the Commission should be careful not to exacerbate that risk.

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

In the Matter of)	
)	
E911 Requirements for IP-Enabled Service Providers)	WC Docket No. 05-196
)	

**JOINT COMMENTS OF

CENTER FOR DEMOCRACY & TECHNOLOGY,
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION,
ELECTRONIC FRONTIER FOUNDATION AND PULVER.COM**

The Center for Democracy & Technology, Computer & Communications Industry Association, Electronic Frontier Foundation, and pulver.com respectfully submit these comments on the Notice of Proposed Rulemaking (“NPRM”) portion of the First Report and Order and Notice of Proposed Rulemaking in WC Dockets No. 04-36 and 05-196, as released June 3, 2005.¹

The parties to these joint comments reflect a diversity of perspectives, ranging from Internet and telecommunications companies to public interest groups, but in this matter we agree on two important points: First, we agree that the Commission should act to promote an effective and technologically advanced emergency reporting and communications system. Second, we agree that in doing so, the Commission must exert great care that its rules do not retard technological progress in the emergency system, and do not stifle innovation and consumer

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) (“*First Order and NPRM*”).

choice in technology more broadly. The Commission's further NPRM in this matter raises questions and suggests tentative conclusions that may do great harm to these critical goals. We look forward to working with the Commission to promote an effective and advanced emergency system.

I. THE COMMISSION SHOULD PROMOTE BOTH THE DEVELOPMENT OF ADVANCED EMERGENCY TECHNOLOGY AND INNOVATION IN NON-EMERGENCY TECHNOLOGY

Underlying the Commission's First Report and Order and Notice of Proposed Rulemaking on emergency communications in the Internet Protocol ("IP") context is the appropriate and laudable goal of promoting the deployment of effective E911 services for VoIP services that emulate 911 in the POTS (plain old telephone service) context. The undersigned support this goal and the Commission's efforts toward it. But at the same time, in both the emergency communications context and IP communications context more broadly, the Commission should ensure that its actions do not hinder the innovation that can bring valuable technological advancements into use.

The goal of promoting technological innovation and the offering of advanced services applies both in the emergency context and more broadly. In the emergency context, as discussed more fully in later in these Comments, the Commission should avoid actions that would hinder the development and deployment of an advanced IP-based system for handling emergency communications. As communications increasingly move onto IP networks (voice communications, but also text communications such as instant messaging and eventually video communications), it is critical that the emergency communications and response system also evolve onto IP networks. Without such evolution (and without the corresponding move away

from legacy network elements like Selective Routers), the emergency system will fail to meet its potential.²

But the Commission should also be concerned about innovation and deployment of non-emergency technology, and thus should seek to avoid imposing emergency-focused mandates that have the result of hindering the development of valuable non-emergency technology. The development of robust emergency communications in the IP context need not prevent new modes of communications from emerging. There are a host of new and potential technologies, including location-based services, that offer enormous benefits for users but that could be hindered by overbroad emergency mandates. And such non-emergency technology can also contribute to public safety. Just as one will be able to instruct a device to “give me directions to the nearest Starbucks,” one will also be able to request directions to the nearest hospital, if this technology is allowed to develop without expensive mandates.

The Commission has correctly focused on consumer expectations in deciding that a VoIP service that seeks to closely emulate POTS should also provide an effective 911 service. But as communications technology moves away from traditional phones service, the Commission should allow new technologies to emerge and mature even if their capability to initiate emergency communications is more limited than a full E911 implementation.

II. NPRM ¶ 57: THE COMMISSION SHOULD BE VERY CAUTIOUS AND LIMITED IN MANDATING AUTOMATIC LOCATION IDENTIFICATION TECHNOLOGY

As the Commission announced in the second paragraph of its First Report and Order and Notice of Proposed Rulemaking, it “intend[s] in a future order to adopt an advanced E911

² Indeed, even referring to the emergency communications and response system as the “E911 system” is backwards-looking, and fails to acknowledge that traditional phone numbers are becoming less relevant.

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.”³

Although we appreciate the value of automatic location identification in the emergency context, for a number of reasons discussed below we urge the Commission to act with great caution in this area. Ill-considered action in this area could go a great distance toward destroying users' control over a highly private piece of information – their location.

A. Automatic Location Identification May Not Be Possible, and a Mandate of Such Identification May in Some Cases Harm Public Safety.

There is a broad range of technical efforts aimed at developing location identification technology that could contribute to automatic location identification, and we agree that in many contexts such technology could enhance IP-based emergency communications. For example, the Internet Engineering Task Force is actively working on modifications to the Dynamic Host Control Protocol to allow a device (such as an IP-based phone) to receive its location from a network upon initial connection to the network.⁴ These technologies, however, are only now being developed, and the technology development process could be short-circuited (and harmed) by governmental mandates.

Moreover, in many contexts, the availability of automatic location identification will depend on whether the operator of the network to which a user's device connects has deployed and activated network elements that can provide location information. If the end network has not deployed the most recent technology, it may well be impossible for an interconnected VoIP

³ *First Order and NPRM* ¶ 2, at 2.

⁴ See, e.g., RFC 3825, “Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information,” published July 2004, *available at* <http://www.ietf.org/rfc/rfc3825.txt>; H.Schulzrinne, Internet Draft, “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information,” published May 2005, *available at* <http://www.ietf.org/internet-drafts/draft-ietf-geopriv-dhcp-civil-06.txt> (work in progress).

provider to provide automatic location information. Unless this Commission intends, for example, to regulate in very fine detail the manufacture and deployment of all WiFi base stations (and to mandate the replacement of all existing base stations), there will for many years to come be non-compliant WiFi base stations through which a user could place an emergency VoIP call. As a threshold matter, as discussed more fully in the following subsections, this Commission lacks the authority to impose this type of mandate on the design and deployment of WiFi networks, and such a mandate could significantly increase the expense and complexity of consumer-oriented devices.

Most critically, although automatic location information is desirable, public safety would be harmed by inhibiting emergency calls that lacked such information. A simple hypothetical can illustrate the point. Assume that a person with a 2005-era laptop with 802.11b WiFi capability (and with a VoIP softphone program on the laptop) is driving down a street and sees a house on fire. Although the person does not have a cell phone, she notices that her laptop is receiving a WiFi signal, probably from a neighbor's open 802.11b base station. Although there is no automatic location information available, the person can use her VoIP softphone and report the fire. In our view, it is better from a public safety perspective to have this capability without a location feature rather than restrict the availability of such services unless they can reliably deliver location to the emergency system.

The broad point is that while the Commission may appropriately act to *encourage* automatic location identification in some context, it should hesitate to *require* VoIP providers to only offer service if such identification is possible. Such a mandate would harm both public safety and the development and deployment of broadly beneficial VoIP services. Ultimately, the Commission should take guidance from the emergency community itself – in a variety of

technical design contexts, leaders of the National Emergency Numbering Association (“NENA”) have indicated that given a choice of receiving an emergency call with no location information, or not receiving the call at all, the emergency community would certainly choose to take the call. Although location information is of course invaluable in the emergency context, the human-to-human communication (whether by voice, text, or other form) is what is most important.

B. Design Mandates on Ordinary Computers Would Exceed the Commission’s Authority and Would in Any Event Be Bad Policy.

In Paragraph 57 of the NPRM, the Commission asks whether it should

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?

First Order and NPRM ¶ 57, at 34. 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 interconnected VoIP services. *Id.* at 14 n.77. Taken together, the Commission appears to be considering imposing design mandates on ordinary personal computers and laptops, all of which (assuming they are of relatively modern vintage) can be used without further modification as VoIP clients. Many such computers are sold with speakers and microphones, and VoIP softphone client software is available for free on the Internet. For at least two reasons, it would be a mistake for the Commission to attempt to impose a design mandate on ordinary computers.

Most importantly, the Commission lacks the statutory authority to impose such mandates. The broadcast flag case is instructive; in that case, the D.C. Circuit wrote that “[t]he FCC has no congressionally delegated authority to regulate receiver apparatus after a transmission is complete.” *American Library Association v. Federal Communications Commission*, 406 F.3d

689, 705 (D.C. Cir. 2005). Similarly, except for narrowly focused authority concerning radio emissions, the Commission has no authority, ancillary or otherwise, to mandate specific features and design elements in general purpose computers, even if such computers can be used in communications that ultimately can reach the public switched telephone network (“PSTN”).

Moreover, such a design mandate would be bad policy because it would raise enormous privacy concerns, as discussed more fully below, and because it would increase the cost and complexity of common computers at a time when they need to be more fully deployed. This country has witnessed an amazing explosion of computer and communications technology, with extraordinary innovation and very broad (though not yet sufficient) deployment. The absence of governmental control over the development of such technology has been critical. The Commission would reverse decades of beneficial hands-off policy if it were to change course and seek to regulate ordinary computers.

C. The Commission Should Promote, Not Discourage or Prohibit, User Control Over Their Own Location Information.

There are four basic architectures in which some form of “automatic location” generation and transmittal is possible. It is crucial that the Commission neither mandates any one of the models nor not prohibits or discourages any of the models. The four basic models – all of which can fully support “automatic location determination” – are:

Source of Location Determination	Source of and Control Over Location Transmittal	Examples
Network	Network	As in most cellular contexts today, the network determines location (through triangulation from cell towers or other technology), and the network transmits the location on behalf of the user
User's Client Device	Network	A user's device determines its location (with GPS or similar technology), transmits the location to the network, and the network further transmits the location on behalf of the user
Network	User's Client Device	The network knows or determines the user's location (based on port mapping or triangulation techniques, for example), provides to the user's client device its location (possibly using the DHCP protocol enhancement discussed above), and the user's device controls the further transmission of the location information
User's Client Device	User's Client Device	A user's device determines its location (with GPS or similar technology), and it also controls the transmission of the location information

In its NPRM, it is unclear what the Commission means by the phrase “*without assistance from the user*” when the Commission states 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.”⁵ We assume that the Commission is concerned primarily about possible human input of location information that is transmitted with an emergency call. But if the Commission means to prohibit the active involvement of the user’s *client device* in the location determination and/or transmittal, then the Commission would effectively be precluding three of the four possible architectures described above. Moreover, the Commission would be creating a huge obstacle to the ability of users to control access to their own location information.

⁵ *First Order and NPRM* ¶ 2, at 2.

Such a prohibition by the Commission would directly undermine years of technology development focused on the transmittal of, and protection of, location information. The Internet Engineering Task Force (“IETF”) has since 2001 been actively developing in the “GeoPriv” working group technology to bind user’s location information with user-created location privacy rules.⁶ A key thrust 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. 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).

If the Commission requires that *neither* the human user *nor* the user’s device can be involved in a location determination in emergency calls, the Commission would severely inhibit a broad range of beneficial technology models. Although some in the emergency community would prefer to require that the network always be the entity to determine the location, such approach is both unrealistic in terms of how best to determine location, and harmful in terms of privacy. As discussed more fully below, if the Commission forces access providing networks to create “Big Brother” style location surveillance systems, the Commission would go a great distance toward destroyed the potential for user-controlled systems.

⁶ 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>.

D. The Commission Should Ensure That it Does Not Further the Development of an Orwellian Surveillance Society.

There is little doubt that emergency communications would benefit from the availability of automatic location technology in IP networks, and it is certainly appropriate for the Commission to encourage VoIP providers to accommodate such technology. But a mandate that automatic location technology always be available for all interconnected VoIP emergency communications – if that is even possible – could force the restructuring of many Internet access networks, and could create a much greater capacity to track the moment-by-moment location of ordinary citizens. Although emergency services might be helped by creating the ability to always track citizens, the society as a whole would be harmed by the loss of privacy and civil liberties that would almost certainly flow from such a system.

Critically, if it were to require the creation of “automatic location” technology as a condition of permitting common VoIP services, this Commission would be directly responsible for a major step toward a surveillance society that would be antithetical to many of the values on which this country is based. It is vitally important that in its laudable desire to promote a robust emergency system, the Commission must avoid creating the potential for constant surveillance.

This caution does not mean that the Commission must give up on an ambition to encourage automatic location information. A crucial element that would avoid the Big Brother scenario could be achieved by an endorsement (without a mandate) of the two “user controlled” models identified in the chart in the preceding subsection. If the user’s device is the locus of control over location information – even in an emergency situation – then users will be better able to protect their privacy in all situations. The Commission should be careful not to undermine such user control.

III. NPRM ¶ 58: THE COMMISSION SHOULD BE CAUTIOUS IN EXTENDING ANY E911 MANDATES TO IP SERVICES OTHER THAN INTERCONNECTED VoIP SERVICES THAT EMULATE POTS SERVICE

In Paragraph 58 of the NPRM, the Commission asks whether it should extend E911 obligations to any entities beyond those identified in its First Report and Order.⁷ The undersigned commenters support efforts by the Commission to promote robust E911 service for those VoIP providers who offer a broadly available commercial service that attempts to emulate the POTS service available from the circuit switched telephone network. But should the Commission impose mandates on other IP-based voice or other services, it would threaten the innovation that has been the hallmark of the Internet to date.

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 POTS, even if they have a way of ultimately connecting to the PSTN. If the Commission imposes 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 from 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 may not then 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

⁷ *First Order and NPRM ¶ 58*, at 34.

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 these technologies may never get off the ground in the first place.

This does not mean that the Commission can do nothing to *promote* robust emergency capabilities in new technologies. The Commission could, for example, require that a voice service that connects to the PSTN should prominently disclose any limitations on the ability to access the E911 system. Such disclosures would lead to market pressures on technology designers and providers to make emergency calling a viable and effective capability. But the Commission should not mandate such a capability for new and non-POTS-like voice services, or else the Commission risks stopping the emergence of such services.

IV. NPRM ¶ 59: THE COMMISSION SHOULD NOT PERPETUATE THE CONTINUED DEPENDENCE ON THE ARCHAIC EMERGENCY TECHNOLOGY IN USE TODAY, AND SHOULD INSTEAD ENSURE THAT THE EMERGENCY SYSTEM EXPEDITIOUSLY MOVES INTO THE TWENTY-FIRST CENTURY

In Paragraph 58 of the NPRM, the Commission asks among other questions whether it should “require VoIP service providers [to install] redundant trunks to each Selective Router?”⁸ But, as this Commission has squarely recognized, existing emergency networks “usually are based on a 25-year-old architecture and implemented with legacy components that place significant limitations on the functions that can be performed over the network.”⁹ Selective Routers are precisely an example of “legacy components” on which the current E911 system is

⁸ *First Order and NPRM* ¶ 59, at 34.

⁹ *Id.* ¶ 14, at 8.

based. Not only do legacy systems have extraordinary limitations in the type and volume of information they can carry, they are also expensive to install, maintain and operate.

Thus, to the extent that the Commission determines that it should require any particular type of connection into the existing emergency system, it should also make clear that such connections are temporary and that the entire system needs to migrate to an IP-based system. The Commission should structure any rules it promulgates to clearly articulate the expectation that the emergency community must move beyond its decades-old architectures and modes of operating, and must permit the more direct integration of IP-based services into the emergency network.

Furthermore, the Commission should also make clear that the current emergency system should also evolve to accept emergency IP-based communications that are *not* carried by interconnected VoIP service providers. For example, there are proposals to facilitate emergency communications using Instant Messaging and other related IP-based services.¹⁰ The emergency services community should be encouraged to develop ways to accept and respond to both voice and non-voice IP-based communications beyond what the Commission has already addressed.

V. NPRM ¶ 62: THE COMMISSION SHOULD CREATE STRONG PRIVACY PROTECTIONS AGAINST THE UNPERMITTED USE OF LOCATION INFORMATION IN NON-EMERGENCY CONTEXTS

In Paragraph 58 of the NPRM, the Commission asks whether it should “adopt any customer privacy protections related to provision of E911 service by interconnected VoIP service providers[.]”¹¹ Because location information is highly sensitive and there are strong temptations

¹⁰ See, e.g., H. Schulzrinne, Internet-Draft, “Emergency Services URI for the Session Initiation Protocol,” published Feb. 2004, available at <http://www.ietf.org/proceedings/04aug/I-D/draft-ietf-sipping-sos-00.txt> (work in progress).

¹¹ *First Order and NPRM* ¶ 62, at 35.

for commercial abuse of such information, to the extent the Commission imposes any obligations on services providers to determine location information, it should also impose accompanying obligations on those providers to make no use of location information outside of the emergency context without the express consent of the users.

As discussed above, the preferred approach would be for the end user to maintain control of his or her location information. Some network implementations, however, may require that the network be able to determine a user's location in an emergency call. To the extent that such technology is necessary, the Commission should ensure that any use of the technology beyond the emergency context would only take place with the user's consent.

The Commission also asks the authority it would have to impose such privacy rules. Without addressing any inherent authority the Commission might have to protect privacy in the IP context, the Commission certainly has authority to impose privacy limitations on any location obligations that the Commission has authority to impose. In other words, to the extent the Commission has any authority to impose location information obligations, that authority can be exercised in a limited matter to ensure that privacy is fully protected.

Location based services – including but not limited to emergency services – offer users enormous potential for beneficial services. But they also offer great room for abuse, and especially in this era of identity theft and stalking, it is important that privacy be a paramount concern of all involved in implementing these new technologies. If users perceive that using a given technology means that either Big Brother can track them at all times, or that commercial entities can flood them with location-based spam, the users will be far less likely to use the technology in the first place. The Commission should ensure that whatever it requires does not exacerbate these problems.

CONCLUSION

For the foregoing reasons, the undersigned commenters believe that the Commission should exercise great caution in imposing further E911 obligations on IP-based services.

ON BEHALF OF

CENTER FOR DEMOCRACY & TECHNOLOGY (www.cdt.org)
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (www.ccianet.org)
ELECTRONIC FRONTIER FOUNDATION (www.eff.org)
pulver.com (www.pulver.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

Daniel L. Johnson
Computer & Communications
Industry Association
666 11th Street, NW
Washington, DC 20001

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

Jonathan Askin
pulver.com
1437 Rhode Island Ave., NW, #109
Washington, DC 20005

Dated: August 15, 2005